VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

VARNOSTNA ANALIZA IN UPORABNIŠKA NADGRADNJA SPLETNE STRANI ANDROMA COLLIES

Kandidatka: Teja Sokalič

Vrsta študija: študentka izrednega študija

Študijski program: Informatika

Mentor predavatelj: mag. Dušan Brglez

Mentor v podjetju: Tim Medveš, inž. inf.

Lektorica: Špela Komac, dipl. slov.

Maribor, 2026

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Teja Sokalič sem avtorica diplomskega dela z naslovom *Varnostna analiza in uporabniška nadgradnja spletne strani Andromа Collies*, ki sem ga napisala pod mentorstvom mag. Dušana Brgleza.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbela, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oziroma citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oziroma misli kot mojih lastnih kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor, september 2026 Podpis študenta:

ZAHVALA

Iskreno se zahvaljujem mentorju **mag. Dušanu Brglezu** za strokovno pomoč, usmerjanje, koristne nasvete in podporo pri pripravi diplomskega dela.

Posebna zahvala gre tudi mentorju v podjetju **Timu Medvešu, inž. inf.,** za pomoč, strokovne predloge in sodelovanje pri izvedbi praktičnega dela naloge.

Zahvaljujem se svoji družini in bližnjim, ki so mi med študijem stali ob strani, me spodbujali in podpirali pri doseganju zastavljenih ciljev.

Posebno zahvalo namenjam tudi vsem, ki so na kakršenkoli način prispevali k nastanku tega diplomskega dela in mi pomagali pri uspešnem zaključku študija.

Teja Sokalič

POVZETEK

Kibernetska varnost in uporabniška izkušnja sta pomembna dejavnika kakovosti sodobnih spletnih strani. Namen diplomskega dela je bil analizirati spletno stran Androma Collies z vidika kibernetske varnosti in uporabniške izkušnje, prepoznati pomanjkljivosti ter predlagati izboljšave.

V teoretičnem delu so predstavljeni temeljni pojmi kibernetske varnosti, najpogostejše ranljivosti spletnih aplikacij po metodologiji OWASP Top 10 ter načela uporabniške izkušnje, dostopnosti in mobilne odzivnosti. Obravnavana sta tudi pomen varnostnih mehanizmov ter povezava med varnostjo in uporabnostjo.

V praktičnem delu je bila izvedena analiza spletne strani Androma Collies, ki je vključevala pregled povezave HTTPS, certifikata SSL, varnostnih headerjev HTTP in kontaktnega obrazca ter testiranje z orodji Mozilla Observatory, Google Lighthouse in SSL Labs. Z vidika uporabniške izkušnje so bili analizirani navigacija, vizualna podoba, mobilna odzivnost, hitrost nalaganja in dostopnost vsebin.

Na podlagi analize so bile izvedene varnostne in uporabniške izboljšave, med drugim implementacija Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), dodatnih varnostnih headerjev HTTP in zaščite kontaktnega obrazca z reCAPTCHA v3. Izboljšani so bili tudi navigacija, kontrasti, tipografija, dostopnost in hitrost nalaganja.

Rezultati ponovnega testiranja so pokazali izboljšanje spletne strani. Ocena Mozilla Observatory se je z D izboljšala na A, pri Google Lighthouse pa se je Performance povečal z 69 na 98, Accessibility z 88 na 100 in Best Practices s 74 na 100. Rezultati potrjujejo učinkovitost izvedenih izboljšav.

Ugotovitve kažejo, da je mogoče z ustreznimi tehničnimi in oblikovnimi izboljšavami hkrati povečati kibernetsko varnost in izboljšati uporabniško izkušnjo. Številni ukrepi ne zahtevajo velikih finančnih vložkov, temveč predvsem ustrezno konfiguracijo obstoječih sistemov in upoštevanje sodobnih priporočil.

Ključne besede: *kibernetska varnost, uporabniška izkušnja, spletna varnost, varnostni headerji HTTP, optimizacija spletnih strani*

ABSTRACT

Improving Cybersecurity and User Experience of the Andromma Collies Website

Cybersecurity and user experience are important factors in the quality of modern websites. The purpose of this thesis was to analyze the Andromma Collies website from the perspectives of cybersecurity and user experience, identify shortcomings, and propose improvements.
The theoretical part presents the fundamental concepts of cybersecurity, the most common web application vulnerabilities according to the OWASP Top 10 methodology, and the principles of user experience, accessibility, and mobile responsiveness. It also addresses the importance of security mechanisms and the relationship between security and usability.

The practical part involved an analysis of the Andromma Collies website, including an examination of the HTTPS connection, SSL certificate, HTTP security headers, and contact form, as well as testing with Mozilla Observatory, Google Lighthouse, and SSL Labs. From the user experience perspective, navigation, visual design, mobile responsiveness, loading speed, and content accessibility were analyzed.
Based on the analysis, security and usability improvements were implemented, including Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), additional HTTP security headers, and contact form protection using reCAPTCHA v3. Navigation, contrast, typography, accessibility, and loading speed were also improved.

The results of the repeated testing showed improvements to the website. The Mozilla Observatory rating improved from D to A, while Google Lighthouse Performance increased from 69 to 98, Accessibility from 88 to 100, and Best Practices from 74 to 100. The results confirm the effectiveness of the implemented improvements.
The findings show that appropriate technical and design improvements can simultaneously enhance cybersecurity and improve user experience. Many measures do not require significant financial investment but primarily proper configuration of existing systems and adherence to modern recommendations.

Keywords: *cybersecurity, user experience, web security, HTTP security headers, website optimization*

KAZALO VSEBINE

1 UVOD 10

1.1 Namen in cilji naloge 11
1.2 Raziskovalna vprašanja 11
1.3 Metodologija dela 12
1.4 Struktura diplomske naloge 13

2 TEORETIČNE OSNOVE KIBERNETSKE VARNOSTI 14

2.1 Opredelitev kibernetske varnosti 14
2.2 Najpogostejše ranljivosti spletnih strani (OWASP Top 10) 16
2.2.1 SQL Injection 16
2.2.2 Cross-Site Scripting (XSS) 17
2.2.3 Cross-Site Request Forgery (CSRF) 18
2.2.4 Nevarnosti pri avtentikaciji in geslih 19
2.3 Standardi in dobre prakse varnega razvoja spletnih strani 20
2.4 Vloga zakonodaje in etike (GDPR), varstvo osebnih podatkov 22

3 UPORABNIŠKA IZKUŠNJA (UX) IN OBLIKOVANJE SPLETNIH STRANI 24

3.1 Pomen uporabniške izkušnje v spletnem razvoju 24
3.2 UX načela (npr. Nielsenova heuristika) 25
3.3 UI oblikovanje in vizualna privlačnost 26
3.4 Mobilna odzivnost in dostopnost (smernice WCAG) 27
3.5 Razmerje med uporabniško izkušnjo in varnostjo (primeri, kjer se UX in varnost križata) 29

4 PREDSTAVITEV SPLETNE STRANI ANDROMA COLLIES 32

4.1 Opis in namen spletne strani (predstavitev psarne, cilji, ciljna publika) 32
4.2 Tehnološko ozadje strani (CMS, programski jeziki, strežnik) 32
4.3 Struktura in funkcionalnosti (npr. galerija, kontaktni obrazec, predstavitev psov) 33

5 ANALIZA OBSTOJEČEGA STANJA SPLETNE STRANI ANDROMA COLLIES 35

5.1 Varnostna analiza 35
5.1.1 Analiza HTTPS in certifikata SSL 36
5.1.2 Pregled varnostnih headerjev 37
5.1.3 Analiza obrazcev in obdelave podatkov 39
5.1.4 Testiranje in ranljivosti (OWASP ZAP, Mozilla Observatory, Lighthouse) 40

5.2 UX/UI ANALIZA 45
5.2.1 Struktura in navigacija *45*
5.2.2 Vizualni dizajn in barvna shema *46*
5.2.3 Mobilna odzivnost in hitrost nalaganja *49*
5.2.4 Dostopnost in berljivost vsebine *50*
6 PREDLAGANE IZBOLJŠAVE 52
6.1 VARNOSTNE IZBOLJŠAVE 52
6.1.1 Vpeljava varnostnih headerjev (CSP, HSTS, X-Frame-Options ...) *53*
6.1.2 Zaščita obrazcev (captcha, sanitizacija vhodov, CSRF tokeni) *56*
6.1.3 Optimizacija SSL/TLS nastavitev *60*
6.2 UX/UI IZBOLJŠAVE 61
6.2.1 Optimizacija navigacije *61*
6.2.2 Prilagoditev barv, tipografije in vizualnih elementov *62*
6.2.3 Izboljšave mobilne odzivnosti *63*
6.2.4 Pospešitev nalaganja strani *64*
6.2.5 Povzetek predlaganih UX/UI izboljšav *66*
7 IMPLEMENTACIJA IN TESTIRANJE 67
7.1 IZVEDBA VARNOSTNIH IZBOLJŠAV 67
7.1.1 Implementacija varnostnih headerjev HTTP *68*
7.1.2 Implementacija Google reCAPTCHA v3 ..... *69*
7.1.3 Rezultati izvedenih varnostnih izboljšav *71*
7.2 IZVEDBA UX/UI IZBOLJŠAV 71
7.2.1 Dodajanje alternativnih opisov slik (ALT) *72*
7.2.2 Optimizacija slik: pretvorba v format WebP *73*
7.2.3 Implementacija Lazy Loading *74*
7.2.4 Povzetek izvedenih UX/UI izboljšav *75*
7.3 TESTIRANJE PO IZBOLJŠAVAH 76
7.3.1 Testiranje z Mozilla Observatory *76*
7.3.2 Testiranje s Qualys SSL Labs *77*
7.3.3 Testiranje z Google Lighthouse *78*
7.3.4 Uporabniško testiranje *80*
7.4 PRIMERJAVA REZULTATOV PRED IZBOLJŠAVAMI IN PO NJIH 81
8 REZULTATI IN RAZPRAVA 83
8.1 ANALIZA DOSEŽENIH IZBOLJŠAV 83
8.2 RAZPRAVA O UČINKOVITOSTI VARNOSTNIH SPREMEMB 84

8.3 Razprava o vplivu UX/UI sprememb na uporabniško izkušnjo 85
8.4 Omejitve raziskave 86
8.5 Odgovori na raziskovalna vprašanja 87
8.6 Potrditev hipotez 88
9 SKLEP 90
10 VIRI IN LITERATURA 92

KAZALO SLIK

Slika 1: Mozilla Observatory Report 37
Slika 2: Kontaktni obrazec na spletni strani 40
Slika 3: Mozilla Observatory rezultat 41
Slika 4: Pregled strežniškega okolja spletne strani z Lighthouse 42
Slika 5: Vizualni dizajn spletne strani 47
Slika 6: Tipografija domače strani 48
Slika 7: Implementacija varnostnih headerjev v datoteki .htaccess 69
Slika 8: Povezava sistema Google reCAPTCHA v3 s kontaktnim obrazcem 70
Slika 9: Nastavitve Google reCAPTCHA v3 70
Slika 10: Dodajanje alternativnega opisa (ALT) fotografiji v knjižnici predstavnosti WordPress 73
Slika 11: Rezultat pretvorbe slik v format WebP z uporabo vtičnika Converter for Media 74
Slika 12: Implementacija atributa loading="lazy" v izvorni kodi spletne strani 75
Slika 13: Rezultat analize Mozilla Observatory po implementaciji varnostnih izboljšav 77
Slika 14: Rezultat analize SSL konfiguracije z orodjem Qualys SSL Labs 78
Slika 15: Rezultati Google Lighthouse za namizne naprave 79
Slika 16: Rezultati Google Lighthouse za mobilne naprave 79

KAZALO TABEL

Tabela 1: Nielsenove heuristike uporabnosti 25
Tabela 2: Rezultat analize varnostnih headerjev z orodjem Mozilla Observatory 37
Tabela 3: Ocena potencialnih izpostavljenosti OWASP tveganj 43
Tabela 4: Skupna ocena varnosti spletne strani 44
Tabela 5: Ocena strukture in navigacije na podlagi Nielsenovih heuristik 46
Tabela 6: Povzetek izvedenih varnostnih izboljšav 71

TABELA 7: POVZETEK IZVEDENIH UX/UI IZBOLJŠAV 75
TABELA 8: REZULTATI UPORABNIŠKEGA TESTIRANJA 80
TABELA 9: PRIMERJAVA REZULTATOV PRED IZVEDENIMI IZBOLJŠAVAMI IN PO NJIH 81
TABELA 10: POVZETEK DOSEŽENIH IZBOLJŠAV 84

SEZNAM KRATIC

KRATICA	POMEN
ALT	Alternative Text
CIA	Confidentiality, Integrity, Availability
CSP	Content Security Policy
CSRF	Cross-Site Request Forgery
CMS	Content Management System
GDPR	General Data Protection Regulation
HSTS	HTTP Strict Transport Security
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
MFA	Multi-Factor Authentication
OWASP	Open Worldwide Application Security Project
SEO	Search Engine Optimization
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UI	User Interface
URL	Uniform Resource Locator
UX	User Experience
WCAG	Web Content Accessibility Guidelines
XSS	Cross-Site Scripting

1 UVOD

V sodobni informacijski družbi spletne strani predstavljajo enega najpomembnejših komunikacijskih kanalov med organizacijami in njihovimi uporabniki. Ne glede na velikost organizacije spletna stran pogosto predstavlja prvi stik potencialnega uporabnika s podjetjem, društvom ali posameznikom, zato mora zagotavljati zanesljivo delovanje, ustrezno raven varnosti in kakovostno uporabniško izkušnjo. Zaradi vse večje digitalizacije poslovanja in vsakodnevne uporabe spletnih storitev se povečujejo tudi tveganja, povezana s kibernetskimi napadi, zlorabami podatkov in različnimi oblikami spletnih ranljivosti.

Kibernetska varnost postaja pomemben del razvoja in vzdrževanja spletnih strani. Lastniki spletnih mest morajo zagotavljati zaščito podatkov uporabnikov, preprečevati nepooblaščen dostop do sistemov ter zmanjševati možnost izkoriščanja ranljivosti spletnih aplikacij. Pri tem se pogosto uporabljajo smernice in priporočila organizacije OWASP (Open Worldwide Application Security Project), ki opredeljuje najpogostejše varnostne grožnje in ranljivosti spletnih aplikacij.

Poleg varnosti imata pomembno vlogo tudi uporabniška izkušnja (UX – User Experience) in oblikovanje uporabniškega vmesnika (UI – User Interface). Uporabniki pričakujejo pregledno navigacijo, hitro nalaganje vsebin, prilagojenost mobilnim napravam in enostavno uporabo spletnih funkcionalnosti. Slabo zasnovana spletna stran lahko uporabnike odvrne od uporabe storitev, ne glede na kakovost vsebine ali izdelkov, ki jih organizacija ponuja.

V diplomskem delu bo obravnavana spletna stran Androma Collies, ki predstavlja družinsko psarno dolgodlakih škotskih ovčarjev (Rough Collie). Spletna stran je namenjena predstavitvi psarne, njenih psov, legel in dosežkov ter vzpostavljanju komunikacije z obiskovalci in potencialnimi kupci mladičev. Ker je spletna stran pomemben informacijski in promocijski kanal, je ključno, da zagotavlja ustrezno raven varnosti ter uporabnikom omogoča prijetno in učinkovito uporabo.

Diplomsko delo združuje področji kibernetske varnosti in uporabniške izkušnje, saj sta obe področji tesno povezani. Ustrezno implementirani varnostni mehanizmi povečujejo zaupanje uporabnikov, medtem ko dobra uporabniška izkušnja omogoča učinkovitejšo in prijetnejšo uporabo spletnega mesta. Namen raziskave je ugotoviti trenutno stanje spletne strani Androma

Collies ter predlagati izboljšave, ki bodo prispevale k večji varnosti in boljši uporabniški izkušnji.

1.1 Namen in cilji naloge

Namen diplomskega dela je analizirati trenutno stanje spletne strani Andromа Collies z vidika kibernetske varnosti in uporabniške izkušnje ter na podlagi ugotovljenih pomanjkljivosti pripraviti predloge izboljšav. Raziskava bo usmerjena v prepoznavanje najpogostejših varnostnih tveganj spletnih aplikacij ter ocenjevanje kakovosti uporabniškega vmesnika in uporabniške izkušnje.

Glavni cilj diplomskega dela je ugotoviti, v kolikšni meri spletna stran izpolnjuje sodobne zahteve na področju varnosti in uporabnosti ter kako lahko predlagane izboljšave prispevajo k večji zaščiti uporabnikov in boljši uporabniški izkušnji.

Posamezni cilji diplomskega dela so:

- predstaviti teoretične osnove kibernetske varnosti spletnih aplikacij;
- predstaviti osnovna načela uporabniške izkušnje in uporabniškega vmesnika;
- analizirati obstoječe stanje spletne strani Andromа Collies;
- identificirati morebitne varnostne ranljivosti in pomanjkljivosti;
- oceniti uporabnost, dostopnost in mobilno odzivnost spletne strani;
- pripraviti predloge za izboljšanje varnosti in uporabniške izkušnje;
- izvesti testiranje predlaganih izboljšav;
- primerjati rezultate pred izvedenimi izboljšavami in po njih.

1.2 Raziskovalna vprašanja

Za doseganje zastavljenih ciljev bodo v diplomskem delu obravnavana naslednja raziskovalna vprašanja:

RV1: Kako varna je obstoječa spletna stran Andromа Collies glede na najpogostejše ranljivosti spletnih aplikacij (OWASP Top 10)?

RV2: Na kakšen način lahko predlagane varnostne izboljšave povečajo zaščito spletne strani, ne da bi negativno vplivale na uporabniško izkušnjo?

RV3: Kako lahko izboljšave uporabniškega vmesnika (UX/UI) prispevajo k večji dostopnosti, uporabnosti in posledično tudi varnejši uporabi spletne strani?

RV4: Zakaj je kibernetska varnost pomembna tudi za manjše organizacije, kot je psarna Andromа Collies, in kako prispeva k zaupanju uporabnikov?

Na podlagi raziskovalnih vprašanj so oblikovane naslednje hipoteze:

H1: Spletna stran Andromа Collies vsebuje varnostne pomanjkljivosti, ki jih je mogoče odkriti s standardnimi orodji za analizo spletnih aplikacij.

H2: Izboljšave na področju varnosti ne bodo negativno vplivale na uporabniško izkušnjo spletne strani.

H3: Izboljšave uporabniškega vmesnika in mobilne odzivnosti bodo povečale dostopnost in uporabnost spletne strani.

H4: Kibernetska varnost predstavlja pomemben dejavnik zaupanja uporabnikov tudi pri manjših organizacijah in spletnih predstavitvah.

1.3 Metodologija dela

Pri izdelavi diplomskega dela bo uporabljen aplikativni raziskovalni pristop, saj se raziskava osredotoča na konkretno spletno stran in na praktično uporabo teoretičnih spoznanj s področja kibernetske varnosti ter uporabniške izkušnje.

V teoretičnem delu bo uporabljena metoda analize strokovne in znanstvene literature s področja kibernetske varnosti, razvoja spletnih aplikacij, uporabniške izkušnje in spletne dostopnosti.

V raziskovalnem delu bodo uporabljene naslednje metode:

- analitična metoda, s katero bo izvedena varnostna in uporabniška analiza spletne strani;
- primerjalna metoda, s katero bodo ugotovitve primerjane s priporočili OWASP, WCAG in drugimi dobrimi praksami;

- razvojno-implementacijska metoda, s katero bodo pripravljeni in izvedeni predlogi izboljšav;
- evalvacijska metoda, s katero bodo ocenjeni učinki izvedenih sprememb.

Za izvedbo analize bodo uporabljena specializirana orodja, kot so OWASP ZAP, Mozilla Observatory in Google Lighthouse. Z njihovo pomočjo bodo pridobljeni podatki o varnostnih nastavitvah, konfiguraciji spletnega strežnika, uporabniški dostopnosti, zmogljivosti in splošni kakovosti spletne strani.

1.4 Struktura diplomske naloge

Diplomsko delo je sestavljeno iz devetih vsebinskih poglavij.

V prvem poglavju so predstavljeni problematika raziskave, namen in cilji naloge, raziskovalna vprašanja, metodologija dela ter struktura diplomskega dela.

Drugo poglavje obravnava teoretične osnove kibernetske varnosti, najpogostejše spletne ranljivosti, standarde varnega razvoja ter zakonodajne in etične vidike varovanja podatkov.

V tretjem poglavju so predstavljeni koncepti uporabniške izkušnje, uporabniškega vmesnika, dostopnosti in mobilne odzivnosti spletnih strani.

Četrto poglavje vsebuje predstavitev spletne strani Androma Collies, njen namen, tehnološko ozadje in funkcionalnosti.

V petem poglavju je izvedena analiza obstoječega stanja spletne strani z vidika kibernetske varnosti in uporabniške izkušnje.

Šesto poglavje vsebuje predloge izboljšav na področju varnosti in UX/UI oblikovanja.

V sedmem poglavju so opisani postopek implementacije izboljšav, testiranje in primerjava rezultatov pred izvedenimi spremembami in po njih.

Osmo poglavje predstavlja rezultate raziskave in razpravo o doseženih izboljšavah.

V devetem poglavju so podani zaključki, ključne ugotovitve raziskave ter predlogi za nadaljnji razvoj spletne strani Androma Collies.

2 TEORETIČNE OSNOVE KIBERNETSKE VARNOSTI

2.1 Opredelitev kibernetske varnosti

Kibernetska varnost predstavlja skupek tehnologij, procesov, politik in ukrepov, namenjenih zaščiti informacijskih sistemov, računalniških omrežij, programske opreme ter podatkov pred nepooblaščenim dostopom, zlorabo, poškodovanjem ali uničenjem. Grgić (2019) kibernetsko varnost opredeljuje kot kombinacijo organizacijskih, tehničnih in procesnih ukrepov, katerih namen je zaščita informacijskih sistemov, omrežij in podatkov pred različnimi varnostnimi grožnjami. Zaradi vse večje digitalizacije poslovanja, storitev in komunikacije postaja kibernetska varnost eno izmed ključnih področij sodobne informatike.

V preteklosti je bila zaščita informacijskih sistemov osredotočena predvsem na zaščito fizične infrastrukture in lokalnih računalniških omrežij. Razvoj interneta, spletnih aplikacij in storitev v oblaku pa je povzročil bistveno povečanje števila potencialnih varnostnih groženj. Posledično se organizacije vseh velikosti srečujejo z izzivi zagotavljanja zaupnosti, celovitosti in razpoložljivosti informacij (International Organization for Standardization, 2013).

Temeljni koncept kibernetske varnosti predstavlja model CIA (Confidentiality, Integrity, Availability). Po standardu ISO/IEC 27001 informacijska varnost temelji na treh ključnih načelih: zaupnosti (confidentiality), celovitosti (integrity) in razpoložljivosti (availability), ki skupaj predstavljajo osnovo za učinkovito zaščito informacijskih sistemov (International Organization for Standardization, 2013).

Zaupnost pomeni, da imajo dostop do informacij samo pooblaščene osebe. Za zagotavljanje zaupnosti organizacije uporabljajo različne mehanizme za nadzor dostopa, šifriranje podatkov in avtentikacijo uporabnikov (International Organization for Standardization, 2013).

Celovitost pomeni zagotavljanje točnosti in nespremenjenosti podatkov. Informacije morajo ostati natančne in zaščitene pred nepooblaščenimi spremembami, bodisi namernimi bodisi nenamernimi. Zagotavljanje celovitosti podatkov je pomembno za zanesljivo delovanje informacijskih sistemov in sprejemanje pravilnih poslovnih odločitev (International Organization for Standardization, 2013).

Razpoložljivost zagotavlja, da so sistemi in podatki dostopni pooblaščenim uporabnikom takrat, ko jih potrebujejo. Med najpogostejše grožnje razpoložljivosti sodijo izpadi strežnikov, tehnične napake in napadi za onemogočanje storitev (DoS oziroma DDoS napadi), ki lahko začasno ali trajno onemogočijo dostop do informacijskih virov (International Organization for Standardization, 2013).

