Implementing and Testing a Web Application Firewall (WAF) – praktični dio

Izradili: Filip Drvoderić, Matija Žnidarić, Luka Videc, Borna Šoštar

Kolegij: Sigurnost informacijskih sustava

Akademska godina: 2025./2026.

Sadržaj

Cilj projekta

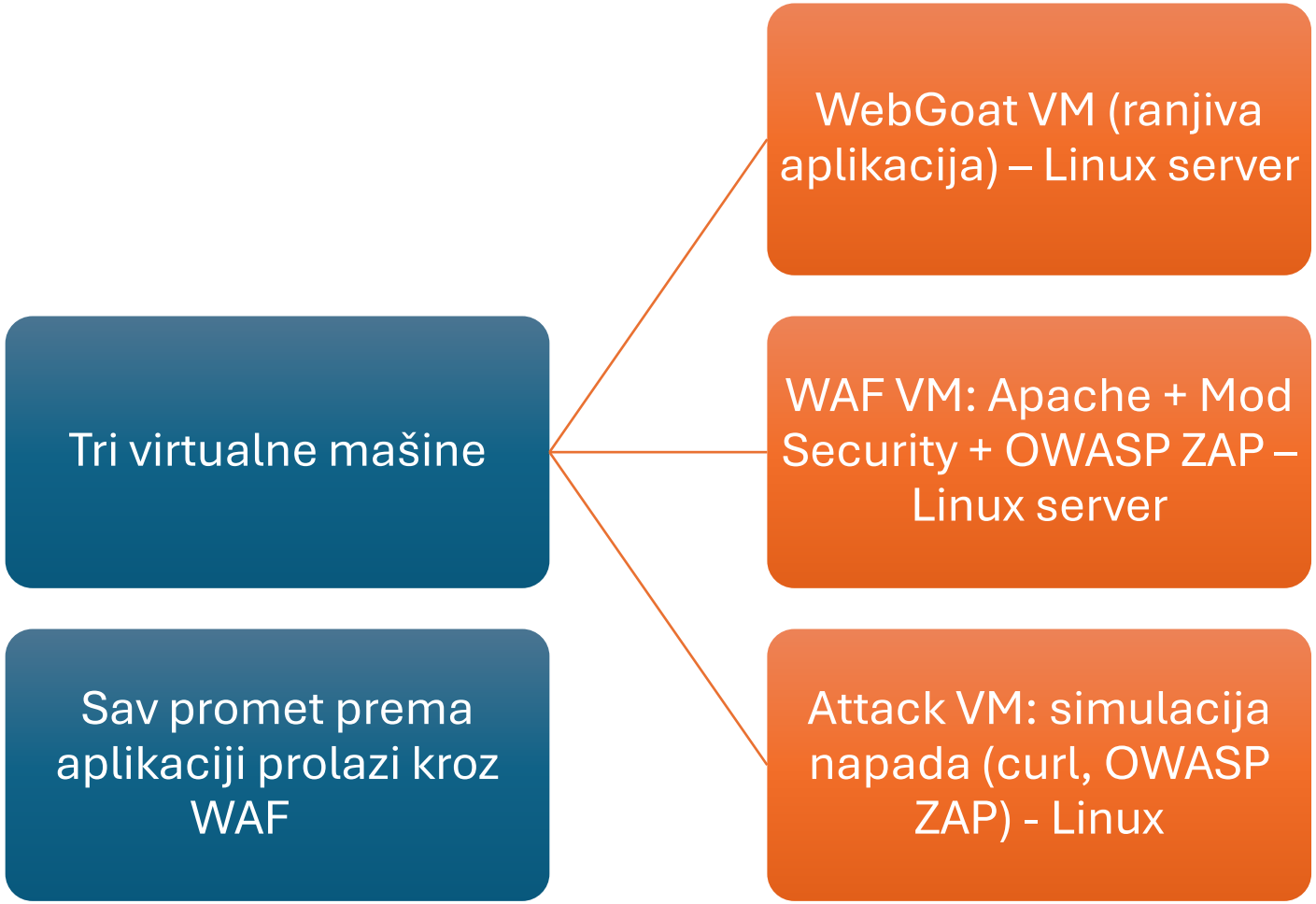
Implementirati WAF koristeći Apache + ModSecurity + OWASP CRS

