Sveučilište u Zagrebu
Fakultet organizacije i informatike

FUZZING AGENCY

Izradili:
Marin Grabovac, bacc.inf
Jan Pobi, bacc.inf.
Lucija Polak, bacc.inf.

Mentor:
Izv. prof. dr. sc., Igor Tomičić

SADRŽAJ

Fuzzing?

Fuzzing je tehnika za

- etičko hakiranje
- testiranje sigurnosti
- šalju nasumični i neočekivani ulazni podaci

Virtualno okruženje

Kreiranje VM

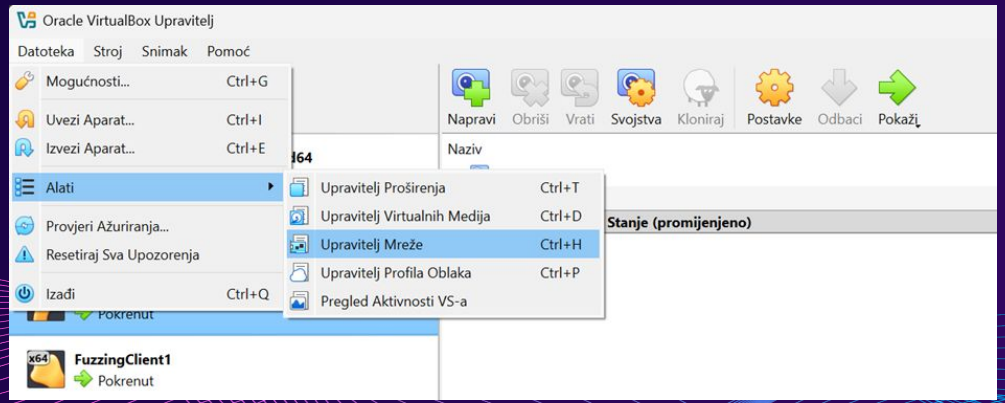
Instalacija aplikacija i biblioteka

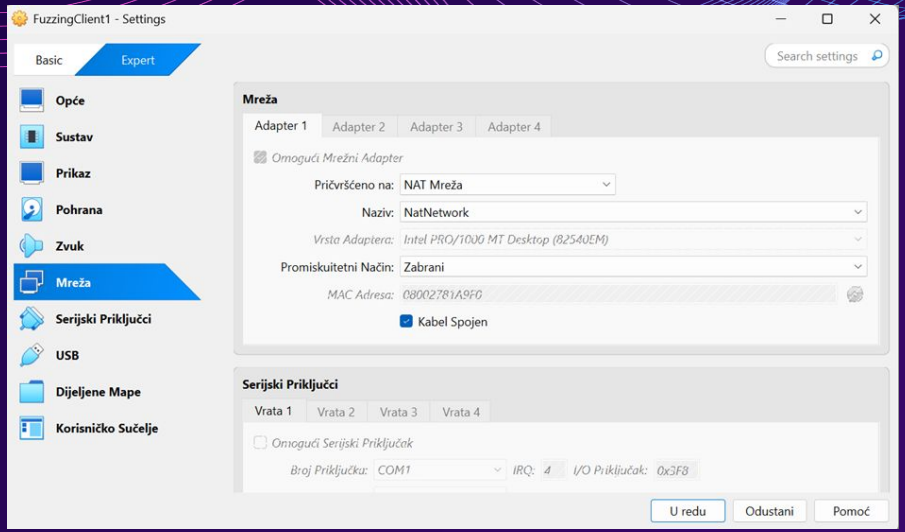
Kreiranje VM-ova

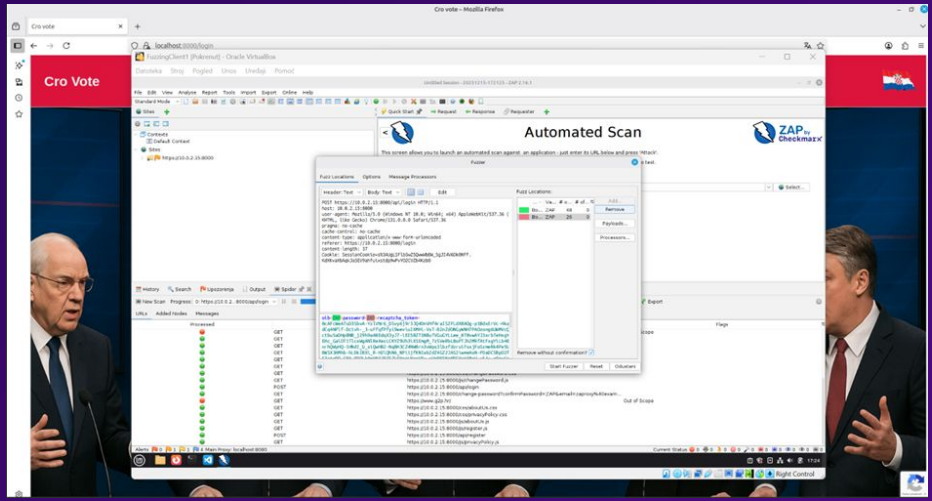
Kreiranje NAT mreže

Povezivanje VM na NAT mrežu

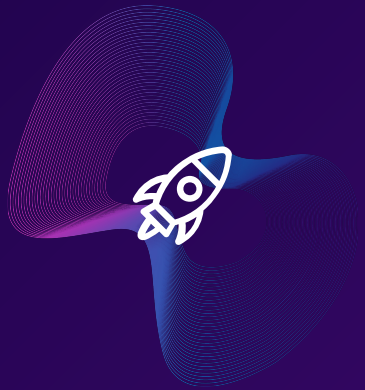
Fuzzing


Oracle VirtualBox Upravitelj
Datoteka
Stroj
Snimak
Pomoć
Mogućnosti... Ctrl+G
Uvezi Aparat... Ctrl+I
Izvezi Aparat... Ctrl+E
Alati
Provjeri Ažuriranja...
Resetiraj Sva Upozorenja
Izađi Ctrl+Q
Upravitelj Proširenja Ctrl+T
Upravitelj Virtualnih Medija Ctrl+D
Upravitelj Mreže Ctrl+H
Upravitelj Profila Oblaka Ctrl+P
Pregled Aktivnosti VS-a
Napravi
Obriši
Vrati
Svojstva
Kloniraj
Postavke
Odbaci
Pokaži
Naziv
Stanje (promijenjeno)
Pokrenut
FuzzingClient1
Pokrenut


FuzzingClient1 - Settings
Basic
Expert
Search settings
Opće
Sustav
Prikaz
Pohrana
Zvuk
Mreža
Serijski Priključci
USB
Dijeljene Mape
Korisničko Sučelje
Mreža
