Icon

Description automatically generated

A picture containing object, clock

Description automatically generated

**Izvještaj o provedenom postupku ispitivanja sigurnosti: *{nazivAPK}***

|  |  |
| --- | --- |
| Datum | {kraj} |
| Verzija | 1.0. |

|  |  |  |
| --- | --- | --- |
| Osnovne informacije | | |
| Naziv dokumenta | {nazivAPK} | |
| Autor | {osoba} | |
| Sažetak dokumenta | Izvještaj o provedenom sigurnosnom testiranju „ručni opis sustava“ | |
| Verzija | 1.0. | Datum verzije:{kraj} |

POVIJEST PROMJENA

|  |  |  |  |
| --- | --- | --- | --- |
| Verzija | Datum | Autor | Opis promjene |
| 1.0 | {kraj} | {osoba} | Inicijalna verzija dokumenta |

Sadržaj

[1 Pojmovnik 3](#_Toc453585229)

[2 Uvod 4](#_Toc8301495)

[2.1 Način korištenja ovog izvještaja 5](#_Toc2025139131)

[2.2 Podaci o ispitivanju 5](#_Toc2116069551)

[2.3 Korišteni alati 5](#_Toc1683537562)

[2.4 Vrste provedenih ispitivanja 6](#_Toc941904858)

[2.4.1 Penetracijsko testiranje 6](#_Toc45883441)

[2.4.2 Ispitivanje sigurnosti frontend-a sustava 6](#_Toc1868114624)

[2.4.3 Ispitivanje sigurnosti backend-a sustava 6](#_Toc613776679)

[2.4.4 Pregled sigurnosti koda 7](#_Toc869906263)

[2.5 Ozbiljnost ranjivosti 7](#_Toc454368088)

[3 Otkrivene ranjivosti 8](#_Toc1772598770)

[4 Detaljni rezultati 9](#_Toc2036109084)

[4.1 Ranjivosti visoke razine 10](#_Toc1679522043)

[4.2 Ranjivosti srednje razine 10](#_Toc2030637457)

[5 Zaključak 11](#_Toc709010998)

[6 Popis tablica 11](#_Toc776360727)

# Pojmovnik

**Black box penteration test** – je vrsta sigurnosnog testiranja u kojem osoba koja provodi testiranje dobiva samo osnovne ili nikakve informacije osim imena mete nad kojom će se provesti testiranje.

**CSRF (cross-site request forgery)** - poznat pod imenom napad jednog klika (eng. one-click attack ili session riding), je tip maliciozne metode iskorištavanja web stranice kada se neovlaštene komande šalju preko korisnika kojem web aplikacija vjeruje. Takve komande se mogu slati posebno napravljenim HTML image tagovima, skrivenim formama te JavaScript XMLHttpRequests zahtjevima, itd.

**Debian** - računalni operativni sustav koji koristi Linux jezgru i druge programske komponente iz GNU projekta.

**Man-in-the-middle napad (MITM)** – napad u kojem se napadač infiltrira u komunikacijski kanal između klijenta i poslužitelja, odnosno dvije točke komunikacije te stekne mogućnost analize kompletnog prometa koji se razmjenjuje, čak i ako je komunikacija kriptirana.

**Patch** – zakrpa, nadogradnja programskog koda koja u sebi sadrži ispravke prethodno pronađenih ranjivosti.

**Exploit** – način iskorištavanja određene ranjivosti.

**Penetration test** – je odobren simuliran cyber napad na računalni sustav u svrhu provjere sigurnosti dotičnog sustava.

**Severity** – označava ozbiljnost pronađene ranjivosti. Postoje 4 nivoa: Kritično, visoko, srednje, nisko.

**Vulnerability** – označava slabost računalnog sustava koju je moguće slučajno aktivirati ili namjerno iskoristiti te tako nanijeti štetu tom sustavu.

**Vulnerability scanner** - računalni program dizajniran za prikupljanje podataka o računalima, mrežama ili aplikacijama pomoću korištenja različitih tehnika skeniraju uređaje u određenom IP rasponu te na temelju prikupljenih podataka dolaze do informacija o topologiji i strukturi mreže, vrsti i tipu uređaja/aplikacije.

**White box penetration test** – vrsta sigurnosnog testiranja u kojem osoba koja provodi testiranje posjeduje sve relevantne informacije vezane za sustav nad kojim se provodi testiranje.

**Grey box penetration test** – vrsta sigurnosnog testiranja u kojem osoba koja provodi testiranje posjeduje samo određeni set informacija vezanih za sustav na kojem se provodi testiranja, no ne sve.

**XSS (cross site scripting)** – vrsta ranjivosti web aplikacije. XSS napadi omogućuju napadaču izvršavanje proizvoljnog programskog koda koji se izvršava na korisničkom računalu.