Postaviti izolirano testno okruženje

Testirati reakciju WAF-a na zlonamjerne zahtjeve

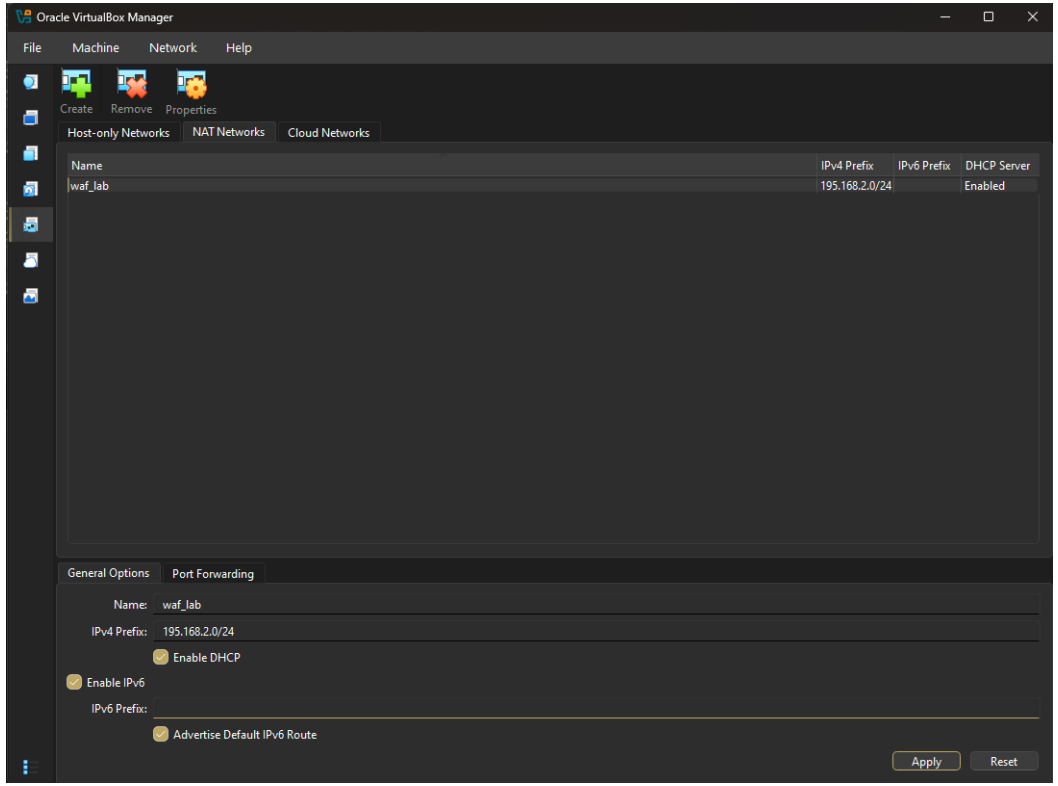
Usporediti ponašanje sustava sa i bez WAF-a