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Omogući Mrežni Adapter
Pričvršćeno na: NAT Mreža
Naziv: NatNetwork
Vrsta Adaptera: Intel PRO/1000 MT Desktop (82540EM)
Promiskuitetni Način: Zabrani
MAC Adresa: 080027B1A9F0
Kabel Spojen
Serijski Priključci
Vrata 1
Vrata 2
Vrata 3
Vrata 4
Omogući Serijski Priključak
Broj Priključka: COM1
IRQ: 4
I/O Priključak: 0x3F8
U redu
Odustani
Pomoć


Cro vote - Mozilla Firefox
Cro Vote
Automated Scan
ZAP by Checkmarx

Mete testiranja



Parseri u C jeziku

Razne datoteke parseri

Web aplikacija

Prošlogodišnji SIS projekt za secure online voting

Fuzzing tehnike i alati

AFL++ (CGF)

Praćenje putanja

Scapy / Custom Python (Generacijski Fuzzing)

Generacija uputa po strukturi

Web fuzzing (Jenkins i OWASP ZAP)

- Jenkins orkestrira pipeline
- ZAP automatizira pozivanje API-ja

Radamsa (Mutacijski Fuzzing)

Black-box sa seed podacima

Grammar Fuzzing (na Python Targetima)

Koristi formalna pravila jezika za spamanje unosa.

Automatizacija fuzzing procesa

Fuzzing: Korišten je AFL++ i Radamsa za pronalaženje grešaka u C kodu.

Ranjivosti: Otkrivene su kritične ranjivosti poput Buffer Overflowa i DoS rizika.

CI/CD: Jenkins je automatizirao pokretanje sigurnosnih provjera.

Sigurnost: OWASP ZAP (DAST) je integriran za automatsko blokiranje nesigurnog koda ("Shift Left").