Sodobna kibernetska varnost zajema več področij, med katerimi so varnost omrežij, varnost aplikacij, varnost podatkov, upravljanje identitet in dostopov ter ozaveščanje uporabnikov. Posebej pomembno področje predstavlja varnost spletnih aplikacij, saj so spletne strani in spletni sistemi pogosto izpostavljeni neposredno internetu in predstavljajo eno najpogostejših tarč kibernetskih napadov (Open Web Application Security Project, 2021).

Razvoj spletnih aplikacij zahteva upoštevanje varnostnih načel že v fazi načrtovanja in razvoja. Neustrezno zaščitene spletne strani lahko vsebujejo ranljivosti, ki napadalcem omogočajo dostop do podatkov, prevzem uporabniških računov ali motenje delovanja sistema. Zaradi tega številne organizacije uporabljajo mednarodne standarde in priporočila, kot so standard ISO/IEC 27001 in priporočila organizacije OWASP, ki pomagajo pri vzpostavljanju ustrezne ravni varnosti.

OWASP (Open Web Application Security Project, 2021) razvija smernice in priporočila za varnejši razvoj spletnih aplikacij ter pomaga organizacijam pri prepoznavanju in odpravljanju najpogostejših spletnih ranljivosti. Organizacija je posebej znana po seznamu OWASP Top 10, ki predstavlja pregled najpomembnejših varnostnih tveganj za spletne aplikacije (Open Web Application Security Project, 2021).

Kibernetska varnost ni pomembna le za velika podjetja in državne institucije, temveč tudi za manjše organizacije, društva in posameznike. Tudi manjše spletne strani pogosto zbirajo osebne podatke uporabnikov prek kontaktnih obrazcev, prijavnih sistemov ali drugih funkcionalnosti, zato morajo zagotavljati ustrezno zaščito teh podatkov. Učinkovita kibernetska varnost zmanjšuje tveganje za zlorabe, povečuje zaupanje uporabnikov in prispeva k dolgoročni uspešnosti spletnih storitev (Grgić, 2019).

2.2 Najpogostejše ranljivosti spletnih strani (OWASP Top 10)

Spletne aplikacije predstavljajo eno najpogostejših tarč kibernetskih napadov, saj pogosto obdelujejo občutljive podatke uporabnikov in omogočajo neposredno interakcijo prek interneta. Zaradi hitrega razvoja spletnih tehnologij se razvijajo tudi metode napadalcev, ki poskušajo izkoristiti ranljivosti v programski kodi, konfiguraciji sistemov ali neustrezno zaščitenih podatkih (Open Web Application Security Project, 2021).

Organizacija OWASP redno objavlja seznam najpogostejših in najnevarnejših varnostnih tveganj za spletne aplikacije, poznan pod imenom OWASP Top 10. Po navedbah organizacije je namen tega seznama razvijalcem, skrbnikom sistemov in organizacijam pomagati pri prepoznavanju, razumevanju ter odpravljanju najpomembnejših varnostnih pomanjkljivosti spletnih aplikacij.

Med najpogostejše ranljivosti sodijo napadi z vrivanjem kode (Injection), neustrezna avtentikacija uporabnikov, izpostavljenost občutljivih podatkov, napačna konfiguracija varnostnih nastavitev in različne oblike napadov na uporabniške seje. OWASP (Open Web Application Security Project, 2021) poudarja, da lahko takšne ranljivosti povzročijo izgubo zaupnosti, celovitosti in razpoložljivosti podatkov ter organizacijam povzročijo finančno in ugledno škodo. V okviru diplomskega dela bodo podrobneje predstavljene ranljivosti, ki so najpogosteje prisotne tudi pri manjših spletnih straneh in spletnih aplikacijah.

2.2.1 SQL Injection

SQL Injection predstavlja eno najstarejših in hkrati najnevarnejših ranljivosti spletnih aplikacij. Do napada pride, kadar aplikacija ne preverja ustrezno uporabniških vhodnih podatkov in omogoča njihovo neposredno vključevanje v SQL poizvedbe. Organizacija OWASP uvršča SQL Injection med najnevarnejše ranljivosti spletnih aplikacij, saj napadalcem omogoča manipulacijo podatkovnih baz in dostop do občutljivih informacij.

Napadalec lahko v obrazce za prijavo, iskalnike ali druge vnosne elemente vnese posebej oblikovane ukaze SQL, ki jih podatkovna baza izvrši kot legitimne poizvedbe. Posledice takšnega napada so lahko zelo resne, saj lahko napadalec pridobi dostop do podatkov, spreminja vsebino podatkovne baze ali celo prevzame popoln nadzor nad sistemom (OWASP Foundation, 2024).

Primer neustrezno zaščitene poizvedbe:

```
SELECT * FROM uporabniki
WHERE uporabnisko_ime = 'uporabnik'
AND geslo = 'geslo';
```

(Vir: lasten prikaz na podlagi OWASP Foundation (2024))

Če aplikacija vhodnih podatkov ne preverja ustrezno, lahko napadalec spremeni logiko poizvedbe in obide postopek prijave. Takšne ranljivosti nastanejo predvsem zaradi neposrednega vključevanja uporabniških podatkov v SQL ukaze brez ustrezne validacije ali filtriranja vhodov (OWASP Foundation, 2024).

Najpogostejše posledice SQL Injection napadov so:

- kraja osebnih podatkov uporabnikov,
- nepooblaščen dostop do administrativnih računov,
- spreminjanje ali brisanje podatkov,
- razkritje strukture podatkovne baze.

Za zaščito pred SQL Injection napadi OWASP Foundation (2024) priporoča uporabo parametriziranih poizvedb (prepared statements), validacijo vhodnih podatkov in dosledno uporabo načela najmanjših privilegijev. Ti ukrepi preprečujejo neposredno izvajanje zlonamernih SQL ukazov in bistveno zmanjšujejo možnost uspešnega napada.

Kljub številnim zaščitnim mehanizmom SQL Injection ostaja ena najpogostejših ranljivosti spletnih aplikacij, predvsem zaradi neustreznih programerskih praks, pomanjkljive validacije vhodnih podatkov in nezadostnega testiranja aplikacij (Open Web Application Security Project, 2021).

2.2.2 Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) predstavlja vrsto napada, pri katerem napadalec v spletno stran vnese zlonamerno skripto, ki se nato izvede v brskalniku drugih uporabnikov. OWASP Foundation (2024) pojasnjuje, da brskalnik takšno skripto obravnava kot zaupanja vredno vsebino spletnega mesta, kar napadalcu omogoča izvajanje zlonamerne kode v uporabnikovem

okolju. Posledice lahko vključujejo krajo sejnih piškotkov, preusmeritve uporabnikov na lažne spletne strani ali izvajanje dejanj brez uporabnikove vednosti.

XSS napadi se najpogosteje pojavljajo v obrazcih za komentarje, kontaktnih obrazcih, iskalnikih in drugih elementih, kjer uporabniki vnašajo besedilo. Če aplikacija teh podatkov ne preverja in ustrezno ne filtrira, se lahko zlonamerna koda shrani v sistem ali izvede neposredno v uporabnikovem brskalniku (OWASP Foundation, 2024).

Poznamo tri osnovne vrste XSS napadov:

- shranjeni (Stored XSS),
- odsevni (Reflected XSS),
- DOM-based XSS.

Pri shranjenem XSS napadu se zlonamerna koda shrani v podatkovno bazo in se nato prikaže vsakemu uporabniku, ki obišče prizadeto spletno stran. Odsevni XSS se izvede neposredno prek posebej oblikovanega URL naslova ali obrazca, medtem ko DOM-based XSS izkorišča ranljivosti v JavaScript kodi na strani odjemalca ter spreminja vsebino dokumenta neposredno v brskalniku uporabnika (OWASP Foundation, 2024).

Napadalec lahko z uspešnim XSS napadom:

- krade piškotke uporabniških sej,
- preusmerja uporabnike na lažne spletne strani,
- spreminja vsebino spletne strani,
- izvaja dejanja v imenu prijavljenega uporabnika.

Za zaščito pred XSS napadi OWASP Foundation (2024) priporoča dosledno validacijo vhodnih podatkov, kodiranje izhodov ter uporabo politike Content Security Policy (CSP). Kombinacija teh ukrepov bistveno zmanjša možnost izvajanja zlonamerne skriptne kode in poveča varnost spletnih aplikacij.

2.2.3 Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) je vrsta napada, pri katerem napadalec zavede prijavljenega uporabnika, da nevede izvede določeno dejanje na spletni strani, na katero je že prijavljen. OWASP Foundation (2024) pojasnjuje, da CSRF napadi izkoriščajo zaupanje

spletne aplikacije v uporabnikov brskalnik, zaradi česar lahko pride do izvajanja neželenih dejanj brez uporabnikove vednosti ali soglasja.

Pri tem napadalec ne pridobi neposrednega dostopa do uporabniškega računa, temveč izkoristi dejstvo, da je uporabnik že avtenticiran v sistemu. Brskalnik samodejno pošilja avtentikacijske piškotke, zato spletni strežnik zahtevo obravnava kot legitimno.

Primer CSRF napada je lahko sprememba uporabniškega gesla, pošiljanje kontaktnega obrazca ali izvedba finančne transakcije brez uporabnikove vednosti. Takšni napadi so posebej nevarni, ker jih uporabnik pogosto sploh ne opazi. Za uspešno izvedbo napada je lahko dovolj že obisk zlonamerne spletne strani ali klik na posebej pripravljeno povezavo (OWASP Foundation, 2024).

Za zaščito pred CSRF napadi se uporabljajo:

- CSRF varnostni žetoni (CSRF Tokens),
- preverjanje izvora zahtevkov,
- atribut SameSite pri piškotkih,
- dodatna avtentikacija za kritične operacije.

OWASP Foundation (2024) priporoča uporabo CSRF žetonov kot enega najučinkovitejših zaščitnih mehanizmov. Poleg tega preverjanje izvora zahtevkov in pravilna konfiguracija piškotkov pomembno zmanjšujeta možnost uspešnega CSRF napada ter povečujeta varnost spletnih aplikacij.

2.2.4 Nevarnosti pri avtentikaciji in geslih

Avtentikacija predstavlja postopek preverjanja identitete uporabnika pred dostopom do sistema. Čeprav gre za osnovni varnostni mehanizem, so prav težave pri upravljanju uporabniških računov in gesel med najpogostejšimi vzroki varnostnih incidentov. Organizacija OWASP (2021) ugotavlja, da neustrezna avtentikacija in upravljanje identitet še vedno sodita med najpogostejše ranljivosti sodobnih spletnih aplikacij.

Med najpogostejše pomanjkljivosti sodijo:

- uporaba šibkih gesel,
- ponovna uporaba istih gesel na različnih sistemih,

- pomanjkanje večfaktorske avtentikacije,
- neustrezna zaščita prijavnih obrazcev,
- pomanjkljiva politika upravljanja uporabniških računov.

Napadalci pogosto uporabljajo tehnike ugibanja gesel (Brute Force), napade s slovarjem (Dictionary Attack) ali uporabo podatkov iz že znanih varnostnih incidentov. Zaradi množičnih uhajanj podatkov se pogosto zgodi, da uporabniki uporabljajo enaka gesla na več različnih spletnih mestih, kar dodatno povečuje tveganje za nepooblaščen dostop do uporabniških računov (Open Web Application Security Project, 2021).

Eden izmed najpomembnejših ukrepov za izboljšanje varnosti je uporaba večfaktorske avtentikacije (MFA). Po priporočilih organizacije OWASP (2021) večfaktorska avtentikacija bistveno zmanjša možnost zlorabe uporabniških računov tudi v primeru kraje ali razkritja uporabniškega gesla, saj poleg gesla zahteva še dodatno obliko preverjanja identitete uporabnika.

Razvijalci morajo zagotoviti ustrezno shranjevanje gesel z uporabo sodobnih kriptografskih zgoščevalnih algoritmov, kot so bcrypt, Argon2 ali PBKDF2. OWASP Foundation (2024) priporoča uporabo teh algoritmov, saj zagotavljajo višjo stopnjo zaščite gesel pred napadi z ugibanjem ali krajo podatkovnih baz. Poleg tega je pomembno uporabnike spodbujati k uporabi močnih, dolgih in edinstvenih gesel.

Neustrezna avtentikacija lahko povzroči nepooblaščen dostop do sistemov, krajo podatkov in izgubo zaupanja uporabnikov, zato predstavlja eno najpomembnejših področij sodobne kibernetske varnosti (Open Web Application Security Project, 2021).

2.3 Standardi in dobre prakse varnega razvoja spletnih strani

Varnost spletnih aplikacij ni odvisna zgolj od posameznih zaščitnih mehanizmov, temveč predvsem od sistematičnega pristopa k načrtovanju, razvoju in vzdrževanju spletnih rešitev. Zaradi vse večjega števila kibernetskih groženj organizacije uporabljajo različne standarde, metodologije in dobre prakse, ki pomagajo zmanjševati tveganja ter zagotavljati ustrezno raven zaščite informacijskih sistemov (International Organization for Standardization, 2013).

Po priporočilih organizacije OWASP (2021) sodobni pristopi k razvoju spletnih aplikacij temeljijo na načelu »Security by Design«, ki predvideva vključevanje varnostnih zahtev že v

zgodnjih fazah razvoja sistema. Namen takšnega pristopa je zmanjšati število ranljivosti že med načrtovanjem in razvojem aplikacije ter preprečiti kasnejše varnostne težave.

Med najbolj znanimi organizacijami na področju spletne varnosti je OWASP (Open Worldwide Application Security Project), ki razvijalcem ponuja smernice za varno programiranje, testiranje in upravljanje spletnih aplikacij. Poleg seznama OWASP Top 10 organizacija objavlja tudi priporočila za varen razvoj programske opreme, ki vključujejo preverjanje vhodnih podatkov, varno upravljanje sej uporabnikov, uporabo kriptografskih mehanizmov in zaščito pred najpogostejšimi vrstami napadov (Open Web Application Security Project, 2021).

Pomembno načelo varnega razvoja predstavlja validacija vhodnih podatkov. OWASP Foundation (2024) poudarja, da morajo biti vsi podatki, ki jih uporabnik vnese v obrazce, prijavne sisteme ali druge elemente spletne aplikacije, ustrezno preverjeni in obdelani pred nadaljnjo uporabo. S tem se zmanjšuje možnost uspešnih napadov, kot so SQL Injection, Cross-Site Scripting (XSS) in druge oblike vbrizgavanja zlonamerne kode.

Drugo pomembno načelo je načelo najmanjših privilegijev (Principle of Least Privilege). Po standardu ISO/IEC 27001 naj imajo uporabniki, aplikacije in procesi dostop le do tistih virov in funkcionalnosti, ki jih nujno potrebujejo za svoje delo (International Organization for Standardization, 2013). S tem se omeji obseg škode v primeru zlorabe uporabniškega računa ali uspešnega vdora v sistem.

Pogosto uporabljeno načelo je tudi večplastna zaščita (Defense in Depth). Mednarodni standardi informacijske varnosti priporočajo uporabo več medsebojno dopolnjujočih zaščitnih ukrepov namesto zanašanja na en sam varnostni mehanizem (International Organization for Standardization, 2013). Primer takšnega pristopa je kombinacija požarnega zidu, zaščite aplikacijskega strežnika, varnostnih headerjev, preverjanja uporabniških vhodov in večfaktorske avtentikacije. Če ena plast zaščite odpove, druge še vedno zmanjšujejo možnost uspešnega napada.

Mednarodno priznani standard na področju upravljanja informacijske varnosti predstavlja standard ISO/IEC 27001. Standard organizacijam omogoča vzpostavitev sistema upravljanja informacijske varnosti (ISMS – Information Security Management System), ki vključuje prepoznavanje tveganj, določanje varnostnih politik, izvajanje nadzornih ukrepov ter redno spremljanje učinkovitosti zaščitnih mehanizmov. Njegov osnovni namen je zagotavljanje

zaupnosti, celovitosti in razpoložljivosti informacij (International Organization for Standardization, 2013).

Pomemben del varnega razvoja so tudi redne posodobitve programske opreme. Po priporočilih WordPress Foundation (2024) zastarele različice sistemov, vtičnikov in programskih knjižnic pogosto vsebujejo znane ranljivosti, ki jih napadalci lahko izkoristijo za pridobitev nepooblaščenega dostopa. Zato morajo organizacije redno spremljati varnostne posodobitve in jih pravočasno nameščati.

Priporočljiva praksa je tudi redno izvajanje varnostnih pregledov in testiranj. Med najpogosteje uporabljene metode sodijo pregled izvorne kode, avtomatizirano testiranje ranljivosti, penetracijsko testiranje ter uporaba specializiranih orodij, kot so OWASP ZAP, Burp Suite, Mozilla Observatory in Google Lighthouse. Takšna orodja omogočajo pravočasno odkrivanje varnostnih pomanjkljivosti in preverjanje skladnosti spletnih aplikacij z varnostnimi priporočili ((Mozilla, 2024); (Google, 2024)).

Varnost spletnih aplikacij je proces, ki zahteva neprekinjeno spremljanje, nadgrajevanje in prilagajanje novim grožnjam. Uporaba mednarodnih standardov, dobrih praks in sodobnih orodij organizacijam omogoča učinkovitejše upravljanje tveganj ter zagotavljanje varnega delovanja spletnih storitev (International Organization for Standardization, 2013).

2.4 Vloga zakonodaje in etike (GDPR), varstvo osebnih podatkov

Poleg tehničnih varnostnih ukrepov morajo upravljavci spletnih strani upoštevati tudi zakonodajne in etične vidike obdelave podatkov. Spletne strani pogosto zbirajo osebne podatke uporabnikov prek kontaktnih obrazcev, prijav na e-novice, registracijskih sistemov ali drugih oblik komunikacije. Zaradi tega je zagotavljanje ustrezne zaščite osebnih podatkov postalo pomembna zakonska in moralna odgovornost organizacij (European Parliament and Council of the European Union, 2016).

Na območju Evropske unije področje varstva osebnih podatkov ureja Splošna uredba o varstvu podatkov (GDPR – General Data Protection Regulation), ki se uporablja od leta 2018. Evropski parlament in Svet Evropske unije (2016) navajata, da je namen uredbe zagotoviti enotno raven zaščite osebnih podatkov vseh državljanov Evropske unije in povečati preglednost obdelave osebnih podatkov.

GDPR določa, da morajo organizacije osebne podatke zbirati zakonito, pošteno in pregledno. Posamezniki morajo biti jasno obveščeni o tem, katere podatke organizacija zbira, za kakšen namen jih uporablja in kako dolgo jih hrani. Poleg tega imajo uporabniki pravico do vpogleda v svoje podatke, popravka netočnih podatkov, omejitve obdelave in izbrisa podatkov, kar prispeva k večjemu nadzoru posameznika nad lastnimi osebnimi podatki (European Parliament and Council of the European Union, 2016).

Za spletne strani je posebej pomembno načelo minimizacije podatkov. Po določilih GDPR naj organizacije zbirajo le tiste podatke, ki so nujno potrebni za izvajanje določene storitve ali dosego zakonitega namena obdelave (European Parliament and Council of the European Union, 2016). Če spletna stran uporablja kontaktni obrazec, ni smiselno zahtevati več podatkov, kot jih dejansko potrebuje za odgovor uporabniku.

Pomembno področje predstavlja tudi uporaba piškotkov. Uporabniki morajo biti ustrezno obveščeni o uporabi piškotkov ter imeti možnost izbire glede njihove uporabe. To je posebej pomembno pri analitičnih in marketinških piškotkih, ki omogočajo spremljanje uporabniškega vedenja in zbiranje dodatnih informacij o obiskovalcih spletnega mesta (European Parliament and Council of the European Union, 2016).

Poleg zakonodajnih zahtev ima pomembno vlogo tudi etika. Upravljavci spletnih strani morajo podatke uporabnikov obdelovati odgovorno, pregledno in skladno z namenom, za katerega so bili zbrani. Evropski parlament in Svet Evropske unije (2016) poudarjata pomen preglednosti in odgovornega ravnanja z osebnimi podatki, saj zaupanje uporabnikov predstavlja enega ključnih dejavnikov uspešnega delovanja spletnih storitev.

Varnostni incidenti, uhajanje podatkov ali neustrezna obdelava osebnih podatkov lahko povzročijo finančno škodo, izgubo ugleda in zmanjšanje zaupanja uporabnikov. Zato morajo organizacije poleg tehničnih rešitev poskrbeti tudi za skladnost z zakonodajo in spoštovanje etičnih načel pri upravljanju informacij (European Parliament and Council of the European Union, 2016).

Za spletno stran Androma Collies je upoštevanje zakonodaje o varstvu osebnih podatkov pomembno predvsem zaradi uporabe kontaktnih obrazcev in komunikacije z obiskovalci spletnega mesta. Ustrezna zaščita podatkov in pregledna politika zasebnosti prispevata k večjemu zaupanju uporabnikov ter skladnosti delovanja spletne strani z veljavnimi predpisi.

3 UPORABNIŠKA IZKUŠNJA (UX) IN OBLIKOVANJE SPLETNIH STRANI

3.1 Pomen uporabniške izkušnje v spletnem razvoju

V sodobnem spletnem razvoju ni več dovolj, da spletna stran zgolj deluje in vsebuje potrebne informacije. Uporabniki pričakujejo hitro, intuitivno in prijetno uporabo spletnih storitev, zato postaja uporabniška izkušnja (UX – User Experience) eden ključnih dejavnikov uspešnosti spletnih strani in aplikacij (Norman, 2013).

Uporabniška izkušnja predstavlja celoten vtis uporabnika med interakcijo z izdelkom, storitvijo ali sistemom. Po mnenju Normana (2013) uporabniška izkušnja zajema vse vidike uporabnikove interakcije s sistemom, vključno z uporabnostjo, dostopnostjo, učinkovitostjo, razumljivostjo in splošnim zadovoljstvom pri uporabi. V kontekstu spletnih strani tako vključuje vse elemente, ki vplivajo na uporabnikovo zadovoljstvo, med drugim navigacijo, hitrost delovanja, dostopnost, razumljivost vsebine in vizualno podobo spletnega mesta.

Pojem uporabniške izkušnje je v devetdesetih letih prejšnjega stoletja popularizíral Don Norman, ki je poudarjal, da mora biti razvoj digitalnih izdelkov osredotočen na potrebe uporabnikov. Cilj UX oblikovanja je ustvariti okolje, v katerem lahko uporabnik svoje naloge opravi hitro, učinkovito in brez nepotrebnih zapletov (Norman, 2013).

Krug (2014) ugotavlja, da uporabniki pri uporabi spletnih strani ne želijo razmišljati o načinu delovanja sistema, temveč želijo čim hitreje doseči svoj cilj. Raziskave uporabniške izkušnje kažejo, da uporabniki zelo hitro oblikujejo prvi vtis o spletni strani ter ocenijo njeno profesionalnost, preglednost in verodostojnost. Če uporabnik težko najde iskane informacije ali se srečuje z zapleteno navigacijo, obstaja velika verjetnost, da bo spletno stran zapustil in poiskal informacije drugje (Krug, 2014).

Pomemben vidik uporabniške izkušnje predstavlja tudi zaupanje uporabnikov. Profesionalna zasnova, pregledna struktura in jasna komunikacija ustvarjajo občutek varnosti in verodostojnosti. Nielsen (1994) poudarja, da dobro zasnovani uporabniški vmesniki zmanjšujejo možnost napak, povečujejo učinkovitost uporabe ter prispevajo k večjemu zaupanju uporabnikov v sistem. To je še posebej pomembno pri spletnih straneh, ki zbirajo osebne podatke uporabnikov ali omogočajo različne oblike spletne komunikacije.

Pri načrtovanju uporabniške izkušnje se običajno upoštevajo naslednja načela:

- uporabnost (usability),
- dostopnost (accessibility),
- učinkovitost uporabe,
- razumljivost vsebine,
- estetska privlačnost,
- zadovoljstvo uporabnikov.

Shneiderman idr. (2017) poudarjajo, da uspešna uporabniška izkušnja temelji na kombinaciji funkcionalnosti, preproste uporabe in estetsko dovršenega uporabniškega vmesnika. Kakovostna uporabniška izkušnja organizacijam prinaša številne koristi, kot so večje zadovoljstvo uporabnikov, večja stopnja zaupanja, daljši čas obiska spletnega mesta in boljša učinkovitost doseganja poslovnih ciljev. Zaradi tega UX danes predstavlja pomemben del razvoja sodobnih spletnih strani in aplikacij.