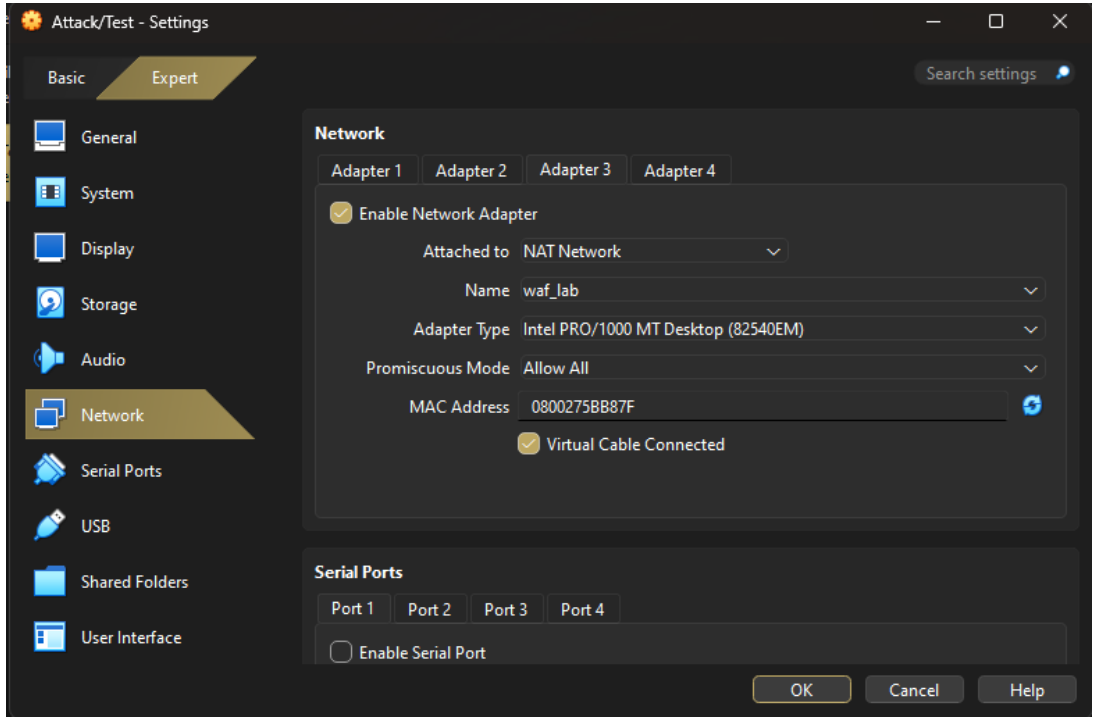
Arhitektura sustava



Mrežna konfiguracija

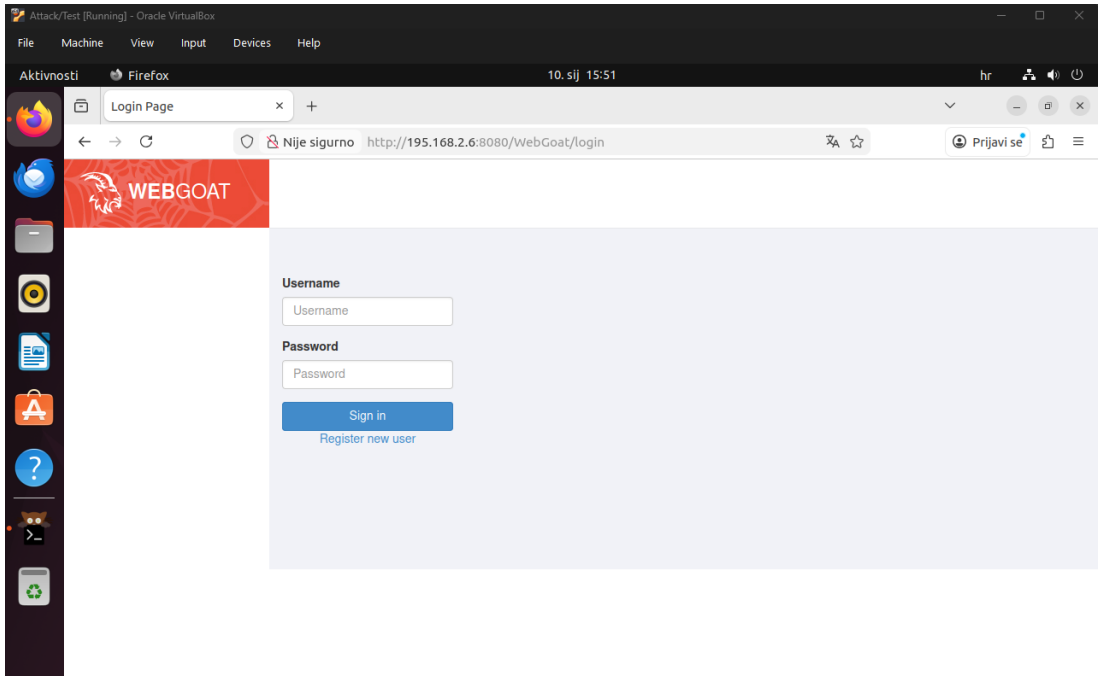
- Nat Network
- Subnet: 195.168.2.0/24
- DHCP omogućen
- Sve VM u istoj mreži





