LABORATORIJSKE VJEŽBE

SIGURNOSNO TESTIRANJE APLIKACIJA

Programsko inženjerstvo | 2025/2026

ZAŠTO SIGURNOSNO TESTIRANJE?

30,000

web stranica hakira se DNEVNO

39 sek

novi napad svakih 39 sekundi

50%

aplikacija ima OWASP Top 10 ranjivost

REPUTACIJSKI RIZIK

Curenje podataka uništava povjerenje korisnika. Primjer: T-Mobile 2023 — 37M korisnika pogođeno.

FINANCIJSKI GUBICI

Prosječni trošak data breach-a: $4.45M. GDPR kazne mogu dostići 4% godišnjeg prometa.

LEGALNA ODGOVORNOST

Developeri i tvrtke su pravno odgovorni za sigurnosne propuste. DevSecOps je standard.

OWASP TOP 10 — 2025

Najkritičniji sigurnosni rizici web aplikacija

- **A01** Broken Access Control
- **A02** Security Misconfiguration
- **A03** Software Supply Chain Failures NOVO!
- **A04** Cryptographic Failures
- **A05** Injection (SQLi, XSS...)
- **A06** Insecure Design
- **A07** Authentication Failures
- **A08** Software and Data Integrity Failures
- **A09** Security Logging and Monitoring Failures
- **A10** Mishandling of Exceptions NOVO!

TOP 3 RANJIVOSTI — DETALJNO

A01:2025

Broken Access Control

Napadač pristupa resursima ili funkcijama za koje nema autorizaciju.

```
GET /api/users/678/data
// Trebao biti /users/677
```

PRIMJER:

Promjena ID-a u URL-u za pristup tuđim podacima (IDOR)

A02:2025

Security Misconfiguration

Neispravne ili zadane konfiguracije sustava i aplikacija.

```
DEBUG = True
// U produkciji!
```

PRIMJER:

Default kredencijali, verbose error poruke, nepotrebni servisi

A03:2025 — NOVO

Supply Chain Failures

Kompromitiranje kroz dependencies, build sustave ili distribuciju.

```
npm install evil-pkg
// Malicious package
```

PRIMJER:

Zaraženi npm/PyPI paketi, kompromitiran CI/CD pipeline

TIPOVI SIGURNOSNOG TESTIRANJA

SAST

Static Analysis

Statička analiza izvornog koda

Skenira source code BEZ pokretanja aplikacije. Pronalazi ranjivosti rano u SDLC-u. White-box pristup.

Alati: SonarQube, Checkmarx, Semgrep, Bandit (Python)

DAST

Dynamic Analysis

Dinamička analiza pokrenute aplikacije

Testira aplikaciju izvana dok je pokrenuta. Simulira napade kao pravi haker. Black-box pristup.

Alati: OWASP ZAP, Burp Suite, Nikto, Acunetix

IAST

Interactive

Interaktivna analiza u runtime-u

Kombinira SAST i DAST — agent unutar aplikacije analizira kod tijekom izvršavanja. Gray-box pristup.

Alati: Contrast Security, Hdiv, Seeker

OWASP ZAP

Zed Attack Proxy — Naš primarni alat za vježbe

BESPLATAN I OPEN-SOURCE

Održava ga Checkmarx (SSP). Idealan za edukaciju i profesionalne pentest zadatke.

PROXY FUNKCIONALNOST

Presreće HTTP/HTTPS promet između browsera i servera. Omogućuje modifikaciju requestova.

AUTOMATED SCANNER

Active Scan detektira 1000+ ranjivosti. Podržava OWASP Top 10, SQL Injection, XSS...

CI/CD INTEGRACIJA

YAML automation framework za DevSecOps. Jenkins, GitHub Actions, GitLab CI...

KLJUČNE ZNAČAJKE

- **Spider** — automatsko pronalaženje URL-ova
- **Fuzzer** — testiranje s malicioznim inputima
- **Forced Browse** — otkrivanje skrivenih resursa
- **API Support** — OpenAPI, GraphQL, SOAP
- **Add-ons** — proširenja iz ZAP Marketplacea

```
$ docker run -t zaproxy/zap-stable zap-baseline.py -t
https://target.com
```

OSTALI ALATI ZA TESTIRANJE

Burp Suite [KOMERCIJALNI]

Industrijski standard za manualni pentest. Snažniji scanner, bolje session handling. Pro verzija ~$449/god. Koristi ga 52,000+ profesionalaca.

Nikto [OPEN SOURCE]

Web server scanner. Brzo pronalazi zastarjele verzije, misconfiguracije i poznate ranjivosti servera. 7,000+ testova u bazi.

Acunetix [KOMERCIJALNI]

Enterprise DAST s 99.98% accuracy (Proof-Based Scanning). Automatski skenira i generira izvještaje. Odličan za compliance.

Nmap + NSE [OPEN SOURCE]

Network scanner s vulnerability scripts (600+ NSE scripts). Port scanning, service detection, OS fingerprinting.

SQLMap [OPEN SOURCE]

Specijalist za SQL Injection. Automatski detektira i exploita SQLi ranjivosti. Podržava MySQL, PostgreSQL, MSSQL, Oracle...

Nuclei [OPEN SOURCE]

Template-based scanner (ProjectDiscovery). Brzo skeniranje s YAML templateima. 8000+ community templates za poznate CVE-ove.