3.2 UX načela (npr. Nielsenova heuristika)

Med najbolj znanimi metodami za ocenjevanje uporabniške izkušnje sodijo Nielsenove heuristike uporabnosti, ki jih je razvil strokovnjak za uporabniško izkušnjo Jakob Nielsen. Gre za deset splošnih načel, ki služijo kot smernice pri načrtovanju in vrednotenju uporabniških vmesnikov ter pomagajo pri prepoznavanju najpogostejših težav uporabnosti (Nielsen Norman Group, 2024).

Tabela 1 prikazuje deset Nielsenovih heuristik, ki se pogosto uporabljajo pri analizi uporabniške izkušnje spletnih strani in aplikacij.

Tabela 1: Nielsenove heuristike uporabnosti

Nielsenova heuristika	**Opis**
Vidnost stanja sistema	Sistem mora uporabniku vedno jasno prikazovati trenutno stanje in ga obveščati o rezultatih njegovih dejanj.
Skladnost med sistemom in resničnim svetom	Uporabljati je treba jezik in izraze, ki jih uporabniki razumejo in poznajo iz vsakdanjega življenja.
Nadzor in svoboda uporabnika	Uporabniki morajo imeti možnost preklicati dejanja, popraviti napake ali se vrniti na prejšnje korake.

Doslednost in standardi	Enaki elementi morajo imeti enak videz in funkcijo skozi celotno spletno stran.
Preprečevanje napak	Oblikovanje mora uporabnikom pomagati preprečiti napake še pred njihovim nastankom.
Prepoznavanje namesto pomnjenja	Pomembne informacije in funkcije morajo biti vidne ter lahko dostopne.
Prilagodljivost in učinkovitost uporabe	Sistem mora omogočati učinkovito uporabo tako začetnikom kot izkušenim uporabnikom.
Estetsko in minimalistično oblikovanje	Vmesnik naj vsebuje le potrebne informacije in elemente, ki podpirajo uporabnikove cilje.
Pomoč pri prepoznavanju in odpravljanju napak	Sporočila o napakah morajo biti jasna, razumljiva in uporabniku ponuditi rešitev problema.
Pomoč in dokumentacija	Uporabnikom je smiselno zagotoviti dodatna pojasnila, navodila ali podporo pri uporabi sistema.

Vir: Prirejeno po Nielsen (1994) in Nielsen Norman Group (2024).

Nielsenove heuristike predstavljajo eno najpogosteje uporabljenih metod za vrednotenje uporabniške izkušnje in se še danes uporabljajo pri analizi uporabniških vmesnikov ter prepoznavanju težav uporabnosti (Nielsen Norman Group, 2024). Zaradi svoje enostavnosti in učinkovitosti bodo uporabljene tudi pri analizi spletne strani Androma Collies.

3.3 UI oblikovanje in vizualna privlačnost

Uporabniški vmesnik (UI – User Interface) predstavlja vizualni del spletne strani, s katerim uporabnik neposredno komunicira. Vključuje postavitev elementov, tipografijo, barve, gumbe, slike, ikone in druge grafične komponente. Po mnenju Shneidermana idr. (2017) uporabniški vmesnik predstavlja povezavo med uporabnikom in informacijskim sistemom ter pomembno vpliva na učinkovitost in zadovoljstvo pri uporabi.

Glavni cilj UI oblikovanja je ustvariti estetsko privlačno in hkrati funkcionalno okolje, ki uporabniku omogoča preprosto uporabo spletne strani. Dobro oblikovan uporabniški vmesnik pozitivno vpliva na prvi vtis uporabnika, izboljšuje uporabniško izkušnjo in povečuje zaupanje v spletno mesto (Krug, 2014).

Pri oblikovanju uporabniškega vmesnika imajo pomembno vlogo naslednji elementi:

- barvna shema,
- tipografija,
- kontrast med elementi,
- razporeditev vsebine,
- uporaba slik in grafičnih elementov,
- vizualna hierarhija informacij.

Barve pomembno vplivajo na uporabnikovo dojemanje spletne strani. Ustrezna kombinacija barv izboljšuje berljivost, usmerja pozornost uporabnikov in prispeva k prepoznavnosti blagovne znamke. Shneiderman idr. (2017) poudarjajo, da mora izbira barv podpirati uporabnikove naloge ter omogočati jasno razlikovanje med posameznimi elementi uporabniškega vmesnika. Prav tako je pomembna uporaba zadostnega kontrasta med ozadjem in besedilom, saj to vpliva na dostopnost vsebine.

Tipografija mora zagotavljati dobro berljivost na različnih napravah. Priporočljiva je uporaba jasnih in preprostih pisav ter ustrezne velikosti besedila. Krug (2014) ugotavlja, da uporabniki vsebine na spletnih straneh pogosto pregledujejo in ne berejo podrobno, zato mora biti besedilo oblikovano tako, da omogoča hitro zaznavanje ključnih informacij.

Pomemben element uporabniškega vmesnika predstavlja tudi vizualna hierarhija, ki uporabnikom pomaga razumeti pomembnost posameznih informacij in jih usmerja skozi vsebino spletne strani. Uporaba naslovov, podnaslovov, kontrastov, velikosti pisav in razmikov omogoča boljšo organizacijo informacij ter hitrejše iskanje želenih vsebin (Shneiderman, in drugi, 2017).

Vizualna privlačnost sama po sebi ni dovolj. Uspešen uporabniški vmesnik mora hkrati zagotavljati preglednost, funkcionalnost in učinkovito podporo uporabniški izkušnji. Po mnenju Kruga (2014) je najboljši uporabniški vmesnik tisti, ki uporabniku omogoča doseganje ciljev na čim bolj preprost in intuitiven način.

3.4 Mobilna odzivnost in dostopnost (smernice WCAG)

V zadnjih letih se je način uporabe spleta precej spremenil. Vedno več uporabnikov dostopa do spletnih strani prek pametnih telefonov in tabličnih računalnikov, zato mora biti sodobna spletna stran prilagojena različnim velikostim zaslonov in načinom uporabe. Takšno

prilagodljivost imenujemo mobilna odzivnost (Responsive Web Design). Po smernicah W3C mora biti uporabniška izkušnja dosledna in učinkovita ne glede na napravo, ki jo uporablja obiskovalec spletne strani (W3C Web Accessibility Initiative, 2018).

Mobilno odzivna spletna stran samodejno prilagaja razporeditev elementov, velikost besedila, slik in navigacijskih menijev glede na napravo, ki jo uporablja obiskovalec. Cilj mobilne odzivnosti je zagotoviti enako kakovostno uporabniško izkušnjo ne glede na velikost zaslona ter omogočiti učinkovito uporabo spletnih vsebin na vseh napravah (W3C Web Accessibility Initiative, 2018).

Neustrezna prilagoditev mobilnim napravam lahko povzroči številne težave, kot so:

- otežena navigacija,
- premajhna velikost besedila,
- nepravilno prikazani elementi,
- počasno nalaganje strani,
- povečano število predčasnih odhodov uporabnikov s spletne strani.

Poleg mobilne odzivnosti je pomembna tudi dostopnost spletnih vsebin. Dostopnost pomeni, da lahko spletno stran uporabljajo vsi uporabniki, vključno z osebami z različnimi oblikami oviranosti, kot so slabovidnost, slepota, gibalne omejitve ali težave pri zaznavanju vsebin. Namen dostopnosti je zagotoviti enakovreden dostop do informacij in funkcionalnosti ne glede na posameznikove sposobnosti ali uporabljeno tehnologijo (W3C Web Accessibility Initiative, 2018).

Najpomembnejše smernice za zagotavljanje dostopnosti predstavljajo smernice WCAG (Web Content Accessibility Guidelines), ki jih razvija organizacija W3C. Namen teh smernic je zagotoviti enakopraven dostop do spletnih vsebin za vse uporabnike in razvijalcem ponuditi priporočila za načrtovanje dostopnih spletnih rešitev (W3C Web Accessibility Initiative, 2018).

WCAG temelji na štirih osnovnih načelih:

- **Zaznavnost (Perceivable)**

Vsebina mora biti predstavljena na način, ki ga uporabniki lahko zaznajo. To vključuje uporabo alternativnih opisov slik (alt opisov), ustrezen kontrast med besedilom in ozadjem ter možnost prilagoditve velikosti besedila.

- **Upravljivost (Operable)**

Vsi elementi spletne strani morajo biti dostopni tudi uporabnikom, ki uporabljajo tipkovnico ali druge pomožne tehnologije. Uporabnik mora biti sposoben uporabljati spletno stran brez miške.

- **Razumljivost (Understandable)**

Informacije in delovanje spletne strani morajo biti jasni in predvidljivi. Uporabniki morajo razumeti pomen vsebine in posledice svojih dejanj.

- **Robustnost (Robust)**

Spletna stran mora biti združljiva z različnimi brskalniki, napravami in pomožnimi tehnologijami, kot so bralniki zaslona.

Navedena načela predstavljajo temelj smernic WCAG 2.1 in služijo kot osnova za razvoj dostopnih spletnih rešitev (W3C Web Accessibility Initiative, 2018).

Pri ocenjevanju dostopnosti spletnih strani se pogosto preverjajo naslednji elementi:

- kontrast med besedilom in ozadjem,
- uporaba alternativnih opisov slik,
- logična struktura naslovov,
- pravilna uporaba HTML oznak,
- dostopnost navigacije s tipkovnico,
- prilagoditev mobilnim napravam.

Dostopnost ni pomembna zgolj zaradi zakonodajnih zahtev, temveč tudi zaradi izboljšanja splošne uporabniške izkušnje. Po smernicah WCAG so dostopne spletne strani običajno preglednejše, bolj razumljive in prijaznejše za vse uporabnike, ne glede na njihove sposobnosti ali uporabljeno tehnologijo (W3C Web Accessibility Initiative, 2018).

3.5 Razmerje med uporabniško izkušnjo in varnostjo (primeri, kjer se UX in varnost križata)

Na prvi pogled se lahko zdi, da sta uporabniška izkušnja in kibernetska varnost ločeni področji, vendar sta v sodobnem spletnem razvoju tesno povezani. Uspešna spletna stran mora zagotavljati ustrezno raven varnosti, hkrati pa uporabnikom omogočati preprosto in prijetno

uporabo. Norman (2013) poudarja, da morajo biti digitalni sistemi zasnovani tako, da podpirajo uporabnikove potrebe ter hkrati zmanjšujejo možnost napak in neželenih dejanj.

V preteklosti so bili varnostni mehanizmi pogosto zasnovani predvsem z vidika zaščite sistema, pri čemer se je uporabniška izkušnja postavljala v ozadje. Posledica tega so bili zapleteni postopki prijave, težko razumljiva varnostna opozorila in zahtevni postopki preverjanja identitete. Takšni sistemi sicer povečujejo varnost, vendar lahko zmanjšajo zadovoljstvo uporabnikov in otežijo učinkovito uporabo spletnih storitev (Krug, 2014).

Sodobni pristopi k razvoju spletnih aplikacij poudarjajo ravnovesje med varnostjo in uporabnostjo. Varnostni mehanizmi morajo biti zasnovani tako, da uporabnikom ne predstavljajo nepotrebnih ovir, temveč jih učinkovito ščitijo pred tveganji. OWASP (Open Web Application Security Project, 2021) priporoča vključevanje varnostnih ukrepov na način, ki ne zmanjšuje uporabnosti sistema in ne spodbuja uporabnikov k nevarnemu vedenju.

Primer uspešnega povezovanja varnosti in uporabniške izkušnje predstavlja večfaktorska avtentikacija (MFA). Organizacija OWASP (Open Web Application Security Project, 2021) poudarja, da večfaktorska avtentikacija bistveno zmanjša tveganje nepooblaščenega dostopa do uporabniških računov, hkrati pa ob pravilni implementaciji nima večjega negativnega vpliva na uporabniško izkušnjo.

Podobno velja za uporabo varnih povezav HTTPS. Večina uporabnikov danes pričakuje, da spletna stran uporablja certifikat SSL/TLS. Prisotnost varnostne ključavnice v brskalniku povečuje občutek zaupanja in profesionalnosti spletnega mesta, kar pozitivno vpliva na uporabniško izkušnjo in zaznano verodostojnost spletne strani (Krug, 2014).

Po drugi strani lahko slabo zasnovani varnostni ukrepi povzročijo negativne posledice. Med pogoste primere sodijo:

- prezapletene zahteve za ustvarjanje gesel,
- prepogoste zahteve za ponovno prijavo,
- nejasna varnostna opozorila,
- predolgi obrazci za registracijo,
- otežena uporaba kontaktnih obrazcev.

Takšne rešitve lahko uporabnike odvrnejo od uporabe spletne strani ali jih celo spodbudijo k manj varnemu vedenju, na primer zapisovanju gesel na papir ali uporabi preprostih gesel.

Norman (2013) opozarja, da uporabniki pogosto iščejo najlažje poti do cilja, zato morajo biti sistemi zasnovani tako, da varno vedenje predstavljajo kot najpreprostejšo možnost.

Pomemben vidik povezave med varnostjo in uporabniško izkušnjo predstavlja tudi transparentnost. Uporabniki morajo razumeti, zakaj se določeni podatki zbirajo, kako se uporabljajo in kako so zaščiteni. Evropski parlament in Svet Evropske unije (2016) poudarjata pomen preglednosti pri obdelavi osebnih podatkov, saj jasna politika zasebnosti in razumljiva obvestila o uporabi piškotkov povečujejo zaupanje uporabnikov ter izboljšujejo njihovo izkušnjo.

Pri razvoju spletne strani je zato pomembno upoštevati načelo ravnovesja med varnostjo in uporabnostjo (Security and Usability Balance), ki poudarja iskanje ustreznega razmerja med zaščito sistema in uporabniško prijaznostjo. Cilj ni zgolj preprečevanje napadov, temveč tudi ustvarjanje okolja, v katerem se uporabniki počutijo varno in samozavestno ((Norman, 2013); (Krug, 2014)).

V okviru diplomskega dela bo to razmerje predstavljalo pomemben del analize spletne strani Andromа Collies, saj bo ocenjevano, kako obstoječe varnostne nastavitve vplivajo na uporabniško izkušnjo in kako je mogoče oboje izboljšati.

4 PREDSTAVITEV SPLETNE STRANI ANDROMA COLLIES

4.1 Opis in namen spletne strani (predstavitev psarne, cilji, ciljno občinstvo)

Spletna stran Andromа Collies predstavlja družinsko psarno dolgodlakih škotskih ovčarjev (Rough Collie), ki deluje pod vzrejno psarno Andromа. Namen spletne strani je predstavitev psarne, njenih psov, legel, dosežkov in drugih aktivnosti, povezanih z vzrejo pasme. Spletno mesto obiskovalcem omogoča dostop do informacij o pasmi, predstavitev posameznih psov, fotografij, novic in kontaktnih podatkov.

Psarna Andromа deluje že vrsto let in se aktivno ukvarja z vzrejo pasemskih psov ter sodeluje na domačih in mednarodnih kinoloških prireditvah. Spletna stran predstavlja pomemben komunikacijski kanal med lastniki psarne in obiskovalci, saj omogoča predstavitev vzrejnega programa ter vzpostavljanje stika s potencialnimi lastniki mladičev in drugimi ljubitelji pasme.

Glavni namen spletne strani je informiranje obiskovalcev o dejavnosti psarne in promocija vzreje dolgodlakih škotskih ovčarjev. Poleg tega omogoča pregled aktualnih legel, predstavitev vzrejnih psov in spremljanje novic, povezanih z delovanjem psarne.

Ciljno skupino spletne strani predstavljajo:

- potencialni kupci mladičev,
- lastniki in ljubitelji pasme Rough Collie,
- kinološki navdušenci,
- obiskovalci, ki iščejo informacije o pasmi,
- udeleženci kinoloških dogodkov in razstav.

Ker spletna stran deluje kot javno dostopna predstavitev organizacije, je pomembno, da zagotavlja zanesljivo delovanje, ustrezno raven varnosti in kakovostno uporabniško izkušnjo za vse obiskovalce.

4.2 Tehnološko ozadje strani (CMS, programski jeziki, strežnik)

Spletna stran Andromа Collies temelji na sistemu za upravljanje vsebin WordPress (CMS – Content Management System), ki omogoča enostavno urejanje in posodabljanje vsebine brez neposrednega poseganja v programsko kodo. Takšen pristop je posebej primeren za manjše

organizacije, saj poenostavi upravljanje spletnega mesta in zmanjšuje stroške vzdrževanja (WordPress Foundation, 2024).

Za prikaz vsebine se uporabljajo standardne spletne tehnologije:

- HTML (HyperText Markup Language),
- CSS (Cascading Style Sheets),
- JavaScript.

HTML skrbi za strukturo spletnih strani, CSS za vizualno oblikovanje in postavitev elementov, JavaScript pa omogoča interaktivne funkcionalnosti in dinamično delovanje določenih komponent.

Spletna stran je dostopna prek varne povezave HTTPS, kar pomeni, da se komunikacija med uporabnikom in spletnim strežnikom šifrira z uporabo certifikata SSL/TLS. Uporaba povezave HTTPS zmanjšuje tveganje prestrezanja podatkov, zagotavlja zaščito prenesenih informacij in povečuje zaupanje obiskovalcev v spletno mesto (Qualys SSL Labs, 2024).

Ker je spletna stran javno dostopna prek interneta, je njena varnost odvisna tudi od ustrezne konfiguracije spletnega strežnika, rednega posodabljanja sistema za upravljanje vsebin in uporabljenih vtičnikov ter implementacije dodatnih zaščitnih mehanizmov.

4.3 Struktura in funkcionalnosti (npr. galerija, kontaktni obrazec, predstavitev psov)

Spletna stran Andromа Collies uporablja klasično hierarhično strukturo navigacije, ki obiskovalcem omogoča preprost dostop do posameznih vsebinskih sklopov. Glavni navigacijski meni je dostopen na vrhu strani in vsebuje povezave do ključnih podstrani.

Med najpomembnejše funkcionalnosti spletne strani sodijo:

- **Predstavitev psarne**

Podstran »O nas« vsebuje predstavitev zgodovine psarne, njenih ciljev in dejavnosti. Obiskovalcem omogoča vpogled v ozadje delovanja psarne in njeno dolgoletno prisotnost na področju vzreje pasemskih psov.

- **Predstavitev psov**

Podstran »Naši psi« vsebuje informacije o posameznih psih, njihovih rodovnikih, dosežkih in fotografijah. Ta vsebina predstavlja enega izmed osrednjih elementov spletnega mesta.

- **Predstavitev mladičev in legel**

Spletna stran omogoča pregled aktualnih in preteklih legel ter informacij o mladičih. Potencialni kupci lahko pridobijo osnovne podatke o razpoložljivosti mladičev in načrtovanih leglih.

- **Galerija fotografij**

Galerija vsebuje fotografsko predstavitev psov in dejavnosti psarne. Vizualna vsebina pomembno prispeva k privlačnosti spletne strani in obiskovalcem omogoča boljši vpogled v življenje psarne.

- **Novice in obvestila**

Na spletni strani je na voljo tudi rubrika z novicami, kjer se objavljajo aktualne informacije, dogodki in pomembna obvestila. Takšna funkcionalnost omogoča redno posodabljanje vsebine in ohranjanje zanimanja obiskovalcev.

- **Kontaktni podatki**

Obiskovalcem so na voljo kontaktni podatki za vzpostavitev komunikacije z lastniki psarne. Kontaktna stran predstavlja pomembno povezavo med obiskovalci in upravljavci spletnega mesta.

Splošna struktura spletne strani je pregledna in logično organizirana, kar uporabnikom omogoča hitro iskanje informacij. V naslednjem poglavju bo podrobneje analizirano, kako učinkovito trenutna struktura podpira uporabniško izkušnjo ter ali vsebuje morebitne varnostne pomanjkljivosti.

5 ANALIZA OBSTOJEČEGA STANJA SPLETNE STRANI ANDROMA COLLIES

V praktičnem delu diplomskega dela je bila izvedena analiza spletne strani Andromа Collies z vidika kibernetske varnosti ter uporabniške izkušnje (UX) in uporabniškega vmesnika (UI). Namen analize je bil oceniti trenutno stanje spletne strani, prepoznati morebitne varnostne pomanjkljivosti ter ugotoviti možnosti za izboljšanje uporabniške izkušnje.

V okviru varnostne analize so bili pregledani implementacija protokola HTTPS in certifikata SSL/TLS, konfiguracija varnostnih headerjev HTTP, kontaktni obrazec ter morebitne ranljivosti spletne strani. Pri tem so bila uporabljena uveljavljena orodja za ocenjevanje varnosti spletnih aplikacij, kot so Mozilla Observatory, Qualys SSL Labs in Google Lighthouse ((Mozilla, 2024); (Qualys SSL Labs, 2024); (Google, 2024)).

Poleg tehničnega pregleda je bila izvedena tudi analiza uporabniške izkušnje, pri kateri so bili ocenjeni struktura spletnega mesta, navigacija, vizualna podoba, mobilna odzivnost in dostopnost. Analiza uporabniške izkušnje temelji na Nielsenovih heuristikah uporabnosti (Nielsen, 1994), dostopnost spletnega mesta pa je bila ocenjena glede na smernice WCAG 2.1 (W3C Web Accessibility Initiative, 2018).

Rezultati analize predstavljajo izhodišče za pripravo predlogov izboljšav, ki so predstavljeni v naslednjem poglavju diplomskega dela.

5.1 Varnostna analiza

Varnost spletnih aplikacij predstavlja enega ključnih dejavnikov za zagotavljanje zaščite uporabniških podatkov, zaupnosti komunikacije in zanesljivega delovanja sistema. Po priporočilih organizacije OWASP (2021) morajo spletne aplikacije zagotavljati ustrezno zaščito pred najpogostejšimi varnostnimi tveganji, saj lahko ranljivosti povzročijo nepooblaščen dostop do podatkov, motnje v delovanju sistema in zmanjšajo zaupanje uporabnikov.

Varnostna analiza spletne strani Andromа Collies je bila izvedena z uporabo orodij Mozilla Observatory in Qualys SSL Labs ter z ročnim pregledom delovanja spletnega mesta. Orodje

Mozilla Observatory omogoča ocenjevanje varnostne konfiguracije spletnih strani, predvsem z vidika implementacije varnostnih headerjev HTTP in drugih zaščitnih mehanizmov (Mozilla, 2024), medtem ko Qualys SSL Labs omogoča podrobno analizo konfiguracije SSL/TLS in pravilne implementacije povezave HTTPS (Qualys SSL Labs, 2024).

Poleg uporabe specializiranih orodij je bil opravljen tudi ročni pregled spletne strani, pri katerem so bili analizirani kontaktni obrazec, način prenosa podatkov, uporaba povezave HTTPS in prisotnost osnovnih varnostnih mehanizmov. Namen analize je bil ugotoviti morebitne pomanjkljivosti in oceniti stopnjo zaščite spletnega mesta pred najpogostejšimi spletnimi grožnjami.

5.1.1 Analiza HTTPS in certifikata SSL

Prvi korak varnostne analize je bil pregled implementacije protokola HTTPS in certifikata SSL/TLS. HTTPS omogoča šifrirano komunikacijo med uporabnikom in spletnim strežnikom ter preprečuje prestrezanje ali spreminjanje podatkov med prenosom. Uporaba povezave HTTPS predstavlja enega temeljnih varnostnih mehanizmov za zaščito spletnih aplikacij in uporabniških podatkov (Qualys SSL Labs, 2024).

Pregled je pokazal, da spletna stran uporablja veljaven certifikat SSL/TLS, ki omogoča vzpostavitev varne povezave. Ob dostopu prek protokola HTTP se uporabnik samodejno preusmeri na različico HTTPS, s čimer je zagotovljena uporaba šifrirane komunikacije pri vseh obiskih spletnega mesta.