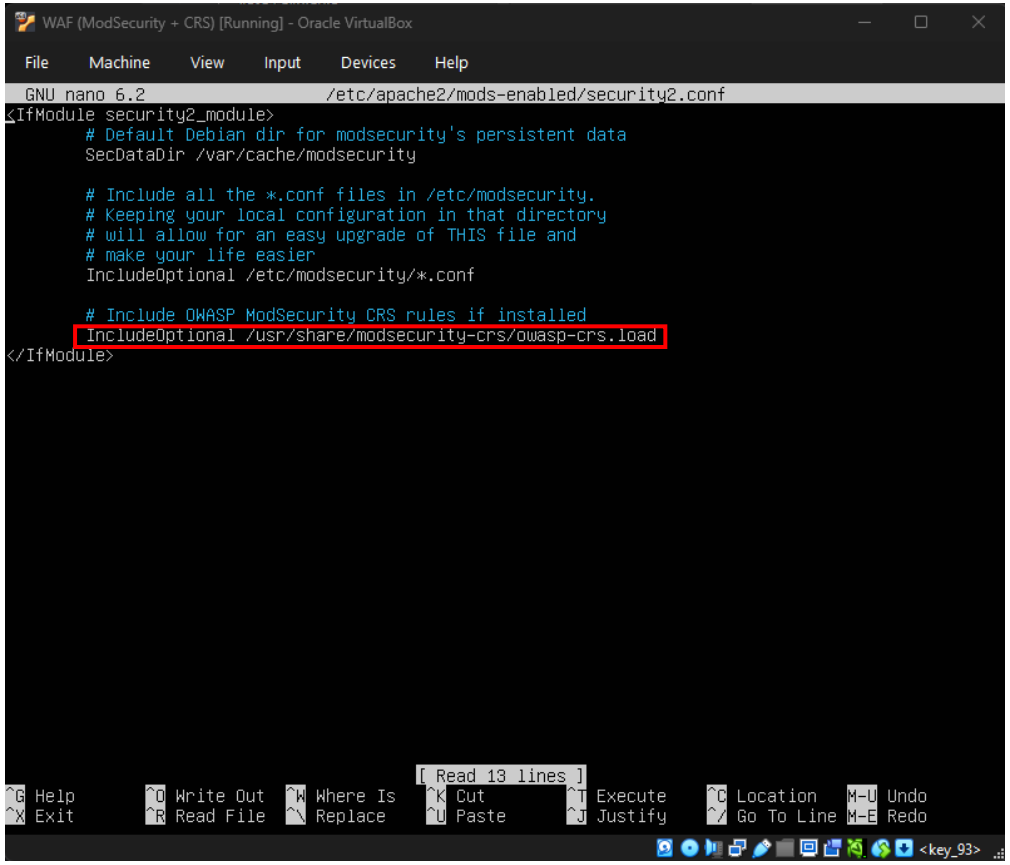
WebGoat aplikacija

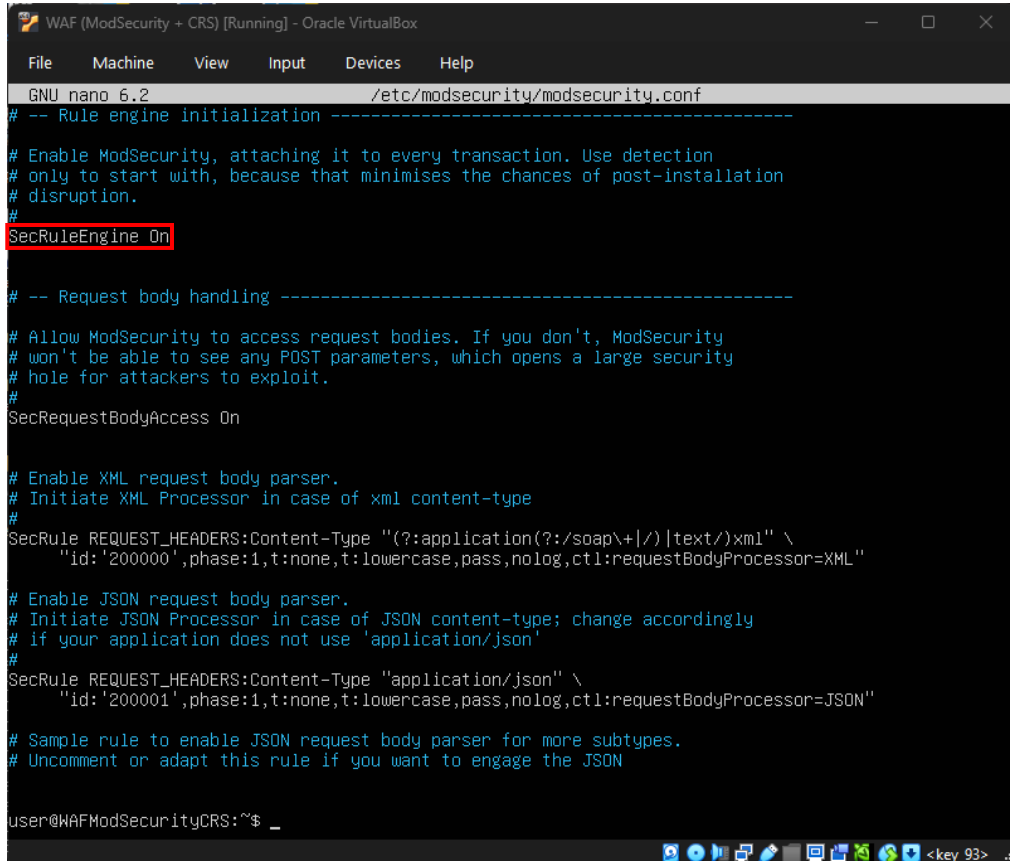
- Testna aplikacija
- Namjerno ranjiva
- Kod za pokretanje: java -jar webgoat-server-8.2.2.jar --server.address=0.0.0.0 --server.port=8080
- Dostupna samo unutar interne mreže