FRONTEND: DEPENDENCY SECURITY

1 od 35 npm paketa sadrži poznatu ranjivost — Shai Hulud napad 2025.

npm audit [UGRAĐEN]

Ugrađen u npm CLI. Skenira package-lock.json za poznate ranjivosti. Brz i besplatan, ali ograničen na npm bazu.

```
$ npm audit --json
```

Snyk [FREEMIUM]

Najopsežnija baza ranjivosti. SAST + SCA. Auto-fix PRovi. IDE integracija (VS Code). Podržava JS, Python, Java, Go...

```
$ snyk test --severity-threshold=high
```

Socket.dev [FREEMIUM]

Specijalist za supply chain napade. Detektira maliciozni kod, obfuskaciju, network pozive u paketima. GitHub app integracija.

```
$ npx socket-security scan
```

npq [OPEN SOURCE]

Zamjena za npm install. Automatski auditira paket PRIJE instalacije. Provjerava typosquatting, maintainere, scripts...

```
$ npq install axios
```

ESLint Security Plugins [OPEN SOURCE]

eslint-plugin-security detektira eval(), prototype pollution, path traversal. eslint-plugin-no-secrets pronalazi hardkodirane tajne.

Semgrep [OPEN SOURCE]

SAST s YAML pravilima. Ultra brz u CI/CD. Community registry s tisućama pravila za React, Express, Next.js...

FRONTEND: BROWSER SECURITY TOOLS

Alati ugrađeni u browser za testiranje sigurnosti klijentske strane

Chrome DevTools Security Tab

Prikazuje HTTPS status, certifikate, mixed content upozorenja. Network tab pokazuje CSP headere i sigurnosne politike.

Google Lighthouse

Best Practices audit: provjerava CSP, HTTPS, deprecated APIs, XSS zaštitu (Trusted Types). Ocjenjuje sigurnosnu higienu.

CSP Evaluator (Google)

Online alat za analizu Content Security Policy. Pronalazi bypass ranjivosti, unsafe-inline, preširoke dozvole.

csp-evaluator.withgoogle.com

RetireJS

Browser ekstenzija i CLI. Skenira web stranice za zastarjele JavaScript biblioteke s poznatim ranjivostima (jQuery, Angular, React...).

Security Headers Scanner

Provjerava sigurnosne HTTP headere: CSP, X-Frame-Options, HSTS, X-Content-Type-Options. Daje ocjenu A-F.

securityheaders.com

DOMPurify Playground

Testira XSS sanitizaciju. DOMPurify je de facto standard za čišćenje HTML-a od malicioznog koda u JS aplikacijama.

CSP Header Primjer

```
Content-Security-Policy: default-src 'self'; script-src 'self' 'nonce-xyz'
```

FUN FACTS I REAL-WORLD STORIES

$2M+

zaradio 19-godišnjak na HackerOne bug bountyju

POZNATI HACKOVI POPULARNIH APLIKACIJA

TikTok 2022

XSS ranjivost omogućila preuzimanje bilo kojeg accounta

Instagram 2024

IDOR bug otkrio privatne podatke 10M+ korisnika

Spotify 2023

API misconfiguration exposed user playlists

KARIJERNE PRILIKE

Security inženjeri zarađuju 30-50% više od prosječnih developera. Globalni manjak od 3.5M security stručnjaka do 2025.

CTF NATJECANJA

Capture The Flag — gamificirano učenje hackinga. Platforme: HackTheBox, TryHackMe, PicoCTF. Odlično za portfolio!

90%

napada koristi poznate ranjivosti s dostupnim patchem

277 dana

prosječno vrijeme za otkrivanje data breach-a

#1

cybersecurity je najtraženija IT vještina 2025.

Izvori: HackerOne, IBM Security, LinkedIn Jobs Report 2025

ZAKLJUČAK I RESURSI

KLJUČNE PORUKE

1. Sigurnost nije opcija — mora biti dio svakog koraka razvoja (DevSecOps)
2. OWASP Top 10 je vaš checklist — poznajte ga napamet
3. Alati poput ZAP-a i Burp Suite su essential skills za svakog developera
4. Supply chain napadi su nova realnost — provjeravajte dependencies!
5. Security je karijera s odličnim perspektivama — investirajte u sebe!

RESURSI ZA UČENJE

OWASP Resources
owasp.org — Top 10, Cheat Sheets, Testing Guide

PortSwigger Academy
portswigger.net/web-security — besplatni labovi

TryHackMe / HackTheBox
Praktični CTF izazovi za sve razine

OWASP Juice Shop
Namjerno ranjiva app za vježbanje

```
$ docker run -p 3000:3000 bkimminich/juice-shop
```

PROJEKTNI ZADATAK

ISPRAVLJANJE SIGURNOSNIH RANJIVOSTI APLIKACIJE (I8 – 1 bod)

1. Pomoću OWASP ZAP ili sličnih alata skenirati aplikaciju u svom dijelu koda i detektirati ranjivosti
2. Kreirati „screenshot” popisa ranjivosti
3. Ispraviti sve najznačajnije ranjivosti (npr. označene crvenom, narančastom i žutom bojom)
4. Kreirati „screenshot” nakon što su ranjivosti ispravljene