Kljub pravilni implementaciji analiza HTTPS ni pokazala uporabe mehanizma HTTP Strict Transport Security (HSTS). Po priporočilih organizacije OWASP (2021) HSTS brskalniku naroči, da za dostop do spletnega mesta vedno uporablja povezavo HTTPS, s čimer zmanjšuje možnost napadov, pri katerih bi lahko napadalec uporabnika preusmeril na nezaščiteno različico spletne strani. Odsotnost tega mehanizma zato predstavlja dodatno varnostno tveganje, predvsem ob prvem obisku spletnega mesta.

Na podlagi ugotovitev je mogoče zaključiti, da je osnovna zaščita komunikacije ustrezno implementirana, vendar bi uvedba HSTS dodatno povečala varnost spletnega mesta ter

izboljšala njegovo odpornost proti napadom, povezanim z nešifrirano komunikacijo (Open Web Application Security Project, 2021).

5.1.2 Pregled varnostnih headerjev

Varnostni headerji HTTP predstavljajo pomemben zaščitni mehanizem, ki zmanjšuje možnost uspešnih napadov na spletne aplikacije. Njihov namen je omejiti potencialno nevarno vedenje spletnih brskalnikov in zmanjšati možnost izkoriščanja znanih spletnih ranljivosti (Mozilla, 2024). Za pregled implementacije varnostnih headerjev je bilo uporabljeno orodje Mozilla Observatory, ki ocenjuje varnostno konfiguracijo spletnih strežnikov in uporabo priporočljivih zaščitnih mehanizmov (Mozilla, 2024).

Rezultat analize je pokazal skupno oceno D (30/100 točk), kar nakazuje na več pomanjkljivosti v konfiguraciji spletnega strežnika.



Slika 1: Mozilla Observatory Report

Vir: Lasten zajem zaslona (2026)

Analiza je pokazala naslednje stanje implementacije varnostnih headerjev:

Tabela 2: Rezultat analize varnostnih headerjev z orodjem Mozilla Observatory

Varnostni header	**Status**
Content-Security-Policy	Ni implementiran
Strict-Transport-Security	Ni implementiran

X-Content-Type-Options	Ni implementiran
X-Frame-Options	Ni implementiran
Referrer-Policy	Ni implementiran
HTTPS Redirect	Implementiran
CORS Policy	Ustrezno konfiguriran

Vir: Mozilla Observatory (2024), lastna izdelava na podlagi rezultatov analize

Največjo varnostno pomanjkljivost predstavlja odsotnost politike Content Security Policy (CSP), ki omogoča določanje dovoljenih virov za nalaganje skript, slik in drugih vsebin. Po priporočilih organizacije OWASP predstavlja CSP enega najpomembnejših zaščitnih mehanizmov pred napadi vrste Cross-Site Scripting (XSS), saj omejuje izvajanje nepooblaščene skriptne kode v brskalniku uporabnika ((OWASP Foundation, 2024); (World Wide Web Consortium, 2024)).

Prav tako ni implementiran header X-Frame-Options, ki preprečuje prikaz spletne strani znotraj elementa *iframe* na drugih spletnih mestih. Odsotnost tega mehanizma povečuje možnost izvedbe napadov vrste *clickjacking*, pri katerih lahko napadalec uporabnika zavede k izvajanju neželenih dejanj (Mozilla, 2024).

Header X-Content-Type-Options preprečuje napačno interpretacijo tipov datotek v spletnih brskalnikih. Ker ta header ni nastavljen, lahko posamezni brskalniki vsebino interpretirajo drugače od predvidenega, kar povečuje možnost izvajanja zlonamerne vsebine (Mozilla, 2024).

Prav tako ni implementiran header Referrer-Policy, ki določa, katere informacije o uporabnikovem obisku spletnega mesta se posredujejo zunanjim spletnim stranem. Njegova odsotnost lahko povzroči nepotrebno razkrivanje informacij in zmanjšuje raven zasebnosti uporabnikov (Mozilla, 2024).

Na podlagi rezultatov analize je mogoče zaključiti, da največjo pomanjkljivost spletne strani predstavljajo neimplementirani varnostni headerji HTTP. Implementacija mehanizmov CSP, HSTS, X-Frame-Options, X-Content-Type-Options in Referrer-Policy bi bistveno povečala odpornost spletne strani proti najpogostejšim spletnim napadom in pomembno izboljšala njeno skupno varnostno oceno.

5.1.3 Analiza obrazcev in obdelave podatkov

Spletna stran Andromа Collies vsebuje kontaktni obrazec, prek katerega lahko obiskovalci vzpostavijo stik z lastnikom spletne strani. Ker kontaktni obrazci predstavljajo eno najpogostejših vstopnih točk za napade na spletne aplikacije, je njihova ustrezna zaščita pomemben del varnega razvoja spletnih sistemov (Open Web Application Security Project, 2021).

V okviru analize so bili pregledani način prenosa podatkov, osnovna validacija uporabniških vnosov in prisotnost zaščitnih mehanizmov, ki zmanjšujejo možnost zlorabe obrazca. Ker je obrazec dostopen prek povezave HTTPS, se vsi podatki med uporabnikom in strežnikom prenašajo šifrirano. Takšen način prenosa zmanjšuje možnost prestrezanja ali spreminjanja podatkov med komunikacijo ter predstavlja osnovni varnostni mehanizem za zaščito osebnih podatkov uporabnikov (Qualys SSL Labs, 2024).

Vizualni pregled obrazca je pokazal uporabo osnovne validacije uporabniških vnosov. Obvezna polja so jasno označena, kar zmanjšuje možnost pošiljanja nepopolnih podatkov. OWASP Foundation (2024) poudarja, da je validacija vhodnih podatkov eden ključnih ukrepov za preprečevanje napadov, kot so SQL Injection, Cross-Site Scripting (XSS) in druge oblike vbrizgavanja zlonamerne kode.

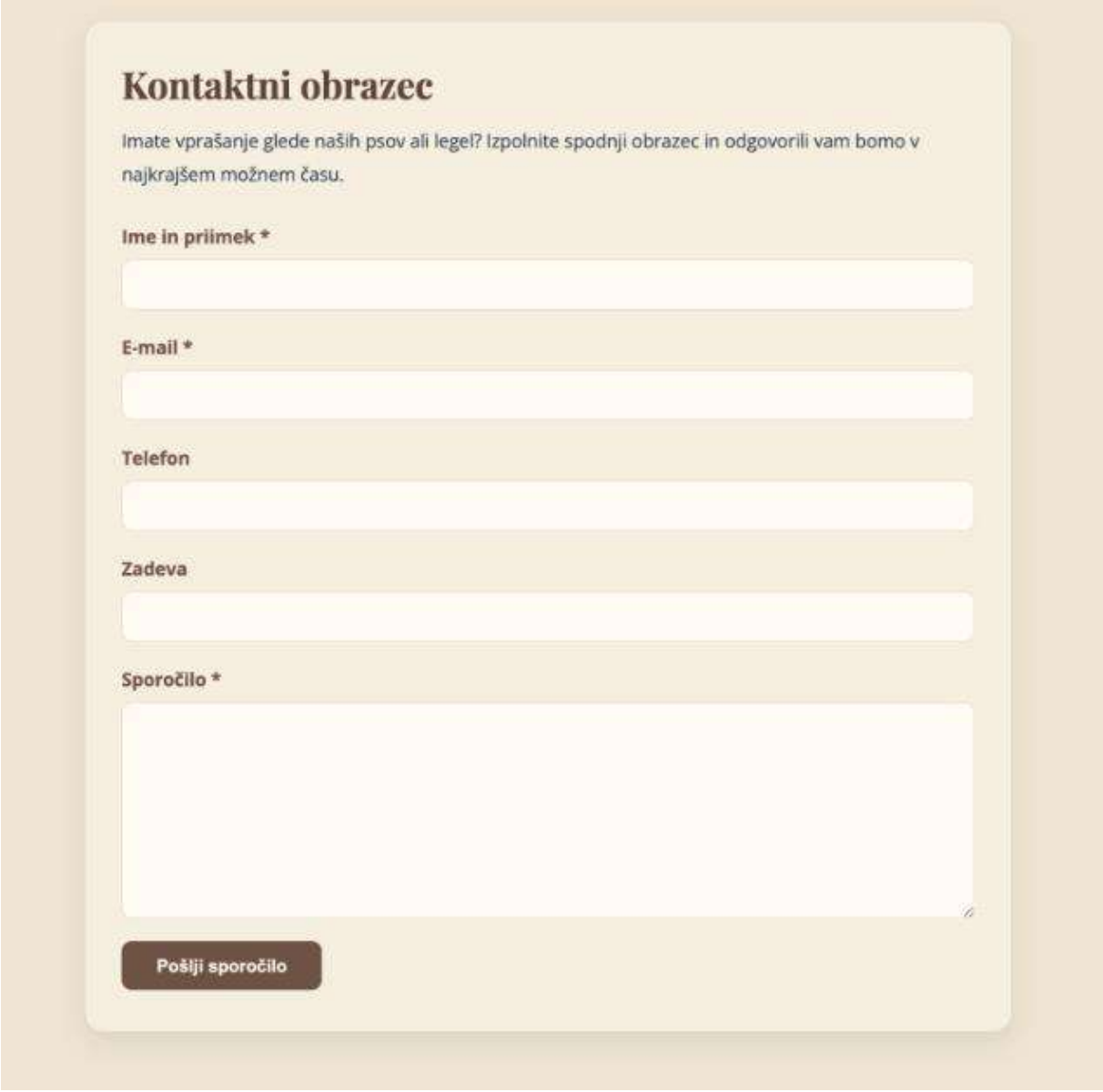
Kljub temu iz javno dostopnih informacij ni bilo mogoče potrditi uporabe naprednejših zaščitnih mehanizmov, kot so:

- zaščita pred napadi Cross-Site Request Forgery (CSRF),
- strežniška validacija vhodnih podatkov,
- zaščita pred avtomatiziranim pošiljanjem obrazcev (CAPTCHA),
- filtriranje potencialno zlonamernih uporabniških vnosov.

OWASP Foundation (2024) priporoča uporabo žetonov CSRF, strežniške validacije vhodnih podatkov in dodatnih zaščitnih mehanizmov, ki zmanjšujejo možnost zlorabe spletnih obrazcev. Prav tako je priporočljiva uporaba sistemov CAPTCHA oziroma podobnih rešitev za omejevanje avtomatiziranih poizvedb in neželene pošte.

Ker delovanje strežniške strani in izvorna koda aplikacije nista javno dostopna, navedenih zaščitnih mehanizmov ni bilo mogoče dokončno preveriti. Ugotovitve zato temeljijo na analizi

javno dostopnega dela spletne strani in ne omogočajo dokončne ocene varnosti aplikacijske logike. Za celovito oceno stopnje zaščite kontaktnega obrazca bi bilo potrebno dodatno testiranje z dostopom do strežniške implementacije.



Slika 2: Kontaktni obrazec na spletni strani

Vir: Lasten zajem zaslona (2026)

5.1.4 Testiranje in ranljivosti (OWASP ZAP, Mozilla Observatory, Lighthouse)

Za pridobitev objektivne ocene varnostnega stanja spletne strani Andromа Collies je bilo izvedeno testiranje z uporabo specializiranih orodij za analizo spletnih aplikacij. Namen

testiranja je bil preveriti konfiguracijo spletnega strežnika, oceniti implementacijo varnostnih mehanizmov in identificirati morebitne ranljivosti. Uporaba avtomatiziranih orodij je pomemben del sodobnega varnostnega testiranja, saj omogoča učinkovito odkrivanje pomanjkljivosti in napačnih konfiguracij spletnih sistemov (Open Web Application Security Project, 2021).

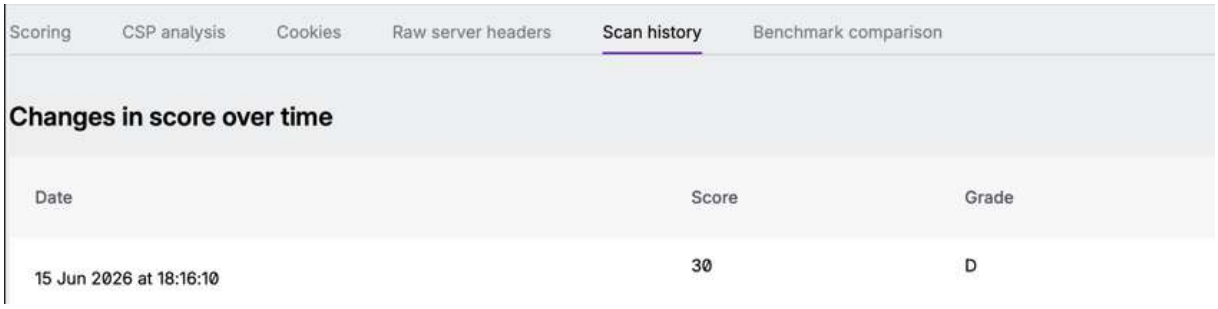
Pri analizi so bila uporabljena naslednja orodja:

- Mozilla Observatory,
- Google Lighthouse,
- ročni pregled spletne strani,
- analiza HTTP odzivnih headerjev.

Rezultati posameznih analiz so predstavljeni v nadaljevanju.

- **Testiranje z Mozilla Observatory**

Rezultati testiranja z orodjem Mozilla Observatory potrjujejo ugotovitve iz poglavja **5.1.2**, kjer je bila podrobno predstavljena analiza varnostnih headerjev HTTP. Dosežena ocena **D (30/100 točk)** kaže predvsem na pomanjkljivo implementacijo sodobnih varnostnih mehanizmov na ravni spletnega strežnika.



Slika 3: Mozilla Observatory rezultat

Vir: Lasten zajem zaslona (2026)

Najpomembnejše ugotovljene pomanjkljivosti so:

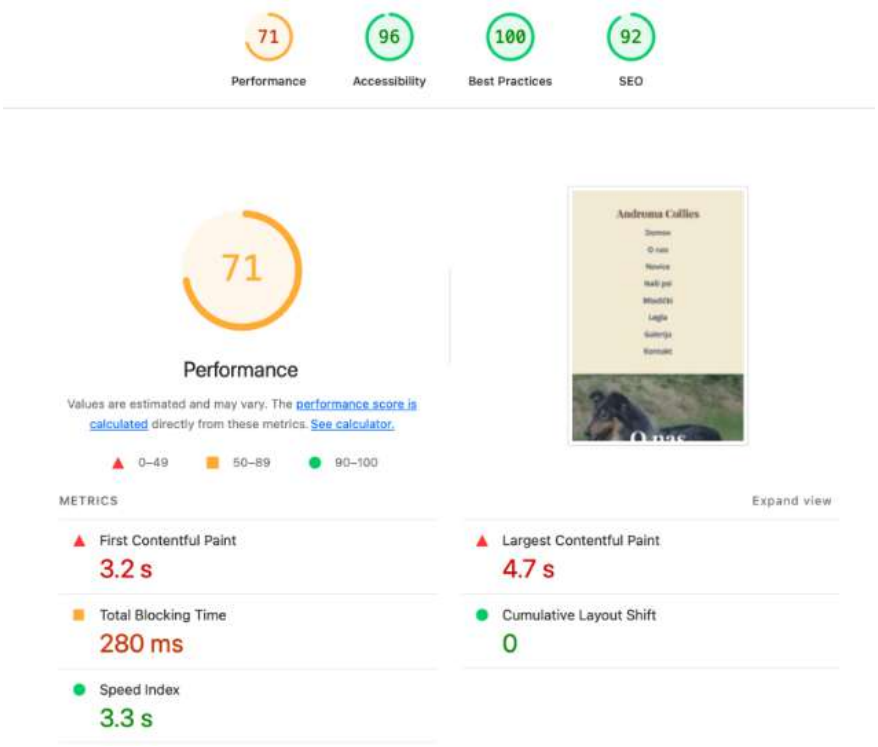
- manjkajoča politika Content Security Policy (CSP),
- odsotnost HTTP Strict Transport Security (HSTS),
- odsotnost X-Frame-Options,
- odsotnost X-Content-Type-Options,

- odsotnost Referrer-Policy.

Rezultati potrjujejo, da največje varnostne pomanjkljivosti ne izhajajo iz funkcionalnosti spletne strani, temveč predvsem iz konfiguracije spletnega strežnika in neimplementiranih zaščitnih mehanizmov.

➢ Analiza strežniškega okolja

V okviru testiranja je bila izvedena tudi analiza strežniškega okolja.



Slika 4: Pregled strežniškega okolja spletne strani z Lighthouse

Vir: Lasten zajem zaslona (2026)

Pregled je pokazal uporabo spletnega strežnika **LiteSpeed**, aktualne različice programskega jezika **PHP** in podporo sodobnemu komunikacijskemu protokolu **HTTP/3**. Redno posodabljanje strežniške programske opreme predstavlja pomemben varnostni ukrep, saj zmanjšuje možnost izkoriščanja znanih ranljivosti zastarelih različic sistemske programske opreme (WordPress Foundation, 2024).

Podpora protokolu HTTP/3 poleg izboljšane varnosti omogoča tudi učinkovitejši prenos podatkov, kar pozitivno vpliva na zmogljivost spletne strani in uporabniško izkušnjo.

➢ Ocena potencialnih tveganj OWASP

Na podlagi izvedenega pregleda je bila ocenjena izpostavljenost spletne strani posameznim kategorijam OWASP Top 10.

Tabela 3: Ocena potencialnih izpostavljenosti OWASP tveganj

OWASP kategorija	**Ocena tveganja**
Broken Access Control	Nizko
Cryptographic Failures	Nizko
Injection	Srednje
Insecure Design	Nizko
Security Misconfiguration	Visoko
Vulnerable Components	Nizko
Authentication Failures	Nizko
Software Integrity Failures	Srednje
Logging and Monitoring Failures	Ni mogoče oceniti
SSRF	Nizko

Vir: Lastna izdelava na podlagi rezultatov analize

Največje tveganje predstavlja kategorija **Security Misconfiguration**, saj analiza jasno kaže na pomanjkljivo implementacijo priporočenih varnostnih nastavitev spletnega strežnika. Organizacija OWASP (2021) napačno konfiguracijo sistemov uvršča med najpogostejše vzroke varnostnih incidentov pri spletnih aplikacijah.

Srednja stopnja tveganja je bila ugotovljena tudi pri kategoriji **Injection**, saj brez dostopa do strežniške kode ni mogoče zanesljivo izključiti možnosti prisotnosti ranljivosti SQL Injection ali Cross-Site Scripting (XSS). Ta ocena temelji na omejitvah izvedene analize in ne predstavlja potrjene prisotnosti omenjenih ranljivosti.

- **Ocena splošne stopnje varnosti**

Na podlagi vseh izvedenih testov je bila pripravljena skupna ocena posameznih varnostnih področij.

Tabela 4: Skupna ocena varnosti spletne strani

Področje	**Ocena (1–5)**
zaščita HTTPS	5
konfiguracija SSL/TLS	4
Varnostni headerji	2
Zaščita obrazcev	3
Konfiguracija strežnika	3
Odpornost proti pogostim napadom	3

Vir: Lastna izdelava

Povprečna ocena znaša **3,3 od 5**, kar pomeni, da spletna stran zagotavlja zadovoljivo osnovno raven varnosti. Kljub temu analiza kaže na več področij, kjer bi bilo mogoče z razmeroma enostavnimi konfiguracijskimi spremembami doseči občutno višjo raven zaščite.

- **Interpretacija rezultatov**

Rezultati testiranja kažejo, da spletna stran Andromа Collies ni neposredno izpostavljena kritičnim ranljivostim, ki bi omogočale takojšen prevzem sistema ali krajo podatkov. Največje pomanjkljivosti so povezane z nepopolno konfiguracijo varnostnih mehanizmov spletnega strežnika, predvsem z odsotnostjo več pomembnih varnostnih headerjev HTTP.

Čeprav ugotovljene pomanjkljivosti same po sebi ne pomenijo neposredne ogroženosti sistema, zmanjšujejo njegovo odpornost proti sodobnim spletnim napadom in posledično vplivajo na skupno raven varnosti spletne strani.

- **Sklep testiranja ranljivosti**

Izvedeno testiranje je pokazalo, da spletna stran Andromа Collies zagotavlja ustrezno osnovno raven zaščite predvsem zaradi uporabe povezave HTTPS, veljavnega certifikata SSL/TLS in sodobnega strežniškega okolja. Največ možnosti za izboljšave se kaže na področju konfiguracije spletnega strežnika in implementacije dodatnih zaščitnih mehanizmov.

Med najpomembnejšimi priporočili so uvedba politike **Content Security Policy (CSP)**, implementacija **HTTP Strict Transport Security (HSTS)**, dodajanje manjkajočih varnostnih headerjev HTTP in dodatna zaščita kontaktnega obrazca pred avtomatiziranimi napadi.

Ugotovitve predstavljajo izhodišče za pripravo varnostnih izboljšav, ki so podrobneje predstavljene v naslednjem poglavju diplomskega dela.

5.2 Analiza UX/UI

Uporabniška izkušnja (UX) in uporabniški vmesnik (UI) pomembno vplivata na kakovost in uspešnost spletne strani. Dobro zasnovana spletna stran uporabnikom omogoča hitro iskanje informacij, intuitivno navigacijo, učinkovito uporabo funkcionalnosti in prijetno uporabniško izkušnjo. Norman (2013) in Krug (2014) poudarjata, da sta uporabnost in razumljivost uporabniškega vmesnika med najpomembnejšimi dejavniki zadovoljstva uporabnikov pri uporabi spletnih storitev.

V okviru analize uporabniške izkušnje spletne strani Androma Collies so bili ocenjeni struktura in navigacija spletnega mesta, vizualno oblikovanje, mobilna odzivnost, hitrost nalaganja ter dostopnost spletnih vsebin. Pri ocenjevanju uporabnosti je bila uporabljena metoda heuristične evalvacije na podlagi Nielsenovih heuristik uporabnosti (Nielsen, 1994), medtem ko je bila dostopnost ocenjena glede na smernice WCAG 2.1 (W3C Web Accessibility Initiative, 2018).

Namen analize je bil ugotoviti, kako učinkovito spletna stran podpira potrebe uporabnikov, ter prepoznati področja, kjer bi bilo mogoče z oblikovalskimi in tehničnimi izboljšavami dodatno izboljšati uporabniško izkušnjo. Rezultati posameznih analiz so predstavljeni v naslednjih podpoglavjih.

5.2.1 Struktura in navigacija

Pri ocenjevanju strukture in navigacije spletne strani je bila uporabljena metoda heuristične evalvacije na podlagi Nielsenovih načel uporabnosti. Nielsen (1994) poudarja, da mora biti navigacija zasnovana tako, da uporabnikom omogoča hitro orientacijo, preprosto iskanje informacij in učinkovito doseganje njihovih ciljev.

Analiza je pokazala, da spletna stran uporablja pregledno hierarhično strukturo, ki obiskovalcem omogoča hitro orientacijo in dostop do ključnih informacij. Glavni navigacijski meni vsebuje jasno poimenovane kategorije, ki uporabnikom omogočajo intuitivno premikanje

med posameznimi vsebinskimi sklopi. Informacije o psarni, psih, leglih, galeriji in kontaktih so logično organizirane in ne zahtevajo dodatnega iskanja.

Takšna organizacija vsebine je skladna z Nielsenovo **heuristiko** skladnosti in standardov ter načelom prepoznavanja namesto pomnjenja, saj uporabnikom omogoča hitro razumevanje strukture spletnega mesta (Nielsen, 1994).

Tabela 5: Ocena strukture in navigacije na podlagi Nielsenovih heuristik

Kriterij	Ocena (1–5)	Komentar
Preglednost menija	5	Jasno strukturiran meni
Logična razporeditev vsebine	5	Vsebina je smiselno organizirana
Dostopnost informacij	4	Večina informacij je hitro dostopnih
Označevanje aktivne strani	3	Možne izboljšave vizualne označitve
Iskalna funkcionalnost	2	Iskalnik ni implementiran

Vir: Lastna izdelava

Analiza je pokazala, da je hierarhija informacij dosledna in pregledna skozi celotno spletno stran. Krug (2014) poudarja, da morajo uporabniki že ob prvem obisku hitro razumeti organizacijo spletnega mesta in brez dodatnega razmišljanja poiskati želene informacije. Na analizirani spletni strani so ključne vsebine jasno razporejene, kar zmanjšuje možnost zmede in pozitivno vpliva na uporabniško izkušnjo.