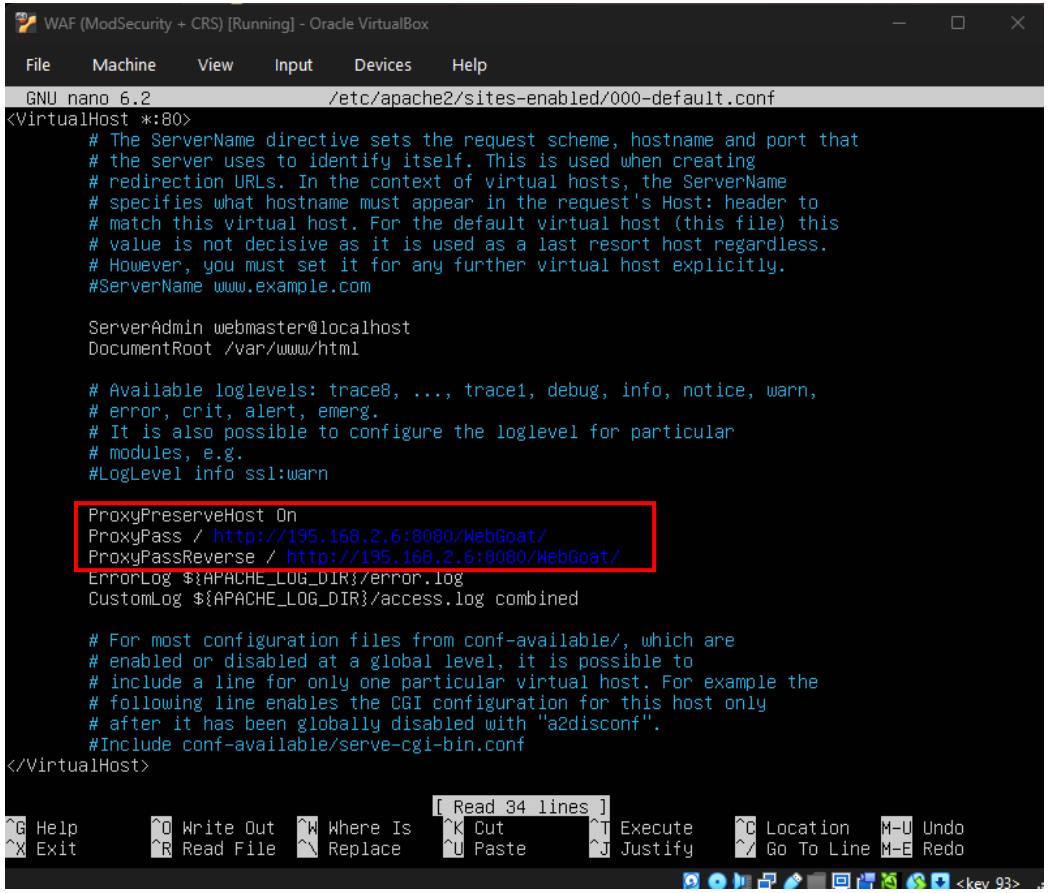


WAF konfiguracija

- Apache webserver - Kod: sudo apt install -y apache2 libapache2-mod-security2 modsecurity-crs
- ModSecurity modul - Kod: sudo cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
- OWASP Core Rule Set (CRS) -KOD: sudo nano /etc/apache2/mods-enabled/security2.conf