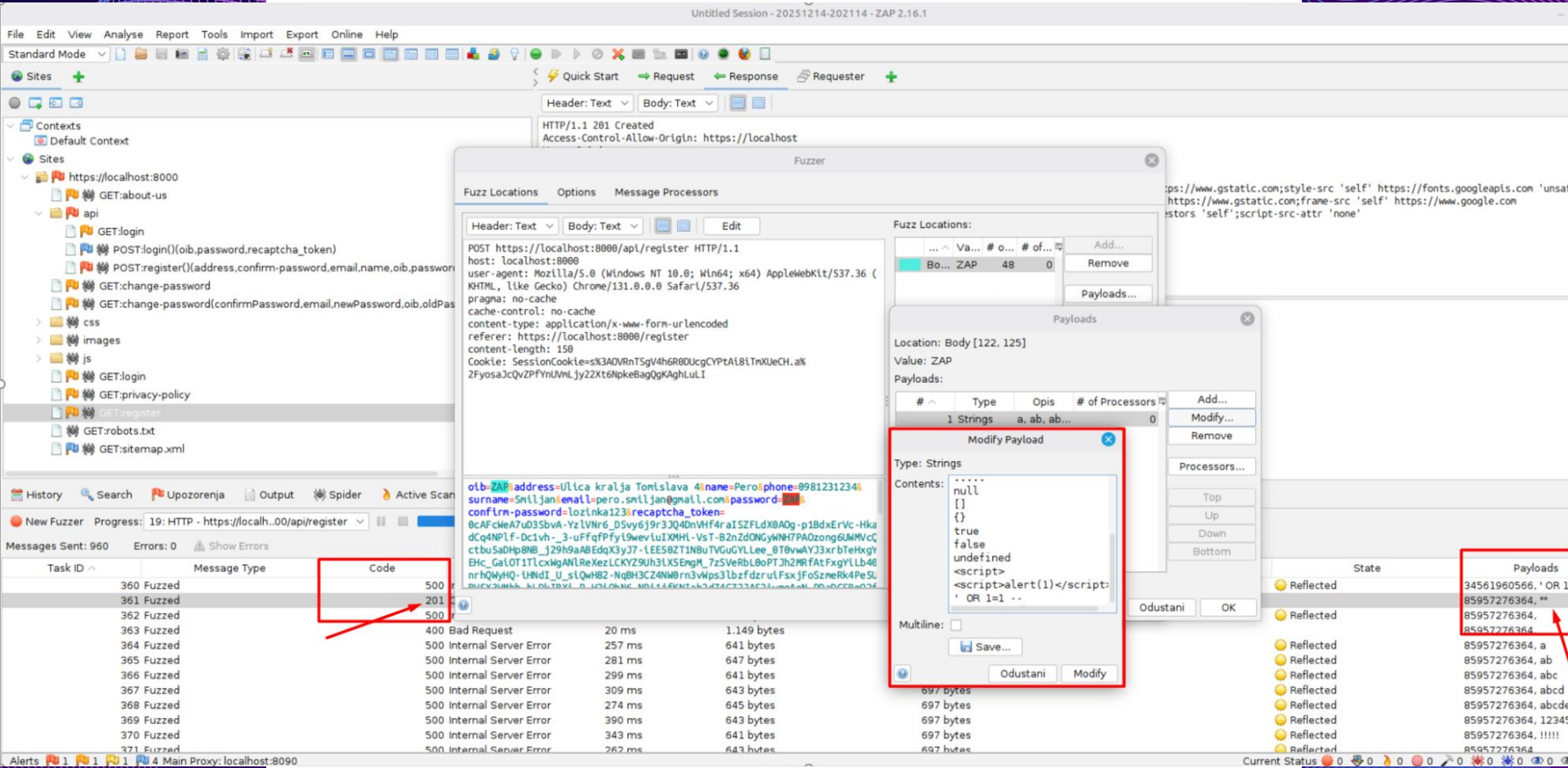
Testni scenariji za web aplikaciju - Login

Scenarij	**Unos**	**Očekivani rezultat**
Brute-force	Višestruki uzastopni pokušaji prijave	Privremeno zaključavanje prijave
Unicode i encoding	Unicode znakovi u polje za OIB, npr: 𝒜ℬ𝒞	Sigurno odbijanje zahtjeva
SQL/XSS ulaz	SQL i specijali znakovi u polje za OIB	Odbijanje zahtjeva bez rušenja
Neispravan reCAPTCHA	Token koji nije valjan ili nedostaje	Odbijanje zahtjeva

Testni scenariji za web aplikaciju - Register

Scenarij	**Unos**	**Očekivani rezultat**
Obavezna polja	Prazna ili izostavljena polja za unos	Odbijanje mogućnosti registracije
SQL Injection	SQL-like payload u polja za OIB ili email	Odbijanje zahtjeva bez utjecaja na bazu
XSS	JS payout u tekstualna polja	Ne izvršava se skripta, zahtjev odbijen
Boundary i format	Jako dugi ili pre kratki unos u polja za OIB ili npr broj mobitela	Odbijanje registracije uz stabilan rad

OIB: Adresa:



Već imaš račun? Prijavi se.