Povprečna ocena navigacije znaša **3,8 od 5**, kar kaže na dobro uporabnost spletne strani. Kljub pozitivni oceni analiza kaže tudi na možnosti za nadaljnje izboljšave, predvsem pri izrazitejši vizualni označitvi trenutno aktivne strani in nadaljnji optimizaciji navigacije na mobilnih napravah. Omenjene izboljšave bi uporabnikom omogočile še hitrejšo orientacijo in dodatno izboljšale uporabniško izkušnjo.

5.2.2 Vizualni dizajn in barvna shema

Vizualna podoba spletne strani pomembno vpliva na prvi vtis uporabnika in njegovo zaznavanje profesionalnosti organizacije. Norman (2013) poudarja, da uporabniki pogosto oblikujejo začetno mnenje o digitalnem izdelku že na podlagi njegovega videza, še preden začnejo uporabljati njegove funkcionalnosti. Vizualni elementi zato pomembno vplivajo na zaupanje uporabnikov in kakovost celotne uporabniške izkušnje.

Analiza je pokazala, da spletna stran Androma Collies uporablja enoten vizualni slog, ki je usklajen z dejavnostjo psarne in njeno ciljno skupino. Fotografije psov predstavljajo osrednji element uporabniškega vmesnika in učinkovito dopolnjujejo predstavitev vsebine.



Slika 5: Vizualni dizajn spletne strani

Vir: Lasten zajem zaslona (2026)

- **Uporaba fotografij**

Fotografije predstavljajo eno največjih prednosti spletne strani. Analiza je pokazala, da so uporabljene slike kakovostne, profesionalno posnete, vsebinsko ustrezne in smiselno vključene v posamezne vsebinske sklope. Ker gre za predstavitveno spletno stran psarne, fotografije pomembno prispevajo k ustvarjanju zaupanja obiskovalcev in predstavljajo pomemben element predstavitve kakovosti vzreje.

Shneiderman idr. (2017) poudarjajo, da ustrezna uporaba vizualnih elementov izboljšuje razumevanje vsebine ter prispeva k prijetnejši in privlačnejši uporabniški izkušnji.

- **Barvna shema**

Barvna paleta spletne strani deluje umirjeno, pregledno in profesionalno ter učinkovito podpira predstavitev vsebine. Uporabljene barve ne odvračajo pozornosti od informacij, temveč omogočajo njihovo jasno izpostavitev. Shneiderman idr. (2017) navajajo, da mora izbira barv uporabnikom olajšati prepoznavanje pomembnih informacij in prispevati k večji preglednosti uporabniškega vmesnika.

Pri analizi so bile ugotovljene naslednje prednosti:

- dobra berljivost besedila,
- ustrezna kontrastna razmerja,
- enotna uporaba barv na vseh podstraneh,
- profesionalen in skladen vizualni videz.

➢ **Tipografija**

Uporabljena pisava je dovolj velika in dobro berljiva na namiznih ter mobilnih napravah. Naslovi jasno ločujejo posamezne vsebinske sklope in uporabnikom omogočajo hitro pregledovanje vsebine.



Slika 6: Tipografija domače strani

Vir: Lasten zajem zaslona (2026)

Na podlagi analize je mogoče zaključiti, da vizualni dizajn učinkovito podpira namen spletne strani in pozitivno vpliva na uporabniško izkušnjo. Enotna vizualna podoba, kakovostne fotografije ter pregledna tipografija prispevajo k profesionalnemu videzu spletnega mesta in povečujejo zaupanje obiskovalcev.

5.2.3 Mobilna odzivnost in hitrost nalaganja

Mobilna odzivnost predstavlja pomemben dejavnik uporabniške izkušnje, saj vse več uporabnikov dostopa do spletnih vsebin prek mobilnih naprav. Smernice W3C poudarjajo, da mora biti sodobna spletna stran prilagojena različnim velikostim zaslonov in omogočati primerljivo uporabniško izkušnjo ne glede na uporabljeno napravo (W3C Web Accessibility Initiative, 2018).

Pri pregledu spletne strani na različnih velikostih zaslonov je bilo ugotovljeno, da se postavitev elementov ustrezno prilagaja napravi uporabnika in ohranja dobro preglednost vsebine.

- **Mobilna prilagoditev**

Analiza je pokazala več pozitivnih značilnosti mobilne različice spletne strani:

- pravilno prilagajanje širine vsebine,
- samodejno prilagajanje fotografij,
- dobra berljivost besedila,
- pregledna in funkcionalna navigacija.

Spletno stran je mogoče uporabljati brez horizontalnega drsenja, kar predstavlja enega od pomembnejših kriterijev kakovostne mobilne odzivnosti.

- **Hitrost nalaganja**

Hitrost nalaganja pomembno vpliva na zadovoljstvo uporabnikov, uporabniško izkušnjo in optimizacijo spletne strani za iskalnike. Analiza je pokazala, da spletna stran deluje zadovoljivo, vendar zaradi večjega števila fotografij visoke ločljivosti obstajajo možnosti za dodatno optimizacijo.

Rezultati analize z orodjem Google Lighthouse kažejo, da bi bilo mogoče zmogljivost spletne strani dodatno izboljšati predvsem z optimizacijo večpredstavnostnih datotek in zmanjšanjem količine prenesenih podatkov.

Med priporočene izboljšave sodijo:

- pretvorba slik v format WebP,
- uporaba tehnike Lazy Loading,

- optimizacija datotek CSS,
- zmanjšanje velikosti datotek JavaScript.

Navedeni ukrepi sodijo med priporočene tehnike optimizacije zmogljivosti spletnih strani ter lahko prispevajo k hitrejšemu nalaganju vsebine in manjši porabi pasovne širine (Google, 2024).

- **Vpliv na uporabniško izkušnjo**

Počasnejše nalaganje spletnih strani lahko negativno vpliva na uporabniško izkušnjo, saj pogosto povzroči večjo stopnjo zapustitve strani, manjše zadovoljstvo uporabnikov in slabšo uvrstitev v spletnih iskalnikih.

Čeprav analizirana spletna stran že zagotavlja zadovoljivo uporabniško izkušnjo, bi optimizacija slik in drugih večjih datotek prispevala k hitrejšemu nalaganju strani ter še izboljšala njeno uporabnost na različnih napravah.

5.2.4 Dostopnost in berljivost vsebine

Dostopnost spletnih vsebin je bila ocenjena na podlagi smernic WCAG 2.1, katerih namen je zagotoviti uporabo spletnih strani tudi uporabnikom s posebnimi potrebami ter omogočiti enakovreden dostop do informacij ne glede na posameznikove sposobnosti ali uporabljeno tehnologijo (W3C Web Accessibility Initiative, 2018). Pri analizi so bili ocenjeni berljivost besedila, dostopnost slik in osnovni elementi navigacije.

- **Berljivost**

Analiza je pokazala, da je besedilo na spletni strani jasno strukturirano, razdeljeno na smiselne odstavke in podprto z ustreznimi vizualnimi elementi. Kontrast med besedilom in ozadjem zagotavlja dobro berljivost, kar uporabnikom omogoča hitro pregledovanje vsebine ter zmanjšuje njihovo kognitivno obremenitev.

Takšna organizacija vsebine je skladna s priporočili smernic WCAG 2.1, ki poudarjajo pomen preglednosti, razumljivosti in enostavne uporabe spletnih vsebin (W3C Web Accessibility Initiative, 2018).

- **Dostopnost slik**

Ker spletna stran vsebuje veliko fotografij, imajo alternativni opisi slik (ALT opisi) pomembno vlogo pri zagotavljanju dostopnosti. ALT opisi uporabnikom bralnikov zaslona omogočajo razumevanje vsebine slik in predstavljajo eno izmed osnovnih zahtev smernic WCAG 2.1 (W3C Web Accessibility Initiative, 2018).

Pri pregledu ni bilo mogoče potrditi prisotnosti alternativnih opisov za vse slike, zato obstaja možnost izboljšav na tem področju. Dodajanje opisnih ALT oznak bi izboljšalo dostopnost spletne strani predvsem za uporabnike, ki uporabljajo pomožne tehnologije.

- **Navigacija s tipkovnico**

Za popolno skladnost s smernicami WCAG mora biti spletna stran dostopna tudi uporabnikom, ki za navigacijo uporabljajo izključno tipkovnico. Takšen način uporabe je pomemben predvsem za osebe z motoričnimi oviranostmi ali uporabnike različnih podpornih tehnologij.

Ker analiza temelji na javno dostopnem pregledu spletne strani, vseh scenarijev uporabe s tipkovnico ni bilo mogoče v celoti preveriti. Za natančnejšo oceno skladnosti s smernicami WCAG bi bilo priporočljivo izvesti dodatno testiranje z uporabo pomožnih tehnologij in različnih načinov navigacije.

- **Sklep ocene dostopnosti**

Na podlagi izvedene analize je mogoče zaključiti, da spletna stran Androma Collies zagotavlja zadovoljivo osnovno raven dostopnosti in berljivosti vsebine. Prednosti predstavljajo pregledna struktura besedila, ustrezna kontrastna razmerja in logična organizacija informacij, ki uporabnikom omogočajo enostavno uporabo spletnega mesta.

Največ možnosti za izboljšave se kaže na področju dosledne uporabe alternativnih opisov slik, preverjanja dostopnosti s pomočjo tipkovnice in dodatnega testiranja skladnosti s smernicami WCAG 2.1 z uporabo pomožnih tehnologij. Ugotovitve predstavljajo izhodišče za izboljšave dostopnosti, ki so predstavljene v naslednjem poglavju diplomskega dela.

6 PREDLAGANE IZBOLJŠAVE

Na podlagi ugotovitev analize, predstavljene v petem poglavju, je bilo ugotovljeno, da spletna stran Androma Collies zagotavlja zadovoljivo osnovno raven varnosti in dobro uporabniško izkušnjo. Kljub temu analiza razkriva več področij, na katerih je mogoče izboljšati tako varnostno konfiguracijo spletnega mesta kot uporabniško izkušnjo obiskovalcev.

Predlagane izboljšave temeljijo na priporočilih organizacije OWASP, smernicah WCAG 2.1, dobrih praksah razvoja spletnih aplikacij ter rezultatih izvedene analize. Njihov namen je povečati odpornost spletne strani proti sodobnim spletnim grožnjam, izboljšati zaščito osebnih podatkov uporabnikov in hkrati ohraniti oziroma izboljšati uporabniško izkušnjo ((Open Web Application Security Project, 2021); (W3C Web Accessibility Initiative, 2018)).

Pri pripravi predlogov je bila posebna pozornost namenjena ravnovesju med varnostjo in uporabnostjo. Norman (2013) poudarja, da morajo biti digitalni sistemi zasnovani tako, da uporabnikom omogočajo učinkovito in intuitivno uporabo, hkrati pa zmanjšujejo možnost napak in varnostnih tveganj. Neustrezno implementirani varnostni mehanizmi lahko negativno vplivajo na uporabniško izkušnjo, na primer z oteženim dostopom do vsebine ali nepravilnim delovanjem posameznih funkcionalnosti (Krug, 2014).

Cilj predlaganih izboljšav zato ni zgolj povečanje stopnje zaščite spletnega mesta, temveč tudi zagotavljanje pregledne, zanesljive in uporabniku prijazne spletne strani. Predlagane rešitve sledijo načelu ravnovesja med varnostjo in uporabnostjo (*Security and Usability Balance*), ki ga sodobne smernice razvoja spletnih aplikacij prepoznavajo kot enega ključnih dejavnikov kakovostnih spletnih storitev (Open Web Application Security Project, 2021).

6.1 Varnostne izboljšave

Analiza, predstavljena v poglavju 5.1, je pokazala, da največje varnostne pomanjkljivosti spletne strani izhajajo predvsem iz konfiguracije spletnega strežnika ter odsotnosti določenih zaščitnih mehanizmov, ki jih priporočajo sodobni standardi kibernetske varnosti. Čeprav spletna stran uporablja povezavo HTTPS in ne vsebuje očitnih kritičnih ranljivosti, obstaja več možnosti za dodatno izboljšanje njene odpornosti proti najpogostejšim spletnim napadom.

6.1.1 Vpeljava varnostnih headerjev (CSP, HSTS, X-Frame-Options …)

Rezultati analize z orodjem Mozilla Observatory so pokazali, da spletna stran ne uporablja več pomembnih varnostnih headerjev HTTP. Ti predstavljajo dodatno plast zaščite med spletnim strežnikom in uporabnikovim brskalnikom ter pomembno zmanjšujejo možnost uspešnega izkoriščanja različnih spletnih ranljivosti (Mozilla, 2024). Njihova implementacija predstavlja eno izmed najučinkovitejših in hkrati stroškovno najmanj zahtevnih izboljšav varnosti spletnega mesta.

- **Implementacija Content Security Policy (CSP)**

Ugotovljena pomanjkljivost

Analiza je pokazala, da spletna stran ne uporablja politike Content Security Policy (CSP). Zaradi tega brskalnik nima omejitev glede izvajanja skript iz zunanjih virov, kar povečuje tveganje za napade vrste Cross-Site Scripting (XSS). Po priporočilih organizacije OWASP predstavlja CSP enega najpomembnejših zaščitnih mehanizmov za zmanjševanje tveganja tovrstnih napadov ((OWASP Foundation, 2024); (World Wide Web Consortium, 2024)).

Predlagana rešitev

Predlagana je implementacija politike CSP, ki omejuje nalaganje vsebin iz zaupanja vrednih virov in preprečuje izvajanje potencialno zlonamerne kode. Brskalnik tako zavrne izvajanje vsebin iz nepooblaščenih virov, tudi če bi napadalcu uspelo vnesti zlonamerno skripto v spletno stran.

Način implementacije

Ker spletna stran uporablja spletni strežnik LiteSpeed, je CSP mogoče implementirati z nastavitvijo headerja HTTP v konfiguraciji strežnika oziroma datoteki *.htaccess*. Zaradi uporabe sistema WordPress in različnih večpredstavnostnih elementov sta priporočljiva postopno uvajanje politike in sprotno preverjanje delovanja spletne strani.

Primer konfiguracije

<IfModule LiteSpeed>
Header set Content-Security-Policy "default-src 'self'; img-src 'self' data:; script-src 'self'; style-src 'self' 'unsafe-inline';"
</IfModule>

Pričakovani učinki

Implementacija CSP pomembno zmanjša možnost uspešnega izvajanja zlonamerne kode JavaScript, izboljša varnostno oceno spletnega mesta in poveča skladnost s priporočili organizacije OWASP. Pri uvajanju je priporočljivo postopno testiranje, saj lahko preveč restriktivna politika vpliva na pravilno delovanje posameznih funkcionalnosti.

- **Implementacija HTTP Strict Transport Security (HSTS)**

Ugotovljena pomanjkljivost

Čeprav spletna stran uporablja povezavo HTTPS, analiza ni pokazala implementacije mehanizma HTTP Strict Transport Security (HSTS). Posledično je uporabnik ob prvem obisku še vedno lahko izpostavljen napadom vrste SSL Stripping.

Predlagana rešitev

Predlagana je implementacija HSTS, ki brskalniku naroči, da mora spletno mesto vedno obiskovati prek povezave HTTPS.

Način implementacije

HSTS se implementira na ravni spletnega strežnika in ne zahteva sprememb programske kode spletne strani, zato predstavlja enostavno in učinkovito izboljšavo varnosti.

Primer konfiguracije

<IfModule LiteSpeed>
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
</IfModule>

Pričakovani učinki

Implementacija HSTS izboljša zaščito povezave HTTPS, zmanjša možnost prestrezanja komunikacije in poveča zaupanje uporabnikov. Pred uvedbo je treba preveriti pravilno delovanje povezave HTTPS, saj lahko napačna konfiguracija povzroči težave pri dostopu do spletnega mesta.

- **Implementacija X-Frame-Options**

Ugotovljena pomanjkljivost

Analiza je pokazala odsotnost zaščite pred prikazovanjem spletne strani znotraj elementov *iframe*, kar povečuje možnost napadov vrste Clickjacking.

Predlagana rešitev

Predlagana je implementacija headerja X-Frame-Options z vrednostjo **SAMEORIGIN**.

Primer konfiguracije

```
Header always set X-Frame-Options "SAMEORIGIN"
```

Pričakovani učinki

Ta nastavitev preprečuje prikaz spletne strani znotraj okvirjev drugih domen in zmanjšuje možnost izvedbe Clickjacking napadov. Čeprav spletna stran ne vsebuje posebej občutljivih funkcionalnosti, predstavlja ta zaščita priporočeno dobro prakso.

- **Implementacija X-Content-Type-Options**

Ugotovljena pomanjkljivost

Mozilla Observatory je zaznal odsotnost zaščite pred napačno interpretacijo tipov datotek (*MIME Sniffing*).

Predlagana rešitev

Predlagana je implementacija headerja X-Content-Type-Options z vrednostjo `nosniff`.

Primer konfiguracije

```
Header always set X-Content-Type-Options "nosniff"
```

Pričakovani učinki

Implementacija preprečuje napačno interpretacijo datotek v spletnih brskalnikih in zmanjšuje možnost izvajanja potencialno nevarne vsebine.

- **Implementacija Referrer Policy**

Ugotovljena pomanjkljivost

Analiza je pokazala, da spletna stran nima določene politike Referrer-Policy, zato se lahko zunanjim spletnim mestom posreduje več informacij o uporabnikovem obisku, kot je potrebno.

Predlagana rešitev

Predlagana je implementacija politike **strict-origin-when-cross-origin**, ki predstavlja eno izmed priporočljivih nastavitev za zaščito zasebnosti uporabnikov.

Primer konfiguracije

Header always set Referrer-Policy "strict-origin-when-cross-origin"

Pričakovani učinki

Implementacija izboljša varovanje zasebnosti uporabnikov, zmanjša možnost razkrivanja informacij tretjim spletnim mestom ter poveča skladnost spletne strani s sodobnimi priporočili na področju varstva podatkov.

6.1.2 Zaščita obrazcev (captcha, sanitizacija vhodov, CSRF tokeni)

Analiza kontaktnega obrazca, predstavljena v poglavju 5.1.3, je pokazala, da spletna stran omogoča neposredno komunikacijo z obiskovalci, vendar iz javno dostopnega pregleda ni bilo mogoče potrditi uporabe vseh priporočljivih zaščitnih mehanizmov. Ker kontaktni obrazci sodijo med najpogostejše vstopne točke za avtomatizirane napade, neželeno pošto in zlonamerne uporabniške vnose, je njihova ustrezna zaščita pomemben del varnega razvoja spletnih aplikacij (Open Web Application Security Project, 2021).

- **Implementacija Google reCAPTCHA v3**

Ugotovljena pomanjkljivost

Med analizo ni bilo mogoče potrditi uporabe zaščite pred avtomatiziranim pošiljanjem obrazcev, zato obstaja možnost zlorabe kontaktnega obrazca za pošiljanje neželene pošte.

Predlagana rešitev

Priporočena je implementacija sistema **Google reCAPTCHA v3** oziroma druge primerljive rešitve za zaznavanje avtomatiziranih zahtevkov. Različica v3 deluje v ozadju in uporabniku ne prikazuje dodatnih preverjanj, zato ne vpliva na običajno uporabo spletne strani.

Način implementacije

V kontaktni obrazec se vključi JavaScript knjižnica Google reCAPTCHA, strežnik pa ob oddaji obrazca preveri oceno tveganja, ki jo vrne sistem. Na podlagi rezultata lahko aplikacija zahtevek sprejme ali zavrne.

Primer kode

```
<script
src="https://www.google.com/recaptcha/api.js?render=SITE_KEY"></script>
```

Pričakovani učinki

Implementacija zmanjša količino neželene pošte, omeji avtomatizirane zahtevke in zmanjša obremenitev upravljavca spletne strani. Ker rešitev deluje brez dodatne interakcije uporabnika, ohranja dobro uporabniško izkušnjo, kar je skladno z načelom ravnovesja med varnostjo in uporabnostjo ((Norman, 2013); (Krug, 2014)).

- **Implementacija CSRF zaščite**

Ugotovljena pomanjkljivost

Iz javno dostopnega pregleda ni bilo mogoče potrditi uporabe zaščite pred napadi vrste Cross-Site Request Forgery (CSRF), zato je priporočljiva uvedba dodatnega zaščitnega mehanizma.

Predlagana rešitev

Vsak kontaktni obrazec naj vsebuje enkraten žeton CSRF, ki ga aplikacija preveri ob oddaji obrazca. Takšen pristop učinkovito preprečuje ponarejene zahtevke, ki jih napadalec poskuša izvesti v imenu legitimnega uporabnika.

Način implementacije

CSRF zaščita temelji na generiranju naključnega žetona, ki se shrani v uporabniško sejo in doda v obrazec kot skrito polje. Ob oddaji obrazca strežnik preveri ujemanje prejetega žetona z vrednostjo v seji.

Primer kode

```
$_SESSION['token'] = bin2hex(random_bytes(32));
```

```
<input type="hidden" name="csrf_token" value="<?= $_SESSION['token']; ?>">
```

Pričakovani učinki

Implementacija CSRF zaščite preprečuje izvajanje ponarejenih zahtevkov, izboljša skladnost s priporočili organizacije OWASP in poveča varnost aplikacijske logike. Ker mehanizem deluje popolnoma v ozadju, uporabniki njegovega delovanja ne zaznajo.

- **Validacija in sanitizacija vhodnih podatkov**

Ugotovljena pomanjkljivost

Analiza ni omogočila potrditve, v kolikšni meri se uporabniški vnosi preverjajo in čistijo na strežniški strani. Neustrezna obdelava vhodnih podatkov lahko predstavlja tveganje za napade vrste Cross-Site Scripting (XSS), SQL Injection in druge oblike vbrizgavanja zlonamerne kode.

Predlagana rešitev

Priporočeni sta dosledna validacija in sanitizacija vseh uporabniških vnosov. Validacija preverja pravilnost vnesenih podatkov (npr. obliko elektronskega naslova, dolžino besedila ali izpolnjenost obveznih polj), sanitizacija pa odstrani oziroma nevtralizira potencialno nevarne znake, HTML oznake in skriptno kodo.

Način implementacije

Validacija mora biti izvedena tako na strani odjemalca kot na strežniški strani. Odjemalska validacija izboljša uporabniško izkušnjo, strežniška validacija pa zagotavlja dejansko varnost, saj lahko napadalec odjemalsko preverjanje obide.

Način implementacije

Validacija naj bo izvedena tako na strani odjemalca kot na strežniški strani. Odjemalska validacija izboljša uporabniško izkušnjo, strežniška validacija pa predstavlja dejanski varnostni mehanizem, saj lahko napadalec odjemalsko preverjanje enostavno obide.

Pričakovani učinki

Uvedba dosledne validacije in sanitizacije zmanjša tveganje za napade XSS in druge oblike vbrizgavanja kode, izboljša kakovost prejetih podatkov in poveča zanesljivost delovanja kontaktnega obrazca.

- **Omejevanje števila zahtevkov (Rate Limiting)**

Ugotovljena pomanjkljivost

Kontaktni obrazec je lahko izpostavljen večjemu številu avtomatiziranih zahtevkov, kar lahko povzroči pošiljanje neželene pošte, dodatno obremenitev strežnika ali druge oblike zlorabe.

Predlagana rešitev

Priporočljiva je uvedba mehanizma Rate Limiting, ki omejuje število zahtevkov z istega IP-naslova v določenem časovnem obdobju. Takšen pristop predstavlja enega najpogosteje uporabljenih zaščitnih mehanizmov pred avtomatiziranimi napadi (Open Web Application Security Project, 2021).

Pričakovani učinki

Implementacija zmanjša možnost avtomatiziranih zlorab, omeji pošiljanje neželene pošte ter prispeva k stabilnejšemu delovanju spletne strani. Ker se omejitve sprožijo le ob neobičajnem številu zahtevkov, običajni uporabniki spremembe ne zaznajo.

6.1.3 Optimizacija SSL/TLS nastavitev

Čeprav analiza ni pokazala težav z veljavnostjo certifikata SSL/TLS, dolgoročna varnost spletne strani ni odvisna zgolj od prisotnosti certifikata, temveč tudi od pravilne konfiguracije komunikacijskih protokolov, šifrirnih algoritmov in strežniških nastavitev (Qualys SSL Labs, 2024).