**Reverse engineering –**  proces učenja i prikupljanja informacija o sustavu za koji ne znamo na koji način točno funkcionira, te o istom nemamo dokumentaciju ili imamo djelomičnu dokumentaciju.

# Uvod

U ovom dokumentu opisan je postupak provjere sigurnosti koji provodi Nacionalni CERT. Pod pojmom servisa se u ovom dokumentu podrazumijeva sustava za „ručni opis sustava“. Razvojno okruženje na kojem se odrađuje sigurnosno testiranje, nalazi se na adresi {urlsrvr}.

Provođenje postupka ispitivanja sigurnosti aplikacije odradio je Tim za sigurnost usluga i infrastrukture pri Nacionalnom CERT-u. Navedeni postupak ima za cilj testirati ranjivosti koje mogu bitno utjecati na sigurnost same aplikacije te njenih podataka kao i korisnika koji koriste aplikaciju.

Provjera sigurnosti podrazumijeva skup automatiziranih i ručnih provjera računalnih, mrežnih sustava i aplikacija kako bi se utvrdilo postojanje sigurnosnih ranjivosti koji mogu rezultirati prestankom rada, neželjenim načinom rada ili nedostupnošću servisa. Provjera sigurnosti aplikacija podrazumijeva i provjeru njenog izvornog programskog koda.

Krajnji cilj provjere sigurnosti je unaprjeđenje servisa sa sigurnosnog stajališta – otklanjanje svih otkrivenih ranjivosti u servisu.

## Način korištenja ovog izvještaja

Krajnji korisnik ovog izvještaja treba biti autor/proizvođač servisa. Njegov je zadatak ukloniti sve navedene ranjivosti. U slučaju da se neka ranjivost ne može ukloniti radi opravdanog tehničkog ili organizacijskog razloga, potrebno je primijeniti neizravne mjere zaštite i o tome sačiniti izvještaj.

Nakon uklanjanja svih navedenih ranjivosti, potrebno je ponoviti provjeru sigurnosti.

Ovaj ciklus ispitivanje-uklanjanje ranjivosti treba ponavljati sve dok ispitivanje više ne otkrije ni jednu ranjivost ili dok autor/proizvođač servisa ne izjavi da se preostale ranjivosti ne mogu ukloniti radi opravdanog tehničkog ili organizacijskog razloga, te poduzme izravne i neizravne mjere zaštite i o tome sačini izvještaj.

## Podaci o ispitivanju

Početka sigurnosnog testiranja: {pocetak}

Kraj sigurnosnog testiranja: {kraj}

## Korišteni alati

Specijalizirani alati za provjeru ranjivosti, računalni su programi koji korištenjem različitih tehnika pretražuju uređaje u određenom rasponu IP mreže te na temelju prikupljenih podataka dolaze do informacija o topologiji i strukturi mreže, vrsti i tipu uređaja, inačici operativnog sustava, popisu otvorenih komunikacijskih portova i sl. Prikupljenim podacima takav alat pridružuje informacije o pronađenim ranjivostima, odnosno informacije o poznatim ranjivostima vezanima za određenu vrstu i tip uređaja, inačicu operativnog sustava, određeni TCP/UDP port i sl. te generira odgovarajući izvještaj. U određenim situacijama, a s obzirom na metodologiju obavljanja provjere ranjivosti i korištene postupke, dio pronađenih ranjivosti može biti lažno pozitivan. U tablici 1, navedeni su svi korišteni alati tijekom sigurnosnog testiranja.

|  |  |  |
| --- | --- | --- |
| **Naziv alata** | **Inačica** | **Opis/svrha alata** |
| {#alati}{naziv} | {inacica} | {opis}{/alati} |

Tablica 1. Korišteni alati

## Vrste provedenih ispitivanja

### Penetracijsko testiranje

Penetracijsko testiranje vrši se u kombinaciji s automatiziranim alatima za sigurnosno testiranje i ručnim provjerama. Postupak izvođenja penetracijskog testiranja specifičan je za svaku uslugu jer ovisi o sustavu kojeg se testira te nema unaprijed definiranih scenarija ispitivanja koji se paušalno mogu primijeniti i u drugim testiranjima. Tipični scenariji penetracijskog testiranja sadrže automatizirane provjere putem vanjske i unutarnje mreže, s i bez prijave korisnika (eng. *authenticated scan*). Automatizirani alati za provjeru ispituju poznate sigurnosne propuste, ali nemaju mogućnost otkrivanja sigurnosnih nedostataka specifičnih za sustav.