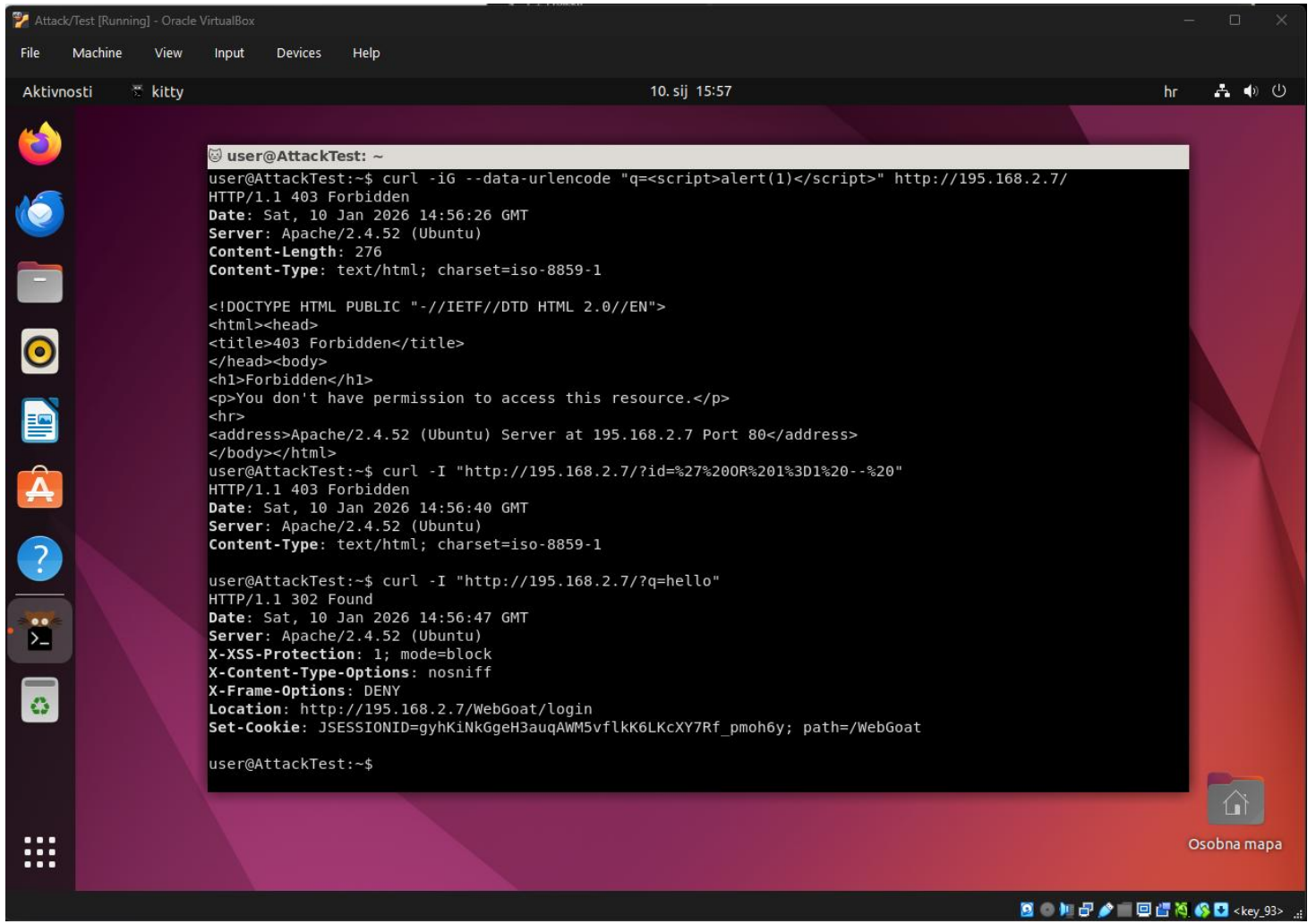


Reverse proxy

- Apache prima sve HTTP zahtjeve
- Prosljeđuje ih WebGoat aplikaciji
- Omogućuje filtriranje prometa
- Kod: sudo nano /etc/apache2/sites-enabled/000-default.conf