- **Ugotovljena pomanjkljivost**

Za zagotavljanje dolgoročne varnosti je priporočljivo redno preverjati konfiguracijo SSL/TLS in jo prilagajati sodobnim priporočilom. Zastarele različice protokolov in šibkejši šifrirni algoritmi lahko predstavljajo nepotrebno varnostno tveganje.

- **Predlagana rešitev**

Priporočljiva je uporaba sodobnih različic protokola **TLS 1.2** in **TLS 1.3**, onemogočanje zastarelih različic (SSL 3.0, TLS 1.0 in TLS 1.1) in redno spremljanje priporočil ponudnikov strežniške programske opreme.

- **Način implementacije**

Optimizacija se izvaja na ravni konfiguracije spletnega strežnika. Priporočljivo je:

- onemogočiti zastarele protokole,
- odstraniti šibke šifrirne algoritme,
- redno preverjati konfiguracijo z orodjem Qualys SSL Labs,
- zagotoviti pravočasno obnavljanje certifikatov SSL/TLS.

Ker spletna stran uporablja strežnik LiteSpeed in aktualno različico PHP, je priporočljivo tudi redno spremljanje varnostnih posodobitev strežniške programske opreme in sistema WordPress. Redno posodabljanje predstavlja enega temeljnih ukrepov za zmanjšanje tveganja izkoriščanja znanih ranljivosti ((WordPress Foundation, 2024); (Open Web Application Security Project, 2021)).

- **Pričakovani učinki**

Izvedba navedenih ukrepov bi zagotovila dolgoročno stabilnost in visoko raven zaščite komunikacije med uporabniki in spletnim strežnikom. Poleg izboljšanja varnosti bi optimizirana konfiguracija SSL/TLS povečala zaupanje uporabnikov in prispevala k boljšim rezultatom pri prihodnjih varnostnih analizah spletnega mesta.

6.2 UX/UI izboljšave

Analiza uporabniške izkušnje je pokazala, da spletna stran Andromа Collies uporabnikom omogoča enostaven dostop do informacij, pregledno navigacijo in prijetno uporabniško izkušnjo. Kljub pozitivnim rezultatom so bile ugotovljene posamezne možnosti za nadaljnje izboljšanje uporabnosti, dostopnosti in učinkovitosti spletnega mesta.

Predlagane izboljšave temeljijo na Nielsenovih heuristikah uporabnosti, smernicah WCAG 2.1 in sodobnih načelih UX/UI oblikovanja ((Nielsen, 1994); (W3C Web Accessibility Initiative, 2018)). Njihov namen je izboljšati dostopnost vsebin, povečati preglednost uporabniškega vmesnika in zagotoviti še učinkovitejšo uporabo spletne strani na različnih napravah.

Pri pripravi predlogov je bila posebna pozornost namenjena ravnovesju med funkcionalnostjo, dostopnostjo in vizualno kakovostjo. Predlagane izboljšave ne zahtevajo večjih sprememb obstoječe strukture spletne strani, temveč predstavljajo nadgradnje, ki lahko dodatno izboljšajo uporabniško izkušnjo in prispevajo k profesionalnejši predstavitvi psarne Andromа Collies.

6.2.1 Optimizacija navigacije

- **Ugotovljena pomanjkljivost**

Analiza je pokazala, da je navigacija pregledna in logično organizirana, vendar bi bilo mogoče uporabnikom še dodatno olajšati orientacijo znotraj spletnega mesta. Nielsen (1994) poudarja, da mora uporabniški vmesnik uporabniku ves čas jasno prikazovati njegov trenutni položaj v sistemu ter omogočati enostavno premikanje med posameznimi vsebinami.

- **Predlagana rešitev**

Priporočljiva je uvedba breadcrumb navigacije, ki uporabniku prikazuje trenutno lokacijo znotraj spletnega mesta ter izrazitejše vizualno označevanje aktivne strani v glavnem meniju. Takšni rešitvi sta skladni z Nielsenovima heuristikama *vidnost stanja sistema* in *prepoznavanje namesto pomnjenja*, saj zmanjšujeta potrebo po pomnjenju strukture spletnega mesta (Nielsen, 1994).

- **Primer breadcrumb navigacije**

Domov > Naši psi > Predstavitev psa

- **Pričakovani učinki**

Uvedba breadcrumb navigacije bi izboljšala orientacijo uporabnikov, zmanjšala njihovo kognitivno obremenitev in omogočila hitrejše premikanje med posameznimi vsebinskimi sklopi. Krug (2014) poudarja, da morajo uporabniki čim hitreje razumeti, kje se nahajajo, kam lahko nadaljujejo in kako se lahko vrnejo na prejšnje vsebine.

Ob nadaljnjem razvoju spletnega mesta bi bilo smiselno razmisliti tudi o uvedbi funkcije iskanja, ki bi uporabnikom omogočila hitrejši dostop do specifičnih informacij. Čeprav trenutni obseg vsebine tega še ne zahteva, bi takšna funkcionalnost predstavljala koristno nadgradnjo v prihodnosti (Shneiderman, in drugi, 2017).

6.2.2 Prilagoditev barv, tipografije in vizualnih elementov

- **Ugotovljena pomanjkljivost**

Vizualna podoba spletne strani predstavlja eno njenih največjih prednosti, saj kakovostne fotografije in profesionalen videz uspešno predstavljajo dejavnost psarne. Kljub temu analiza kaže, da obstajajo možnosti za dodatno izboljšanje dostopnosti in doslednosti vizualnega oblikovanja.

Smernice WCAG 2.1 priporočajo zagotavljanje ustreznega kontrasta med besedilom in ozadjem, dobro berljivost in jasno organizacijo informacij, saj ti elementi pomembno vplivajo na dostopnost spletnih vsebin (W3C Web Accessibility Initiative, 2018).

- **Predlagana rešitev**

Priporočljivo je preveriti kontrastna razmerja med posameznimi elementi in po potrebi izboljšati skladnost s smernicami WCAG 2.1. Posebno pozornost je smiselno nameniti berljivosti besedila, predvsem pri naslovih, gumbih in drugih pomembnih elementih uporabniškega vmesnika.

Prav tako je priporočljivo zagotoviti dosledno uporabo tipografije na vseh podstraneh. Enotna uporaba pisav, velikosti besedila in razmikov izboljšuje preglednost uporabniškega vmesnika ter zmanjšuje možnost zmede pri uporabnikih (Shneiderman, in drugi, 2017).

Dodatna izboljšava je lahko izrazitejša vizualna hierarhija, ki uporabnikom omogoča hitrejše razlikovanje med naslovi, podnaslovi in osnovnim besedilom. Jasno strukturirana vsebina

uporabnikom olajša pregledovanje strani in hitrejše iskanje pomembnih informacij (Krug, 2014).

- **Pričakovani učinki**

Izvedba predlaganih izboljšav bi povečala berljivost in dostopnost spletne strani ter izboljšala njeno vizualno preglednost. Ustrezna kontrastna razmerja, dosledna tipografija in jasna vizualna hierarhija bi uporabnikom omogočili hitrejše zaznavanje ključnih informacij ter prispevali k še bolj profesionalnemu videzu spletnega mesta.

Norman (2013) poudarja, da uporabniki lažje uporabljajo digitalne sisteme, kadar so informacije predstavljene jasno, dosledno in vizualno organizirano. Predlagane izboljšave zato ne prispevajo le k večji dostopnosti, temveč tudi k boljši splošni uporabniški izkušnji.

6.2.3 Izboljšave mobilne odzivnosti

- **Ugotovljena pomanjkljivost**

Analiza je pokazala, da se spletna stran Andromа Collies pravilno prilagaja različnim velikostim zaslonov in na mobilnih napravah ne kaže večjih težav pri prikazu vsebine. Kljub temu obstajajo možnosti za dodatno optimizacijo uporabniške izkušnje, predvsem pri uporabi interaktivnih elementov in mobilne navigacije.

Smernice WCAG 2.1 poudarjajo, da mora biti sodobna spletna stran prilagojena različnim velikostim zaslonov in omogočati učinkovito uporabo tudi na napravah z zasloni na dotik (W3C Web Accessibility Initiative, 2018).

- **Predlagana rešitev**

Priporočljivo je povečati klikabilna območja gumbov, povezav in drugih interaktivnih elementov, saj večje površine zmanjšujejo možnost napačnih klikov ter izboljšujejo uporabniško izkušnjo na mobilnih napravah.

Prav tako je priporočljivo preveriti delovanje navigacijskega menija na različnih velikostih zaslonov ter zagotoviti, da ključne funkcionalnosti ostanejo hitro dostopne tudi na manjših napravah. Krug (2014) poudarja, da morajo uporabniki iskane informacije najti hitro in brez nepotrebnega iskanja, ne glede na napravo, ki jo uporabljajo.

- **Način implementacije**

Izboljšave je mogoče izvesti s prilagoditvijo slogov CSS, povečanjem velikosti interaktivnih elementov in optimizacijo mobilnega navigacijskega menija. Pri implementaciji je priporočljivo preveriti delovanje spletne strani na različnih velikostih zaslonov in mobilnih brskalnikih.

- **Pričakovani učinki**

Predlagane izboljšave bi povečale preglednost uporabniškega vmesnika, zmanjšale možnost napačnih klikov ter izboljšale orientacijo uporabnikov na mobilnih napravah. Poleg tega bi optimizacija navigacije zmanjšala potrebo po pretiranem drsenju in prispevala k hitrejšemu dostopu do ključnih vsebin.

Izvedba navedenih ukrepov bi dodatno izboljšala uporabniško izkušnjo mobilnih uporabnikov ter povečala dostopnost spletne strani, kar je skladno s sodobnimi načeli uporabniško usmerjenega oblikovanja (Norman, 2013).

6.2.4 Pospešitev nalaganja strani

- **Ugotovljena pomanjkljivost**

Analiza uporabniške izkušnje je pokazala, da spletna stran vsebuje veliko fotografij visoke kakovosti, ki predstavljajo osrednji element predstavitve psarne. Ker slike predstavljajo največji delež prenesenih podatkov, pomembno vplivajo na hitrost nalaganja spletne strani.

Rezultati analize z orodjem Google Lighthouse so pokazali, da obstajajo možnosti za izboljšanje zmogljivosti predvsem z optimizacijo večpredstavnostnih vsebin. Google (2024) poudarja, da velikost slik predstavlja enega najpogostejših razlogov za počasnejše nalaganje spletnih strani, kar lahko negativno vpliva na uporabniško izkušnjo, optimizacijo za spletne iskalnike in stopnjo zapustitve strani.

- **Predlagana rešitev**

Ker kakovostne fotografije predstavljajo pomemben del predstavitve psarne, njihovo zmanjšanje ni smiselno. Primernejša rešitev je optimizacija načina shranjevanja in nalaganja slik.

Priporočeni ukrepi vključujejo:

- pretvorbo slik v format **WebP**,
- samodejno kompresijo slik,
- uporabo tehnologije **Lazy Loading**,
- pripravo različnih velikosti slik glede na napravo uporabnika.

Google Lighthouse med priporočene tehnike optimizacije uvršča uporabo sodobnih slikovnih formatov, zmanjšanje velikosti datotek in nalaganje vsebine po potrebi, saj takšni ukrepi pomembno izboljšajo zmogljivost spletnih strani (Google, 2024).

- **Primer implementacije**

Primer implementacije tehnologije Lazy Loading:

<img src="pes.webp" loading="lazy" alt="Rough Collie">

Poleg tega je priporočljiva uporaba WordPress vtičnikov oziroma strežniških mehanizmov za samodejno pretvorbo slik v format WebP in njihovo sprotno optimizacijo ob nalaganju na spletno stran.

- **Pričakovani učinki**

Uporaba formata WebP omogoča bistveno manjše velikosti datotek ob primerljivi kakovosti slik, kar zmanjša količino prenesenih podatkov in izboljša hitrost nalaganja spletne strani. Tehnologija Lazy Loading omogoča nalaganje slik šele takrat, ko jih uporabnik dejansko potrebuje, zato se začetni čas nalaganja strani občutno skrajša.

Izvedba predlaganih izboljšav bi prinesla več pomembnih prednosti:

- hitrejše nalaganje spletne strani,
- boljšo uporabniško izkušnjo,
- manjšo porabo mobilnih podatkov,
- višjo oceno pri analizi Google Lighthouse,
- boljšo optimizacijo za spletne iskalnike.

Po izvedbi optimizacije je priporočljivo preveriti prikaz slik na različnih napravah in velikostih zaslonov, da se zagotovi ohranitev kakovosti prikaza. Kljub temu predstavljajo navedeni ukrepi razmeroma enostavno in stroškovno učinkovito izboljšavo, ki lahko pomembno prispeva k večji zmogljivosti in uporabnosti spletne strani.

6.2.5 Povzetek predlaganih UX/UI izboljšav

Predlagane izboljšave uporabniške izkušnje temeljijo na rezultatih analize, predstavljene v petem poglavju, ter na priporočilih Nielsenovih heuristik uporabnosti in smernic WCAG 2.1. Večina predlaganih ukrepov ne zahteva večjih posegov v strukturo spletne strani, temveč predstavlja manjše oblikovalske in tehnične nadgradnje, ki lahko pomembno izboljšajo uporabniško izkušnjo, dostopnost in zmogljivost spletnega mesta.

Predlagane rešitve vključujejo izboljšanje navigacije, optimizacijo vizualnih elementov, povečanje dostopnosti, izboljšanje mobilne odzivnosti ter optimizacijo nalaganja strani z uporabo sodobnih tehnik, kot sta format WebP in mehanizem Lazy Loading. Izvedba teh ukrepov naj bi prispevala k hitrejšemu delovanju spletnega mesta, večji preglednosti in boljši uporabniški izkušnji na različnih napravah.

Predlagane izboljšave predstavljajo izhodišče za praktični del diplomskega dela, v katerem bodo implementirane in nato ovrednotene z uporabo ustreznih testnih orodij in uporabniškega testiranja.

7 IMPLEMENTACIJA IN TESTIRANJE

Na podlagi ugotovitev analize obstoječega stanja spletne strani Andromа Collies, predstavljenih v petem poglavju, ter predlaganih izboljšav iz šestega poglavja so bile izvedene konkretne spremembe na področju kibernetske varnosti in uporabniške izkušnje. Namen implementacije je bil odpraviti ugotovljene pomanjkljivosti, povečati raven zaščite spletnega mesta ter izboljšati njegovo dostopnost, uporabnost in zmogljivost.

Izvedene izboljšave so bile usmerjene predvsem v implementacijo dodatnih varnostnih mehanizmov, zaščito kontaktnega obrazca, optimizacijo slik in izboljšanje dostopnosti spletnih vsebin. Pri implementaciji so bila upoštevana priporočila organizacije OWASP, smernice WCAG 2.1 in dobre prakse razvoja spletnih aplikacij.

Po izvedbi vseh izboljšav je bilo ponovno izvedeno testiranje spletne strani z uporabo orodij Mozilla Observatory, SSL Labs in Google Lighthouse. Namen ponovnega testiranja je bil preveriti, ali so izvedene spremembe izboljšale varnostno konfiguracijo, zmogljivost in uporabniško izkušnjo spletnega mesta. Poleg avtomatiziranega testiranja sta bila izvedena tudi preverjanje delovanja posameznih funkcionalnosti in uporabniško testiranje, s katerim je bila ocenjena uporabnost spletne strani po izvedenih izboljšavah.

7.1 Izvedba varnostnih izboljšav

Na podlagi rezultatov varnostne analize so bile na spletni strani Andromа Collies izvedene izboljšave, katerih cilj je bil povečati odpornost spletnega mesta proti najpogostejšim spletnim grožnjam in izboljšati varnostno konfiguracijo strežniškega okolja. Posebna pozornost je bila namenjena implementaciji dodatnih varnostnih headerjev HTTP in zaščiti kontaktnega obrazca pred avtomatiziranimi zlorabami.

Izvedene izboljšave so bile implementirane neposredno na spletnem strežniku in v sistemu za upravljanje vsebin WordPress. Po zaključeni implementaciji je bilo ponovno izvedeno testiranje z uporabo orodij Mozilla Observatory in Qualys SSL Labs, s katerim je bila preverjena uspešnost izvedenih sprememb.

V nadaljevanju so predstavljene posamezne izvedene varnostne izboljšave in njihov vpliv na skupno raven varnosti spletne strani.

7.1.1 Implementacija varnostnih headerjev HTTP

V okviru izboljšanja varnosti spletne strani je bila izvedena implementacija dodatnih varnostnih headerjev HTTP. Analiza obstoječega stanja je pokazala, da spletna stran pred izvedbo izboljšav ni uporabljala več pomembnih varnostnih mehanizmov, zaradi česar je bila dosežena nizka ocena pri analizi z orodjem Mozilla Observatory.

Implementacija je bila izvedena z urejanjem konfiguracijske datoteke *.htaccess* na spletnem strežniku. Dodani so bili varnostni headerji Strict-Transport-Security (HSTS), X-Frame-Options, X-Content-Type-Options, Referrer-Policy in Permissions-Policy. Njihov namen je povečati zaščito spletnega mesta pred pogostimi spletnimi napadi, kot so Clickjacking, MIME Sniffing in prestrezanje komunikacije, hkrati pa izboljšati varovanje zasebnosti uporabnikov.

Pri implementaciji je bila načrtovana tudi uvedba politike Content Security Policy (CSP). Med testiranjem se je pokazalo, da je zaradi uporabe sistema WordPress in gradnika Oxygen Builder stroga CSP politika povzročila nepravilno delovanje posameznih elementov spletne strani. Zaradi zagotavljanja stabilnega delovanja spletnega mesta ta varnostni mehanizem ni bil implementiran, kar predstavlja eno izmed možnih nadaljnjih izboljšav.

Po izvedeni implementaciji je bilo ponovno izvedeno testiranje z orodjem Mozilla Observatory, ki je pokazalo bistveno izboljšanje varnostne konfiguracije spletnega strežnika in višjo skupno varnostno oceno.

```
# Security headers - Andromo Collies
<IfModule mod_headers.c>
Header always set Strict-Transport-Security "max-age=31536000;
    includeSubDomains"
Header always set X-Content-Type-Options "nosniff"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "camera=(), microphone=(), geolocation=()"
</IfModule>

# BEGIN WordPress
# The directives (lines) between "BEGIN WordPress" and "END WordPress" are
# dynamically generated, and should only be modified via WordPress filters.
# Any changes to the directives between these markers will be overwritten.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>

# END WordPress
```

Slika 7: Implementacija varnostnih headerjev v datoteki .htaccess

Vir: Lasten zajem zaslona (2026)

7.1.2 Implementacija Google reCAPTCHA v3

Naslednja izvedena izboljšava je bila implementacija sistema Google reCAPTCHA v3 za zaščito kontaktnega obrazca. Namen uvedbe je bil zmanjšati možnost avtomatiziranega pošiljanja neželenih sporočil in izboljšati zaščito obrazca pred zlorabami.

Implementacija je bila izvedena v sistemu WordPress z uporabo vtičnika Contact Form 7 in povezavo z Google reCAPTCHA v3 prek uradnega Google API-ja. Po uspešni registraciji spletne strani v storitvi Google reCAPTCHA sta bila ustvarjena javni in zasebni ključ, ki sta bila uporabljena za povezavo spletnega mesta z varnostnim sistemom.

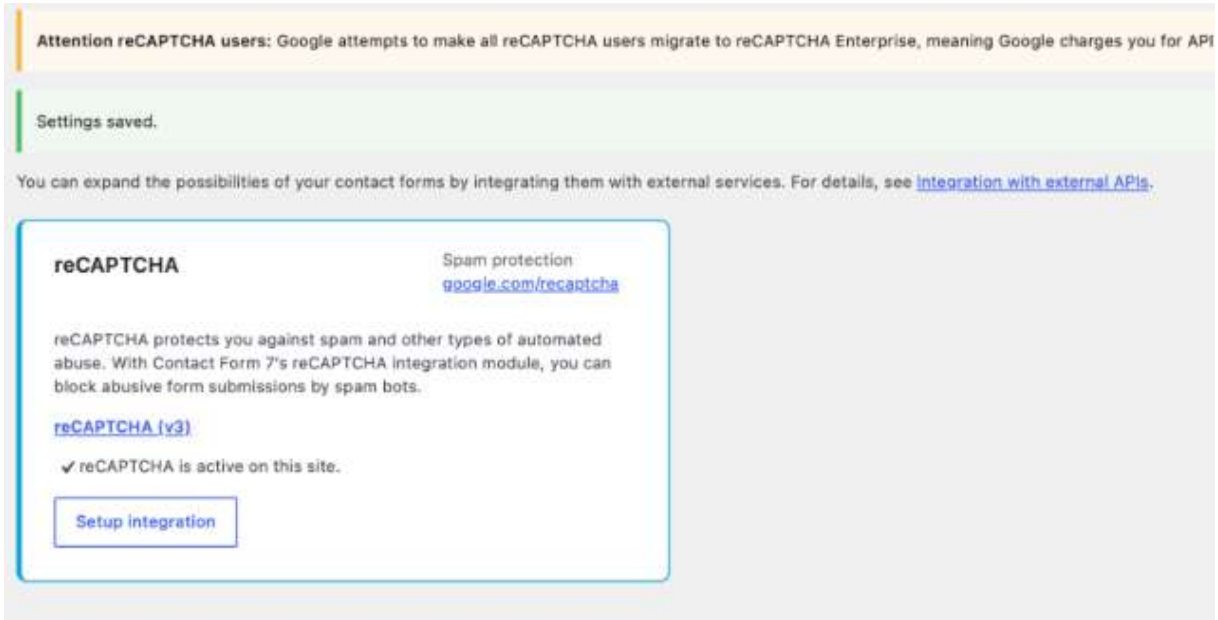
Za razliko od starejših različic reCAPTCHA različica v3 deluje v ozadju in uporabniku med izpolnjevanjem kontaktnega obrazca ne prikazuje dodatnih preverjanj ali slikovnih izzivov. Sistem samodejno analizira vedenje obiskovalca in na podlagi ocene tveganja ugotavlja, ali gre za legitimnega uporabnika ali za avtomatizirano poizvedbo. Takšna rešitev zagotavlja učinkovito zaščito kontaktnega obrazca, pri tem pa ne vpliva negativno na uporabniško izkušnjo.

Po uspešni implementaciji je bilo preverjeno pravilno delovanje povezave med WordPressom in storitvijo Google reCAPTCHA, kontaktni obrazec pa je uspešno uporabljal novo zaščito pred avtomatiziranimi zahtevki.



Slika 8: Povezava sistema Google reCAPTCHA v3 s kontaktnim obrazcem

Vir: Lasten zajem zaslona (2026)



Slika 9: Nastavitve Google reCAPTCHA v3

Vir: Lasten zajem zaslona (2026)

7.1.3 Rezultati izvedenih varnostnih izboljšav

Po zaključeni implementaciji varnostnih izboljšav je bilo ponovno izvedeno testiranje spletne strani z uporabo orodij Mozilla Observatory in Qualys SSL Labs. Namen ponovnega testiranja je bil preveriti vpliv izvedenih sprememb na varnostno konfiguracijo spletnega mesta.

Rezultati analize z orodjem Mozilla Observatory so pokazali občutno izboljšanje skupne varnostne ocene. Medtem ko je spletna stran pred implementacijo dosegla oceno **D**, je po uvedbi dodatnih varnostnih headerjev HTTP dosegla oceno **B**. Izboljšanje potrjuje, da je implementacija pomembno prispevala k večji skladnosti spletnega mesta s priporočili sodobnih varnostnih standardov.

Ponovno testiranje z orodjem Qualys SSL Labs je potrdilo pravilno konfiguracijo povezave HTTPS in nastavitev SSL/TLS, ki je tudi po izvedenih izboljšavah ohranila oceno A+.

Na podlagi izvedenih testov je mogoče zaključiti, da so implementirane izboljšave pomembno povečale raven varnosti spletnega mesta. Posebej se je izboljšala konfiguracija spletnega strežnika, povečala zaščita komunikacije in zmanjšala izpostavljenost nekaterim najpogostejšim spletnim grožnjam.