Ovakvi alati nisu u stanju otkriti *Zero Day* ranjivosti koje mogu postojati u testiranom sustavu. Rezultati dobiveni korištenjem automatiziranih alata ručno se provjeravaju kako bi se rezultati potvrdili ili na drugi način isključili lažno pozitivni rezultati. Ručno provjeravanje rezultata često je dugotrajan proces i nužna je odgovarajuća ravnoteža između uporabe automatiziranih testova i ručnih provjera.

### Ispitivanje sigurnosti *frontend-a sustava*

Ispitivanjem sigurnosti *frontend-a sustava* aplikacije ispituje se sigurnost korisničkog sučelja, a provodi se kao kombinacija automatiziranih testova i ručnog pregleda stručnjaka za ispitivanje sigurnosti informacijskih sustava.

U ovoj fazi naglasak je na sljedećem:

* otkrivanje osjetljivih podataka (podaci prikupljeni putem web sučelja koje je moguće zloupotrijebiti),
* otkrivanje web ranjivosti (XSS, CSRF, SQLI, itd.),
* upravljanje korisničkim pristupom,
* otkrivanje ranjivosti unutar web okvira (eng. *frameworka*) ili CMS-a vezan za sigurnosna ažuriranja

### Ispitivanje sigurnosti *backend*-a *sustava*

Ispitivanjem sigurnosti backend-a *sustava* provjerava se unutarnja konfiguracija aplikacije i sigurnost ostalih softverskih i mrežnih komponenti koje aplikacija koristi. Ispitivanje ovisi o vrsti aplikacije i obično se sastoji od ispitivanja sljedećih elemenata:

* web poslužitelj (Apache, nginx, IIS, itd.),
* poslužitelj baze podataka (MySQL, PostgreSQL, MSSQL, itd.),
* konfiguracijski parametri operativnog sustava,
* postavljanje sigurnosti operativnog sustava (pravila vatrozida, korisnička prava, dozvole za direktorije i datoteke, aktivni servisi, itd.),
* politika zakrpa operativnog sustava,
* druge ovisnosti o softveru (MTA, LDAP, itd.),
* mrežna sigurnost (topologija i segmentacija, pokrenute mrežne usluge)

### Pregled sigurnosti koda

Pregled sigurnosti koda idealno nadopunjuje ostale metode procjene sigurnosti. Iz perspektive metodologije koja se koristi u sigurnosnim testiranjima, ovakva metoda smatra se *white-box* testiranjem u kojoj penetracijski tester ima potpuni pristup izvornom kodu, dodatno podržan raspoloživom dokumentacijom te informacijama dobivenim od tima za razvoj softvera, itd.

Pregled sigurnosti koda najprije se provodi pomoću automatiziranih alata, a naknadno ručnim pregledom stručnjaka za ispitivanje sigurnosti informacijskih sustava. Stoga se analiza provodi u dvije faze:

* u prvoj fazi provodi se automatizirana analiza čitavog izvornog koda
* u drugoj fazi provodi se ručni pregled odabranih dijelova izvornog koda.

Rezultati vraćeni automatiziranim alatima pregledavaju se ručno kako bi se dodatno istražile i klasificirale pronađene ranjivosti te uklonili svi lažno pozitivni rezultati. Kako bi se osigurala maksimalna kvaliteta procjene, za veći projekt se radi i ručni pregled na djelomičnom izvornom kodu s naglaskom na najvažnije ili kritične dijelove.

U tablici 2 navedene su sve vrste ispitivanja koje su izvršene tijekom ispitivanja sigurnosti sustava PiXi platforme.

|  |  |  |  |
| --- | --- | --- | --- |
| **Glavne vrste ispitivanja** | **Vrsta ispitivanja** | **Provedeno za servis? (Da/Ne)** | **Opis** |
| **Analiza izvornog koda** | Automatizirana provjera izvornog koda s pregledom ranjivosti i kategorizacijom istih | {automatDaNe} | Provjera izvornog koda automatiziranim alatima  (skeneri za analizu izvornog koda). |
| Ručna provjera pronađenih problema u izvornom kodu | {rucnoDaNe} | Stručni pregled (čitanje) dijela izvornog koda identificiranog kao kritičnog ili „mogućeg kandidata”. |
| **Sigurnost** | Penetracijsko ispitivanje | {pentDaNe} | Ispitivanje sigurnosti s gledišta korisnika.  Automatizirana i ručna provjera. |
| Sigurnosni pregled  *frontend-*a | {frontDaNe} | Sigurnosno ispitivanje korisničkog sučelja.  Automatizirana i ručna provjera. |
| Sigurnosni pregled  *backend-*a | {backDaNe} | Sigurnosno ispitivanje radnog okruženja servisa. |

Tablica 2. Pregled vrsta ispitivanja prilikom sigurnosnog testiranja

## Ozbiljnost ranjivosti

**Ozbiljnost (engl. *severity*)**: Stupanj utjecaja koji otkrivena ranjivost ima na razvoj ili rad komponente ili sustava (ISTQB[[1]](#footnote-2) definicija).