Rezultati - mreža računala

reCAPTCHA

Task ID	Message Type	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Req. Header	Size Req. Body	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	Original	Mon Dec 15 17:22:04 CET 2025	POST	https://10.0.2.15:8000/api/login	401	Unauthorized	88	452	37	1150	68			[]
4	Fuzzed	Mon Dec 15 17:39:57 CET 2025	POST	https://10.0.2.15:8000/api/login	400	Bad Request	756	454	1602	1149	35			[48425966747, lozinka123]
1	Fuzzed	Mon Dec 15 17:39:57 CET 2025	POST	https://10.0.2.15:8000/api/login	400	Bad Request	781	454	1593	1153	35			[15082092164, .]
3	Fuzzed	Mon Dec 15 17:39:57 CET 2025	POST	https://10.0.2.15:8000/api/login	400	Bad Request	783	454	1593	1155	35			[48425966747, .]
2	Fuzzed	Mon Dec 15 17:39:57 CET 2025	POST	https://10.0.2.15:8000/api/login	400	Bad Request	791	454	1602	1151	35			[15082092164, lozinka123]

bez reCAPTCHA

Task ID	Message Type	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Req. Header	Size Req. Body	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	Original	Mon Dec 15 17:22:04 CET 2025	POST	https://10.0.2.15:8000/api/login	401	Unauthorized	88	452	37	1150	68			[]
1	Fuzzed	Mon Dec 15 17:42:50 CET 2025	POST	https://10.0.2.15:8000/api/login	401	Unauthorized	226	454	1602	1150	68			[15082092164, lozinka123]
2	Fuzzed	Mon Dec 15 17:42:50 CET 2025	POST	https://10.0.2.15:8000/api/login	401	Unauthorized	253	454	1593	1158	68			[15082092164, .]
4	Fuzzed	Mon Dec 15 17:42:50 CET 2025	POST	https://10.0.2.15:8000/api/login	401	Unauthorized	318	454	1593	1154	68			[48425966747, .]
3	Fuzzed	Mon Dec 15 17:42:50 CET 2025	POST	https://10.0.2.15:8000/api/login	200	OK	372	454	1602	1144	31			[48425966747, lozinka123]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TLSv1.2	106	Application Data
2	0.000002	10.0.2.4	10.0.2.15	TLSv1.2	106	Application Data
3	0.000003	10.0.2.4	10.0.2.15	TLSv1.2	106	Application Data
4	0.000003	10.0.2.4	10.0.2.15	TLSv1.2	106	Application Data
5	0.000083	10.0.2.15	10.0.2.4	TCP	54	8000 → 51974 [RST] Seq=1 Win=0 Len=0
6	0.000229	10.0.2.15	10.0.2.4	TCP	54	8000 → 52014 [RST] Seq=1 Win=0 Len=0
7	0.000331	10.0.2.15	10.0.2.4	TCP	54	8000 → 52014 [RST] Seq=1 Win=0 Len=0
8	0.000422	10.0.2.15	10.0.2.4	TCP	54	8000 → 51974 [RST] Seq=1 Win=0 Len=0
9	0.004743	10.0.2.4	10.0.2.15	TLSv1.2	106	Application Data
10	0.004745	10.0.2.4	10.0.2.15	TLSv1.2	106	Application Data
11	0.004745	10.0.2.4	10.0.2.15	TCP	66	51974 → 8000 [FIN, ACK] Seq=81 Ack=1 Win=497 Len=0 TSval=2406701158 TSecr=782376104
12	0.004814	10.0.2.15	10.0.2.4	TCP	54	8000 → 51972 [RST] Seq=1 Win=0 Len=0
13	0.005003	10.0.2.15	10.0.2.4	TCP	54	8000 → 51972 [RST] Seq=1 Win=0 Len=0
14	0.005105	10.0.2.15	10.0.2.4	TCP	54	8000 → 51974 [RST] Seq=1 Win=0 Len=0
15	0.022719	10.0.2.4	10.0.2.15	TCP	74	58214 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2406701180 TSecr=0 WS=128
16	0.022877	10.0.2.15	10.0.2.4	TCP	74	8000 → 58214 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=782543035 TSecr=2406701180 WS=128
17	0.023413	10.0.2.4	10.0.2.15	TCP	74	58208 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2406701179 TSecr=0 WS=128
18	0.023511	10.0.2.15	10.0.2.4	TCP	74	8000 → 58208 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=782543036 TSecr=2406701179 WS=128
19	0.024146	10.0.2.4	10.0.2.15	TLSv1.2	106	Application Data
20	0.024147	10.0.2.4	10.0.2.15	TCP	66	58214 → 8000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2406701182 TSecr=782543035
21	0.024148	10.0.2.4	10.0.2.15	TLSv1.2	106	Application Data
22	0.024148	10.0.2.4	10.0.2.15	TCP	66	58208 → 8000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2406701182 TSecr=782543036
23	0.024181	10.0.2.15	10.0.2.4	TCP	54	8000 → 51998 [RST] Seq=1 Win=0 Len=0
24	0.024375	10.0.2.15	10.0.2.4	TCP	54	8000 → 51998 [RST] Seq=1 Win=0 Len=0
25	0.024908	10.0.2.4	10.0.2.15	TCP	74	58230 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2406701183 TSecr=0 WS=128
26	0.024940	10.0.2.15	10.0.2.4	TCP	74	8000 → 58230 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=782543037 TSecr=2406701183 WS=128

HVALA NA PAŽNJI