Tabela 6: Povzetek izvedenih varnostnih izboljšav

Izvedena izboljšava	Status
HTTPS preusmeritev	Izvedeno
HTTP Strict Transport Security (HSTS)	Izvedeno
X-Frame-Options	Izvedeno
X-Content-Type-Options	Izvedeno
Referrer-Policy	Izvedeno
Permissions-Policy	Izvedeno
Google reCAPTCHA v3	Izvedeno

Vir: Lastna izdelava

7.2 Izvedba UX/UI izboljšav

Na podlagi rezultatov analize uporabniške izkušnje in dostopnosti spletne strani so bile izvedene izboljšave, katerih namen je bil povečati dostopnost, izboljšati hitrost nalaganja in optimizirati prikaz vsebine na različnih napravah. Posebna pozornost je bila namenjena

izboljšavam, ki pomembno vplivajo na uporabniško izkušnjo, ne zahtevajo večjih sprememb strukture spletnega mesta ter so skladne s smernicami WCAG 2.1 in priporočili Google Lighthouse.

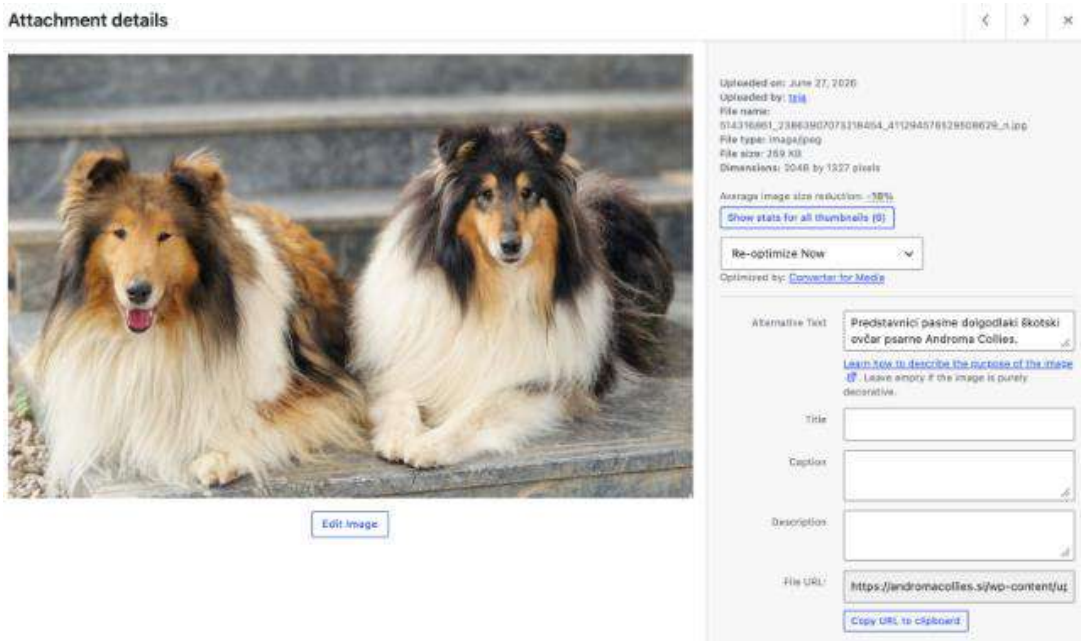
Izvedene izboljšave vključujejo dodajanje alternativnih opisov slik (ALT), optimizacijo slik z uporabo formata WebP in implementacijo mehanizma Lazy Loading. Po zaključeni implementaciji je bilo ponovno izvedeno testiranje z orodjem Google Lighthouse, s katerim je bil preverjen vpliv izvedenih sprememb na zmogljivost in uporabniško izkušnjo spletne strani.

7.2.1 Dodajanje alternativnih opisov slik (ALT)

Pri pregledu dostopnosti spletne strani je bilo ugotovljeno, da vse slike niso imele ustrezno določenih alternativnih opisov. Zaradi izboljšanja dostopnosti so bili ključnim fotografijam na spletni strani dodani opisni ALT atributi.

Alternativni opisi omogočajo uporabnikom bralnikov zaslona razumevanje vsebine slik, hkrati pa izboljšujejo optimizacijo spletne strani za spletne iskalnike. Pri pripravi opisov je bila upoštevana vsebina posamezne fotografije, pri čemer so bili opisi kratki, razumljivi in dovolj opisni, da so uporabnikom posredovali bistvene informacije o prikazani vsebini.

Dodajanje ALT opisov predstavlja enega izmed osnovnih ukrepov za izboljšanje dostopnosti spletnih vsebin in prispeva k večji skladnosti spletnega mesta s smernicami WCAG 2.1.



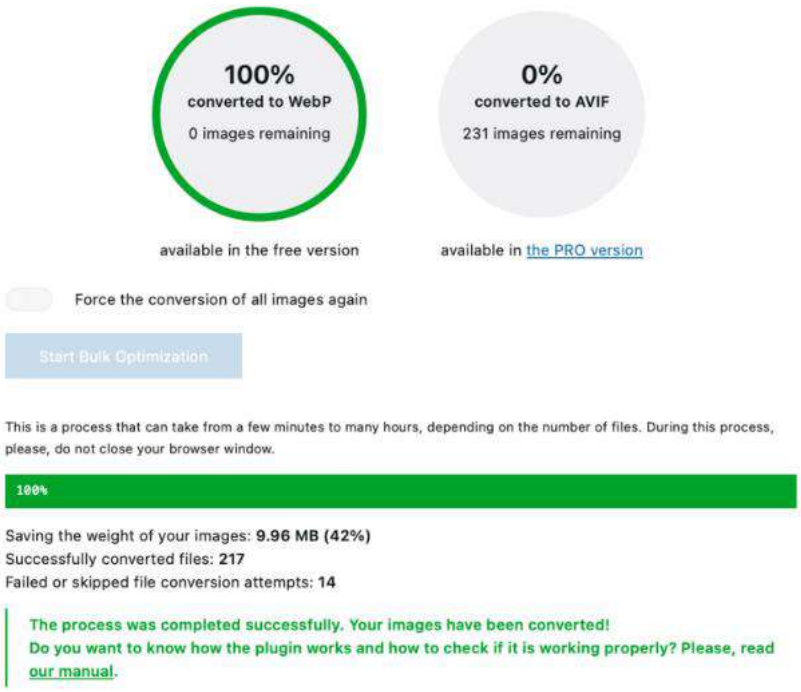
Slika 10: Dodajanje alternativnega opisa (ALT) fotografiji v knjižnici predstavnosti WordPress

Vir: Lasten zajem zaslona (2026)

7.2.2 Optimizacija slik: pretvorba v format WebP

Ker spletna stran vsebuje veliko fotografij visoke ločljivosti, je bila izvedena optimizacija slik z uporabo vtičnika Converter for Media. V okviru optimizacije so bile obstoječe slike pretvorjene v sodobni slikovni format WebP, ki omogoča manjšo velikost datotek ob primerljivi kakovosti prikaza.

Po zaključeni pretvorbi je bilo uspešno optimiziranih 217 slik, skupna velikost slik pa se je zmanjšala za približno 9,96 MB, kar predstavlja približno 42-odstotno zmanjšanje glede na prvotno velikost. Zmanjšanje količine prenesenih podatkov pozitivno vpliva na hitrost nalaganja spletne strani in izboljšuje uporabniško izkušnjo, zlasti pri dostopu prek mobilnih naprav.



Slika 11: Rezultat pretvorbe slik v format WebP z uporabo vtičnika Converter for Media

Vir: Lasten zajem zaslona (2026)

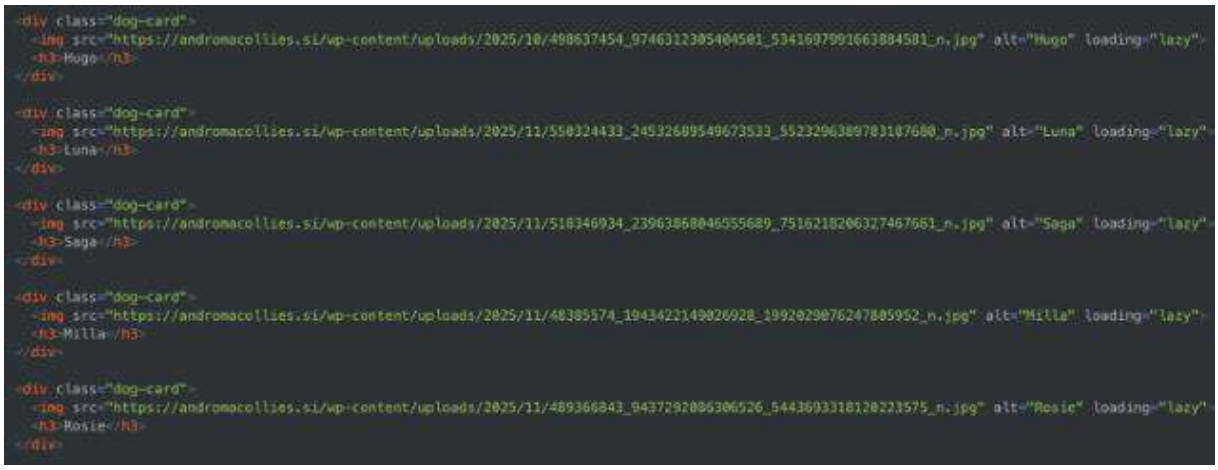
Izvedena optimizacija predstavlja pomembno izboljšavo zmogljivosti spletnega mesta in je skladna s priporočili orodja Google Lighthouse za optimizacijo spletnih vsebin.

7.2.3 Implementacija Lazy Loading

Za dodatno optimizacijo hitrosti nalaganja spletne strani je bil pri vseh fotografijah, kjer je bilo to smiselno, implementiran atribut **loading="lazy"**. Ta omogoča, da se slike ne naložijo ob odprtju spletne strani, temveč šele takrat, ko uporabnik med pregledovanjem strani doseže njihov položaj.

Implementacija je bila izvedena z dodajanjem atributa *loading="lazy"* elementom <img> v izvorni kodi posameznih podstrani. Takšen način nalaganja zmanjšuje začetno količino prenesenih podatkov, skrajša čas nalaganja strani in izboljša zaznano hitrost delovanja spletnega mesta.

Ker spletna stran vsebuje več fotografij, predvsem na straneh s predstavitvijo psov, legel in galerije, uvedba mehanizma Lazy Loading pomembno prispeva k učinkovitejšemu delovanju spletnega mesta in boljši uporabniški izkušnji.



Slika 12: Implementacija atributa loading="lazy" v izvorni kodi spletne strani

Vir: Lasten zajem zaslona (2026)

7.2.4 Povzetek izvedenih UX/UI izboljšav

Na podlagi izvedenih izboljšav je mogoče ugotoviti, da so bile uspešno implementirane vse načrtovane spremembe na področju uporabniške izkušnje in dostopnosti spletne strani. Dodani alternativni opisi slik izboljšujejo dostopnost spletnega mesta za uporabnike pomožnih tehnologij, optimizacija slik v format WebP zmanjšuje količino prenesenih podatkov, implementacija mehanizma Lazy Loading pa prispeva k hitrejšemu nalaganju vsebine in boljši zmogljivosti spletnega mesta.

Izvedene izboljšave predstavljajo pomembno nadgradnjo obstoječe spletne strani ter prispevajo k večji skladnosti s smernicami WCAG 2.1 in priporočili Google Lighthouse.

Tabela 7: Povzetek izvedenih UX/UI izboljšav

Izvedena izboljšava	Status
Dodani ALT opisi slik	Izvedeno
Pretvorba slik v format WebP	Izvedeno
Implementacija Lazy Loading	Izvedeno
Optimizacija hitrosti nalaganja	Izvedeno

Vir: Lastna izdelava

7.3 Testiranje po izboljšavah

Po izvedbi vseh načrtovanih izboljšav je bilo ponovno izvedeno testiranje spletne strani Andromа Collies z uporabo enakih orodij, kot so bila uporabljena pri analizi obstoječega stanja. Namen ponovnega testiranja je bil preveriti vpliv izvedenih sprememb na varnost, zmogljivost in uporabniško izkušnjo spletnega mesta ter oceniti uspešnost implementiranih izboljšav.

Testiranje je bilo izvedeno z uporabo orodij Mozilla Observatory, Qualys SSL Labs in Google Lighthouse. Poleg tehničnega testiranja je bilo izvedeno tudi uporabniško testiranje, s katerim je bila preverjena uporabnost spletne strani po izvedenih izboljšavah.

7.3.1 Testiranje z Mozilla Observatory

Po implementaciji dodatnih varnostnih headerjev HTTP je bilo ponovno izvedeno testiranje spletne strani z uporabo orodja Mozilla Observatory. Rezultati so pokazali bistveno izboljšanje varnostne konfiguracije spletnega strežnika.

Medtem ko je spletna stran pred izvedbo izboljšav dosegla oceno **D (30/100)**, je po implementaciji varnostnih headerjev dosegla oceno **B**, kar predstavlja pomemben napredek. Izboljšanje je predvsem posledica uvedbe mehanizmov HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy in Permissions-Policy.

Kljub izboljšanju najvišje ocene ni bilo mogoče doseči, saj zaradi zagotavljanja pravilnega delovanja spletne strani ni bila implementirana politika Content Security Policy (CSP). Ta predstavlja eno izmed možnih nadaljnjih izboljšav spletnega mesta.



Slika 13: Rezultat analize Mozilla Observatory po implementaciji varnostnih izboljšav

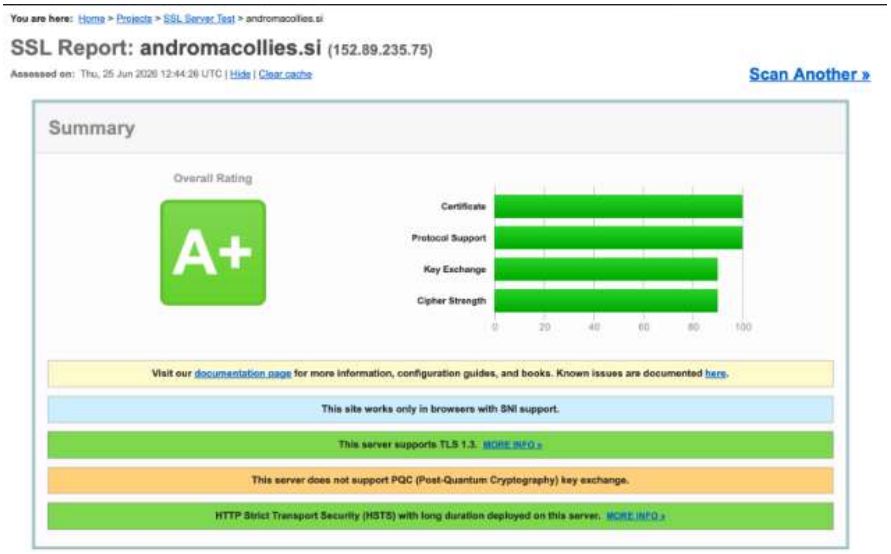
Vir: Lasten zajem zaslona (2026)

7.3.2 Testiranje z Qualys SSL Labs

Po izvedenih izboljšavah je bila ponovno preverjena tudi SSL/TLS konfiguracija spletnega mesta z uporabo orodja Qualys SSL Labs.

Rezultati analize so pokazali, da spletna stran dosega oceno **A+**, kar potrjuje pravilno implementacijo povezave HTTPS, ustrezno konfiguracijo SSL/TLS protokolov ter uporabo sodobnih varnostnih nastavitev. Dosežena ocena potrjuje, da spletna stran zagotavlja visoko raven zaščite komunikacije med uporabnikom in spletnim strežnikom.

Izvedene izboljšave so prispevale predvsem k večji zanesljivosti povezave HTTPS in boljši skladnosti s priporočili sodobnih varnostnih standardov.



Slika 14: Rezultat analize SSL konfiguracije z orodjem Qualys SSL Labs

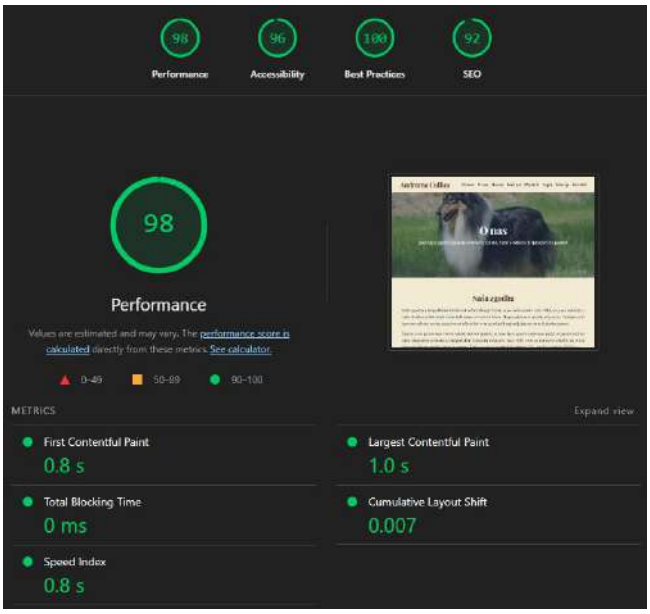
Vir: Lasten zajem zaslona (2026)

7.3.3 Testiranje z Google Lighthouse

Po izvedenih UX/UI izboljšavah je bilo ponovno izvedeno testiranje spletne strani z uporabo orodja Google Lighthouse. Namen analize je bil preveriti vpliv optimizacije slik, implementacije mehanizma Lazy Loading in drugih izboljšav na zmogljivost ter uporabniško izkušnjo spletnega mesta.

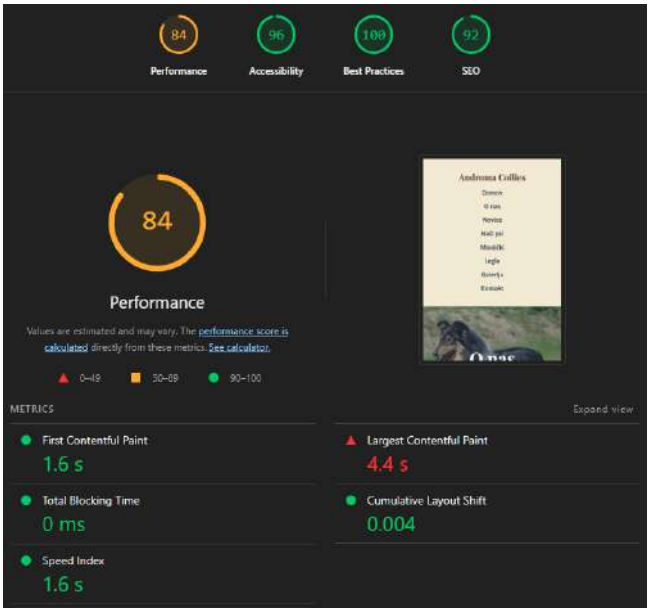
Analiza je bila izvedena ločeno za mobilne in namizne naprave. Rezultati so pokazali izboljšanje zmogljivosti spletne strani ter zelo dobre ocene na področjih dostopnosti, dobrih praks in optimizacije za spletne iskalnike.

Izboljšanje rezultatov je predvsem posledica optimizacije slik v format WebP, zmanjšanja velikosti prenesenih datotek, uvedbe mehanizma Lazy Loading in drugih izvedenih optimizacij.



Slika 15: Rezultati Google Lighthouse za namizne naprave

Vir: Lasten zajem zaslona (2026)



Slika 16: Rezultati Google Lighthouse za mobilne naprave

Vir: Lasten zajem zaslona (2026)

Za preverjanje hitrosti nalaganja, dostopnosti, skladnosti z dobrimi praksami in optimizacije za iskalnike je bilo uporabljeno orodje Google Lighthouse. Testiranje je bilo izvedeno tako za namizno kot mobilno različico spletne strani. Rezultati kažejo, da so izvedene optimizacije bistveno izboljšale delovanje spletne strani. Namizna različica je dosegla **98 točk** pri

zmogljivosti (Performance), **96 točk** pri dostopnosti (Accessibility), **100 točk** pri skladnosti z dobrimi praksami (Best Practices) in **92 točk** pri optimizaciji za iskalnike (SEO). Mobilna različica je dosegla **84 točk** pri zmogljivosti, medtem ko so druge kategorije dosegle enake oziroma primerljive rezultate. Nekoliko nižja ocena zmogljivosti na mobilnih napravah je pričakovana, saj Lighthouse uporablja strožje pogoje testiranja z omejenimi strojnimi viri in simulacijo počasnejšega mobilnega omrežja. Zato nižja ocena mobilne različice ne pomeni slabše kakovosti spletne strani, temveč predstavlja rezultat zahtevnejše metodologije testiranja. Rezultati potrjujejo, da je spletna stran dobro optimizirana tako z vidika uporabniške izkušnje kot tudi tehnične kakovosti.

7.3.4 Uporabniško testiranje

Poleg tehničnega testiranja je bilo izvedeno tudi uporabniško testiranje spletne strani. Namen testiranja je bil preveriti uporabnost spletnega mesta po izvedenih izboljšavah ter oceniti, ali uporabniki brez težav dostopajo do ključnih informacij in funkcionalnosti.

Pri testiranju je sodelovalo pet uporabnikov, ki predhodno niso sodelovali pri razvoju spletne strani. Vsak uporabnik je izvedel enake naloge, pri čemer so bile ocenjene uspešnost njihove izvedbe in morebitne težave pri uporabi spletnega mesta.

Uporabniki so morali opraviti naslednje naloge:

- poiskati kontaktne podatke psarne,
- poiskati informacije o leglih,
- poiskati predstavitev določenega psa,
- poslati testno sporočilo prek kontaktnega obrazca.

Rezultati uporabniškega testiranja so pokazali, da so vsi uporabniki uspešno opravili zastavljene naloge brez večjih težav. Navigacija je bila ocenjena kot pregledna, informacije pa so bile hitro dostopne. Uporabniki niso poročali o težavah pri uporabi kontaktnega obrazca ali pri iskanju vsebin na spletni strani.

Tabela 8: Rezultati uporabniškega testiranja

Naloga	Uspešno
Iskanje kontaktnih podatkov	5/5

Iskanje informacij o leglih	5/5
Iskanje podatkov o psih	5/5
Pošiljanje kontaktnega obrazca	5/5

Vir: Lastna analiza rezultatov testiranja uporabnikov

Rezultati kažejo, da uporabniki niso imeli težav pri iskanju informacij in uporabi spletne strani in potrjujejo, da izvedene izboljšave niso zmanjšale uporabnosti spletnega mesta, temveč so jo ohranile oziroma dodatno izboljšale. Uporabniki so kot prednosti izpostavili pregledno strukturo strani, kakovostne fotografije in hitro dostopnost kontaktnih informacij. Nobeden izmed sodelujočih uporabnikov med testiranjem ni poročal o tehničnih težavah ali napakah pri uporabi spletne strani. Vsi so ocenili, da je navigacija pregledna, kontaktni obrazec pa enostaven za uporabo.

7.4 Primerjava rezultatov pred izboljšavami in po njih

Za oceno uspešnosti izvedenih izboljšav je bila pripravljena primerjava rezultatov testiranj pred implementacijo in po njej. Primerjava temelji na rezultatih orodij Mozilla Observatory, Qualys SSL Labs in Google Lighthouse ter na izvedenem uporabniškem testiranju.

Rezultati kažejo, da so izvedene izboljšave pozitivno vplivale tako na varnostno konfiguracijo spletne strani kot na njeno zmogljivost, dostopnost in uporabniško izkušnjo. Posebej izrazito izboljšanje je bilo doseženo na področju implementacije varnostnih headerjev HTTP, zaščite kontaktnega obrazca in optimizacije slik.

Tabela 9 prikazuje primerjavo najpomembnejših kazalnikov pred izvedenimi izboljšavami in po njih.