U ovom je ispitivanju korišten radni okvir *Common Vulnerability Scoring System* (CVSS), inačica 3.1, za ocjenjivanje ozbiljnosti ranjivosti. Radni okvir CVSS v3.1 dodjeljuje kvantitativnu ocjenu ozbiljnosti ranjivosti u rasponu od 0 do 10, te odgovarajuću kvalitativnu ocjenu:

|  |  |
| --- | --- |
| **Kvalitativna CVSS ocjena ozbiljnosti** | **Raspon kvantitativnih CVSS ocjena ozbiljnosti** |
| Kritična (engl. *critical*) | 9.0 - 10.0 |
| Visoka (engl. *high*) | 7.0 - 8.9 |
| Srednja (engl. *medium*) | 4.0 - 6.9 |
| Niska (engl. *low*) | 0.1 - 3.9 |
| Nepostojeća (engl. *none*) | 0.0 |

Tablica 3. Common Vulnerability Scoring System

# Otkrivene ranjivosti

*Napomena:*

*Neke srodne ranjivosti su grupirane u jednu ranjivost kako bi izvještaj bio pregledniji i njihov popravak efikasniji, tako da broj i struktura ranjivosti navedenih u donjoj tablici ne prikazuju u potpunosti stanje sustava.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Vrsta ispitivanja** | **Broj ranjivosti kritične razine** | **Broj ranjivosti visoke razine** | **Broj ranjivosti srednje razine** | **Broj ranjivosti niske razine** | **Ukupan broj ranjivosti** |
| **Pregled analize izvornog koda** | {KodK} | {KodV} | {KodS} | {KodN} | - |
| **Sigurnosni pregled frontend-a** | {FrK} | {FrV} | {FrS} | {FrN} | - |
| **Sigurnosni pregled backend-a** | {BcK} | {BcV} | {BcS} | {BcN} | - |
| **Ukupno** | **{kritUk}** | **{visUk}** | **{sredUk}** | **{nisUk}** | **{sveUku}** |

Tablica 4. Brojčani prikaz otkrivenih ranjivosti

Tablica 3 prikazuje kratki pregled otkrivenih ranjivosti:

|  |  |  |
| --- | --- | --- |
| **ID** | **Ranjivost** | **Ozbiljnost** |
| {#ranjivosti}{id\_ranjivosti} | {naziv\_ranjivosti} | {ocjena\_ozbiljnosti}/10{/ranjivosti} |

Tablica 5. Pregled otkrivenih ranjivosti i ozbiljnosti

# Detaljni rezultati

## Ranjivosti kritične razine

{#ranjivostiKritična}

|  |  |
| --- | --- |
| ID | {id\_ranjivosti} |
| Ozbiljnost | {ozbiljnost\_detalji} ({ocjenaOzb}/10)  {cvss\_score}  {cvss\_link} |
| Ranjivost | **{naziv\_ranjivosti}** |
| Kategorija | **{owaspKategorija}** |

{/ranjivostiKritična}

## Ranjivosti visoke razine

{#ranjivostiVisoka}

|  |  |
| --- | --- |
| ID | {id\_ranjivosti} |
| Ozbiljnost | {ozbiljnost\_detalji} ({ocjenaOzb}/10)  {cvss\_score}  {cvss\_link} |
| Ranjivost | **{naziv\_ranjivosti}** |
| Kategorija | **{owaspKategorija}** |

{/ranjivostiVisoka}

## Ranjivosti srednje razine

{#ranjivostiSrednja}

|  |  |
| --- | --- |
| ID | 3 |
| Ozbiljnost | {ozbiljnost\_detalji} ({ocjenaOzb}/10)  {cvss\_score}  {cvss\_link} |
| Ranjivost | **{naziv\_ranjivosti}** |
| Kategorija | **{owaspKategorija}** |

{/ranjivostiSrednja}

## Ranjivosti niske razine

{#ranjivostiNiska}

|  |  |
| --- | --- |
| ID | 1 |
| Ozbiljnost | {ozbiljnost\_detalji} ({ocjenaOzb}/10)  {cvss\_score}  {cvss\_link} |
| Ranjivost | **{naziv\_ranjivosti}** |
| Kategorija | **{owaspKategorija}** |

{/ranjivostiNiska}

# Zaključak

Ručno pisanje

# Popis tablica

Ručno generiranje

1. ISTQB = International Software Testing Qualifications Board [www.istqb.org] [↑](#footnote-ref-2)