Tabela 9: Primerjava rezultatov pred izvedenimi izboljšavami in po njih

Kazalnik	**Pred izboljšavami**	**Po izboljšavah**
Mozilla Observatory	D	B
SSL Labs	A	A+
HTTPS preusmeritev	Da	Da
HSTS	Ne	Da
X-Frame-Options	Ne	Da

X-Content-Type-Options	Ne	Da
Referrer-Policy	Ne	Da
Permissions-Policy	Ne	Da
Google reCAPTCHA	Ne	Da
ALT opisi ključnih slik	Delno	Da
Format WebP	Ne	Da
Lazy Loading	Ne	Da
Mobilna odzivnost	Ustrezna	Izboljšana in ponovno preverjena
Lighthouse Performance (Desktop)	88	98
Lighthouse Performance (Mobile)	71	84

Vir: Lastna analiza rezultatov

Na področju varnosti je največje izboljšanje predstavljala implementacija dodatnih varnostnih headerjev HTTP, zaradi katerih se je ocena Mozilla Observatory izboljšala z D na B. Prav tako je bila uspešno uvedena zaščita kontaktnega obrazca z uporabo sistema Google reCAPTCHA v3, ki zmanjšuje možnost avtomatiziranih zlorab.

Na področju uporabniške izkušnje so bile izvedene izboljšave dostopnosti in optimizacije zmogljivosti. Dodani so bili alternativni opisi slik, vse ključne fotografije so bile optimizirane v format WebP, implementiran pa je bil tudi mehanizem Lazy Loading. Posledično se je zmanjšala količina prenesenih podatkov in izboljšala hitrost nalaganja spletnega mesta.

Ponovno testiranje z orodji Mozilla Observatory, Qualys SSL Labs in Google Lighthouse je potrdilo, da so izvedene izboljšave uspešno odpravile večino ugotovljenih pomanjkljivosti. Poleg tehničnih rezultatov je uporabniško testiranje pokazalo, da uporabniki tudi po izvedenih spremembah spletno stran uporabljajo brez težav ter da so navigacija, preglednost in dostop do informacij ostali enostavni in intuitivni. Na podlagi primerjave rezultatov je mogoče zaključiti, da so bile načrtovane izboljšave uspešno implementirane in da so pomembno prispevale k večji varnosti, boljši uporabniški izkušnji in večji kakovosti spletne strani Andromа Collies.

8 REZULTATI IN RAZPRAVA

V tem poglavju so predstavljeni rezultati izvedenih izboljšav na področju kibernetske varnosti in uporabniške izkušnje spletne strani Andromа Collies. Rezultati temeljijo na primerjavi stanja pred izvedbo izboljšav in po njihovi implementaciji ter na ponovnem testiranju z uporabo orodij Mozilla Observatory, Qualys SSL Labs in Google Lighthouse.

Namen poglavja ni zgolj predstavitev doseženih rezultatov, temveč tudi njihova interpretacija in kritična presoja. Poseben poudarek je namenjen oceni učinkovitosti izvedenih varnostnih in UX/UI izboljšav, njihovemu vplivu na delovanje spletnega mesta ter preverjanju, ali so bili doseženi zastavljeni cilji diplomskega dela.

Na podlagi primerjave rezultatov je mogoče oceniti, v kolikšni meri so izvedene izboljšave prispevale k večji varnosti spletne strani, izboljšani dostopnosti in boljši uporabniški izkušnji. Rezultati predstavljajo tudi osnovo za odgovore na raziskovalna vprašanja in preverjanje zastavljene hipoteze.

8.1 Analiza doseženih izboljšav

Analiza rezultatov kaže, da so bile načrtovane izboljšave uspešno implementirane in da so pomembno prispevale k povečanju varnosti ter izboljšanju uporabniške izkušnje spletne strani Andromа Collies.

Na področju kibernetske varnosti je največji napredek predstavljala implementacija dodatnih varnostnih headerjev HTTP, zaradi katerih se je ocena orodja Mozilla Observatory izboljšala z ocene D na oceno B. Poleg tega je bila uspešno implementirana zaščita kontaktnega obrazca z uporabo sistema Google reCAPTCHA v3, ki zmanjšuje možnost avtomatiziranega pošiljanja neželene pošte in drugih zlorab.

Ponovno testiranje z orodjem Qualys SSL Labs je potrdilo ustrezno konfiguracijo povezave HTTPS in SSL/TLS nastavitev, kar potrjuje dosežena ocena A+. Izvedene izboljšave so tako povečale odpornost spletnega mesta proti najpogostejšim spletnim napadom in izboljšale skladnost z dobrimi praksami varnega razvoja spletnih aplikacij.

Na področju uporabniške izkušnje so bile izvedene izboljšave dostopnosti in zmogljivosti. Dodani alternativni opisi slik izboljšujejo dostopnost spletnega mesta za uporabnike pomožnih tehnologij, optimizacija slik v format WebP pa je zmanjšala količino prenesenih podatkov in izboljšala hitrost nalaganja strani. Implementacija mehanizma Lazy Loading je dodatno prispevala k učinkovitejšemu nalaganju vsebine predvsem na podstraneh z večjim številom fotografij.

Rezultati testiranja z orodjem Google Lighthouse potrjujejo izboljšanje zmogljivosti spletne strani ter zelo dobre rezultate na področjih dostopnosti, dobrih praks in optimizacije za spletne iskalnike. Izvedene spremembe niso negativno vplivale na uporabniško izkušnjo, kar potrjujejo tudi rezultati uporabniškega testiranja.

Tabela 10: Povzetek doseženih izboljšav

Področje	**Dosežena izboljšava**
Mozilla Observatory	D - B
Qualys SSL Labs	A - A+
http Security Headers	Implementirani
Google reCAPTCHA	Implementirana
ALT opisi	Dodani
WebP	Implementiran
Lazy Loading	Implementiran

Vir: Lastna izdelava

8.2 Razprava o učinkovitosti varnostnih sprememb

Izvedene varnostne izboljšave so pomembno prispevale k povečanju ravni zaščite spletne strani Andromа Collies. Ponovno testiranje z orodjema Mozilla Observatory in Qualys SSL Labs je potrdilo, da je implementacija dodatnih varnostnih mehanizmov izboljšala konfiguracijo spletnega strežnika in povečala skladnost spletnega mesta s sodobnimi priporočili kibernetske varnosti.

Največji napredek je bil dosežen na področju implementacije varnostnih headerjev HTTP. Uvedba mehanizmov HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy in Permissions-Policy je zmanjšala izpostavljenost spletnim napadom, kot so Clickjacking, MIME

Sniffing in prestrezanje nezaščitene komunikacije. Posledično se je ocena orodja Mozilla Observatory izboljšala z D na B, kar potrjuje večjo varnostno ustreznost spletnega mesta.

Pomembna izboljšava je bila tudi implementacija sistema Google reCAPTCHA v3, ki zmanjšuje možnost avtomatiziranega pošiljanja neželenih sporočil prek kontaktnega obrazca. Ker reCAPTCHA deluje v ozadju, izboljšava ni negativno vplivala na uporabniško izkušnjo, hkrati pa je povečala zaščito obrazca pred zlorabami.

Kljub doseženim izboljšavam analiza kaže, da obstajajo tudi določene omejitve. Zaradi uporabe sistema WordPress in gradnika Oxygen Builder implementacija politike Content Security Policy (CSP) ni bila izvedena, saj je povzročala nepravilno delovanje posameznih elementov spletne strani. To pomeni, da obstaja možnost nadaljnjega izboljšanja varnostne konfiguracije, vendar bi bilo pred uvedbo treba izvesti podrobnejše testiranje in prilagoditev politike uporabljenim tehnologijam.

Na podlagi rezultatov je mogoče ugotoviti, da so izvedene spremembe pomembno povečale varnost spletne strani, pri tem pa niso vplivale na njeno funkcionalnost ali uporabniško izkušnjo. Izvedene izboljšave zato predstavljajo učinkovito ravnovesje med varnostjo in uporabnostjo spletnega mesta.

8.3 Razprava o vplivu UX/UI sprememb na uporabniško izkušnjo

Izvedene izboljšave na področju uporabniške izkušnje so pozitivno vplivale na dostopnost, zmogljivost in splošno uporabnost spletne strani. Čeprav je analiza obstoječega stanja pokazala, da je bila spletna stran že pred izvedbo izboljšav pregledna in uporabnikom prijazna, so izvedene spremembe prispevale k njeni nadaljnji optimizaciji.

Dodajanje alternativnih opisov slik je izboljšalo dostopnost spletnega mesta za uporabnike bralnikov zaslona in povečalo skladnost s smernicami WCAG 2.1. Poleg tega alternativni opisi prispevajo tudi k boljši optimizaciji spletne strani za spletne iskalnike.

Pomemben vpliv na uporabniško izkušnjo je imela optimizacija slik v format WebP, saj se je skupna velikost slik zmanjšala za približno 42 %. Manjša količina prenesenih podatkov omogoča hitrejše nalaganje spletne strani, kar je še posebej pomembno za uporabnike mobilnih naprav in počasnejših internetnih povezav.

Dodatno izboljšanje predstavlja implementacija mehanizma Lazy Loading, ki omogoča postopno nalaganje slik glede na položaj uporabnika na strani. Takšen način nalaganja zmanjšuje začetni čas odpiranja strani in izboljšuje zaznano hitrost delovanja spletnega mesta.

Rezultati uporabniškega testiranja potrjujejo, da izvedene izboljšave niso otežile uporabe spletne strani. Uporabniki so brez težav dostopali do ključnih informacij, navigacija je ostala pregledna, kontaktni obrazec pa je kljub dodatni zaščiti omogočal enostavno komunikacijo z upravljavci spletnega mesta.

Na podlagi rezultatov lahko zaključimo, da so izvedene UX/UI izboljšave uspešno povečale dostopnost in zmogljivost spletne strani, ne da bi pri tem negativno vplivale na njeno preglednost ali uporabniško izkušnjo.

8.4 Omejitve raziskave

Kljub uspešno izvedenim izboljšavam in pozitivnim rezultatom ima raziskava tudi določene omejitve, ki jih je treba upoštevati pri interpretaciji rezultatov.

Prva omejitev je povezana z obsegom raziskave, saj je bila analiza izvedena na eni spletni strani. Zaradi tega rezultatov ni mogoče neposredno posplošiti na vse spletne strani ali druge spletne aplikacije, saj se uporabljene tehnologije, konfiguracije strežnikov in funkcionalnosti med posameznimi sistemi razlikujejo.

Druga omejitev izhaja iz omejenega dostopa do strežniškega okolja in aplikacijske logike. Analiza je temeljila predvsem na javno dostopnih informacijah in rezultatih specializiranih orodij za varnostno testiranje. Zaradi tega ni bilo mogoče v celoti preveriti nekaterih varnostnih mehanizmov, kot so strežniška validacija vhodnih podatkov, zaščita pred napadi CSRF ali notranje varnostne nastavitve aplikacije.

Omejitev predstavlja tudi dejstvo, da zaradi uporabe sistema WordPress in gradnika Oxygen Builder ni bilo mogoče implementirati politike Content Security Policy (CSP), ne da bi pri tem vplivali na pravilno delovanje spletnega mesta. Zato ta izboljšava v okviru raziskave ni bila izvedena in predstavlja možnost za nadaljnje delo.

Uporabniško testiranje je bilo izvedeno na manjšem številu uporabnikov, zato rezultati predstavljajo predvsem orientacijsko oceno uporabniške izkušnje. Za natančnejšo oceno bi bilo

smiselno vključiti več uporabnikov različnih starostnih skupin in z različnimi stopnjami digitalnih kompetenc.

Kljub navedenim omejitvam raziskava dosega zastavljene cilje. Izvedene izboljšave so bile uspešno implementirane, njihovi učinki pa potrjeni z uporabo uveljavljenih orodij za testiranje spletnih aplikacij. Rezultati zato predstavljajo verodostojno osnovo za oceno vpliva izvedenih izboljšav na varnost in uporabniško izkušnjo spletne strani Androma Collies.

8.5 Odgovori na raziskovalna vprašanja

RV1: Kako varna je obstoječa spletna stran Androma Collies glede na najpogostejše ranljivosti spletnih aplikacij (OWASP Top 10)?

Analiza spletne strani je pokazala, da ta zagotavlja zadovoljivo osnovno raven varnosti, saj uporablja povezavo HTTPS in veljaven certifikat SSL/TLS. Z uporabo orodij Mozilla Observatory, Qualys SSL Labs in Google Lighthouse so bile ugotovljene predvsem pomanjkljivosti na področju konfiguracije varnostnih headerjev HTTP in zaščite kontaktnega obrazca. Kritične ranljivosti niso bile zaznane, vendar so rezultati pokazali več možnosti za izboljšanje varnostne konfiguracije spletnega mesta.

RV2: Na kakšen način lahko predlagane varnostne izboljšave povečajo zaščito spletne strani, ne da bi negativno vplivale na uporabniško izkušnjo?

Izvedene izboljšave, kot so implementacija varnostnih headerjev HTTP, uvedba sistema Google reCAPTCHA v3, optimizacija SSL/TLS nastavitev in izboljšana zaščita kontaktnega obrazca so povečale raven zaščite spletne strani brez opaznega vpliva na njeno uporabnost. Uporabniško testiranje je pokazalo, da uporabniki spletno stran uporabljajo enako enostavno kot pred uvedbo izboljšav, saj večina varnostnih mehanizmov deluje v ozadju.

RV3: Kako lahko izboljšave uporabniškega vmesnika (UX/UI) prispevajo k večji dostopnosti, uporabnosti in posledično tudi varnejši uporabi spletne strani?

Izvedene UX/UI izboljšave so izboljšale dostopnost, preglednost in uporabnost spletnega mesta. Dodani alternativni opisi slik, optimizacija slik v format WebP, implementacija mehanizma Lazy Loading in izboljšana dostopnost vsebine omogočajo hitrejše nalaganje strani, boljšo uporabniško izkušnjo in enostavnejšo uporabo spletnega mesta na različnih napravah.

Posledično uporabniki lažje razumejo vsebino in učinkoviteje uporabljajo funkcionalnosti spletne strani.

RV4: Zakaj je kibernetska varnost pomembna tudi za manjše organizacije, kot je psarna Andromа Collies, in kako prispeva k zaupanju uporabnikov?

Rezultati raziskave potrjujejo, da je kibernetska varnost pomembna tudi za manjše organizacije. Tudi manjša spletna mesta obdelujejo osebne podatke uporabnikov in predstavljajo potencialno tarčo različnih spletnih napadov. Uvedba sodobnih varnostnih mehanizmov povečuje zaupanje obiskovalcev, izboljšuje zaščito osebnih podatkov ter prispeva k profesionalni in verodostojni podobi organizacije.

8.6 Potrditev hipotez

H1: Spletna stran Andromа Collies vsebuje varnostne pomanjkljivosti, ki jih je mogoče odkriti z uporabo standardnih orodij za analizo spletnih aplikacij (Qualys SSL Labs, Mozilla Observatory, Lighthouse).

Hipoteza H1 je potrjena. Analiza z uporabo orodij Mozilla Observatory, Qualys SSL Labs in Google Lighthouse je pokazala več pomanjkljivosti, predvsem na področju konfiguracije varnostnih headerjev HTTP, zaščite kontaktnega obrazca in optimizacije spletnega mesta. Ugotovitve so predstavljale osnovo za izvedbo predlaganih izboljšav.

H2: Izboljšave v varnostnem pristopu (npr. implementacija varnostnih headerjev, zaščita obrazcev, optimizacija SSL) ne vplivajo negativno na uporabniško izkušnjo, temveč jo lahko celo izboljšajo z večjim občutkom zaupanja.

Hipoteza H2 je potrjena. Izvedene varnostne izboljšave niso povzročile zmanjšanja uporabnosti spletne strani. Nasprotno, implementacija dodatnih zaščitnih mehanizmov je povečala raven varnosti, uporabniško testiranje pa je pokazalo, da uporabniki pri uporabi spletnega mesta niso zaznali dodatnih ovir. Poleg večje zaščite spletne strani izboljšave prispevajo tudi k večjemu občutku zaupanja uporabnikov.

H3: Nadgradnja uporabniškega vmesnika (UX/UI) in mobilne odzivnosti poveča dostopnost strani ter prispeva k večji varnosti, saj uporabnikom omogoča jasnejše razumevanje in varnejšo interakcijo s spletnimi obrazci in podatki.

Hipoteza H3 je potrjena. Izvedene UX/UI izboljšave, kot so dodajanje alternativnih opisov slik, optimizacija slik v format WebP, implementacija mehanizma Lazy Loading in izboljšave dostopnosti so povečale uporabnost in dostopnost spletnega mesta. Mobilna odzivnost je ostala na visoki ravni, hitrejše nalaganje strani in boljša preglednost pa uporabnikom omogočata učinkovitejšo in varnejšo uporabo spletnega mesta.

H4: Kibernetska varnost je ključna za zaupanje uporabnikov v digitalne storitve – primer Andromа Collies potrjuje, da tudi manjša organizacija potrebuje učinkovite varnostne prakse, saj so tveganja kibernetskih napadov prisotna ne glede na velikost sistema.

Hipoteza H4 je potrjena. Raziskava je pokazala, da tudi manjša organizacija potrebuje ustrezno raven kibernetske zaščite. Implementirani varnostni mehanizmi povečujejo zaščito spletnega mesta, zmanjšujejo možnost zlorab in prispevajo k večjemu zaupanju uporabnikov. Rezultati potrjujejo, da velikost organizacije ne zmanjšuje potrebe po izvajanju sodobnih varnostnih praks.

9 SKLEP

Diplomsko delo je obravnavalo področje kibernetske varnosti in uporabniške izkušnje spletne strani Andromа Collies. Namen raziskave je bil analizirati trenutno stanje spletnega mesta, prepoznati morebitne varnostne in uporabniške pomanjkljivosti ter na podlagi ugotovitev izvesti izboljšave, ki bi povečale raven varnosti, dostopnosti in uporabnosti spletne strani.

V teoretičnem delu so bili predstavljeni temeljni pojmi kibernetske varnosti, najpogostejše ranljivosti spletnih aplikacij, priporočila organizacije OWASP ter osnovna načela uporabniške izkušnje (UX) in uporabniškega vmesnika (UI). Posebna pozornost je bila namenjena povezavi med varnostjo in uporabnostjo, saj sodobne spletne aplikacije zahtevajo ustrezno ravnovesje med učinkovito zaščito in prijazno uporabniško izkušnjo.

V praktičnem delu je bila izvedena analiza spletne strani Andromа Collies z uporabo specializiranih orodij Mozilla Observatory, Qualys SSL Labs in Google Lighthouse. Rezultati analize so pokazali, da spletna stran zagotavlja dobro osnovno raven varnosti in uporabniške izkušnje, vendar obstajajo možnosti za izboljšave predvsem na področju konfiguracije varnostnih headerjev HTTP, zaščite kontaktnega obrazca, dostopnosti spletnih vsebin in optimizacije zmogljivosti.

Na podlagi ugotovitev so bile izvedene konkretne izboljšave. Na področju kibernetske varnosti so bili implementirani varnostni headerji HTTP, izboljšana SSL/TLS konfiguracija in uvedena zaščita kontaktnega obrazca z uporabo sistema Google reCAPTCHA v3. Na področju uporabniške izkušnje so bili dodani alternativni opisi slik (ALT), izvedena optimizacija slik v format WebP, implementiran mehanizem Lazy Loading in izboljšana dostopnost spletnih vsebin. Ponovno testiranje po izvedenih izboljšavah je pokazalo izboljšanje varnostne ocene Mozilla Observatory, ohranitev najvišje ocene A+ pri SSL Labs in izboljšanje zmogljivosti spletne strani pri testiranju z orodjem Google Lighthouse. Izvedeno uporabniško testiranje je dodatno potrdilo, da uvedene izboljšave niso negativno vplivale na uporabniško izkušnjo, temveč so prispevale k večji preglednosti, hitrejšemu nalaganju vsebine in boljši dostopnosti spletnega mesta.

Raziskava je pokazala, da je mogoče z razmeroma enostavnimi in stroškovno učinkovitimi tehničnimi posegi hkrati povečati raven kibernetske varnosti in izboljšati uporabniško izkušnjo,

ne da bi pri tem negativno vplivali na uporabnost spletne strani. Diplomsko delo tako potrjuje, da kibernetska varnost ni pomembna le za velika podjetja, temveč tudi za manjše organizacije, saj spletna stran pogosto predstavlja prvi stik uporabnikov z organizacijo in pomembno vpliva na njihovo zaupanje. Prikazan postopek analize, načrtovanja, implementacije in preverjanja izboljšav lahko predstavlja uporabno usmeritev drugim razvijalcem spletnih strani in manjšim organizacijam, ki želijo izboljšati varnost, dostopnost in uporabniško izkušnjo svojih spletnih mest brez večjih finančnih ali tehničnih posegov. Diplomsko delo hkrati poudarja pomen povezovanja področij kibernetske varnosti in uporabniške izkušnje, saj učinkovita zaščita spletnih aplikacij ne sme zmanjševati njihove uporabnosti, temveč mora prispevati k večjemu zaupanju uporabnikov in višji kakovosti digitalnih storitev.

Kljub izvedenim izboljšavam ostajajo možnosti za nadaljnji razvoj spletne strani Andromа Collies. Med pomembnejše nadaljnje aktivnosti sodijo uvedba celovite Content Security Policy (CSP), dodatna optimizacija dostopnosti v skladu z najnovejšimi smernicami WCAG, redno izvajanje varnostnih pregledov ter sprotno posodabljanje programske opreme in vtičnikov. Na področju uporabniške izkušnje bi bilo mogoče razmisliti o uvedbi funkcije iskanja po vsebini, izboljšani navigaciji z uporabo breadcrumb povezav, dodatni optimizaciji za mobilne naprave in nadaljnji optimizaciji hitrosti nalaganja večpredstavnostnih vsebin. Ker se področje kibernetske varnosti nenehno razvija, sta redno spremljanje novih varnostnih priporočil in vzdrževanje spletnega mesta ključnega pomena za zagotavljanje dolgoročno varne, dostopne in kakovostne spletne predstavitve.

Na podlagi izvedene raziskave je mogoče zaključiti, da so bili zastavljeni cilji diplomskega dela doseženi, raziskovalna vprašanja uspešno odgovorjena, postavljene hipoteze pa potrjene. Ugotovitve predstavljajo uporabno osnovo za nadaljnji razvoj spletne strani Andromа Collies ter lahko služijo kot primer dobre prakse tudi drugim manjšim organizacijam, ki želijo izboljšati varnost in kakovost svojih spletnih predstavitev.

10 VIRI IN LITERATURA

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).* Official Journal of the European Union.

Google. (2024). *Lighthouse*. Pridobljeno iz https://developer.chrome.com/docs/lighthouse

Grgić, M. (2019). *Kibernetska varnost: Sodobni izzivi in prakse.* Ljubljana: Fakulteta za računalništvo in informatiko.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.* ISO.

Krug, S. (2014). *Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability.* Berkeley, CA: New Riders.

Mozilla. (2024). *Mozilla Observatory*. Pridobljeno s https://observatory.mozilla.org

Nielsen Norman Group. (2024). *10 Usability Heuristics for User Interface Design*. Pridobljeno iz https://www.nngroup.com/articles/ten-usability-heuristics

Nielsen, J. (1994). *Usability Engineering.* San Francisco: Morgan Kaufmann.

Norman, D. A. (2013). *The Design of Everyday Things.* New York: Basic Books.

Open Web Application Security Project. (2021). *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. Pridobljeno s https://owasp.org/Top10

OWASP Foundation. (2024). *Cross Site Scripting Prevention Cheat Sheet*. Pridobljeno iz https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

OWASP Foundation. (2024). *Cross-Site Request Forgery Prevention Cheat Sheet*. Pridobljeno iz https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

Qualys SSL Labs. (2024). *SSL Server Test*. Pridobljeno s https://www.ssllabs.com/ssltest/

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2017). *Designing the User Interface: Strategies for Effective Human-Computer Interaction.* Boston: Pearson.

W3C Web Accessibility Initiative. (2018). *Web Content Accessibility Guidelines (WCAG) 2.1*. Pridobljeno iz https://www.w3.org/TR/WCAG21/

WordPress Foundation. (2024). *WordPress Security*. Pridobljeno s https://wordpress.org/about/security/

World Wide Web Consortium. (2024). *Content Security Policy Level 3*. Pridobljeno s https://www.w3.org/TR/CSP3/