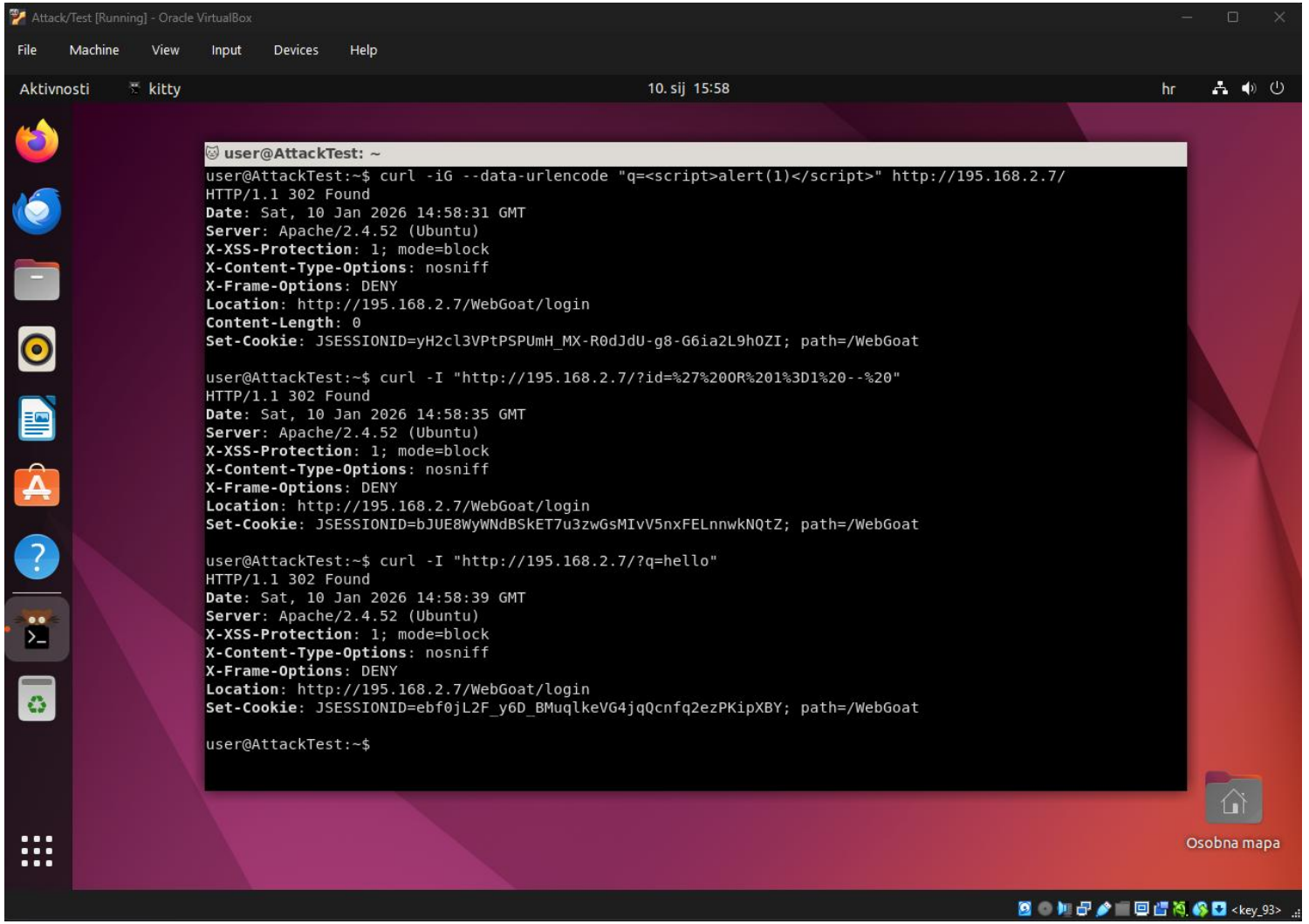
Testiranje

- Sa WAF-om
- SecRuleEngine On
- Legitimni promet dopušten
- Blokira XSS i SQL Injection



Testiranje

- Bez WAF-a
- SecRuleEngine Off
- Prolaze svi zahtjevi
- Aplikacija nije zaštićena



Zaključak

- WAF uspješno detektira i blokira napade
- OWASP CRS pruža osnovnu, ali učinkovitu zaštitu
- Sustav se može dodatno prilagoditi smanjenjem false positive-a

- Usporedba Sa WAF-om i bez WAF-a

Sa WAF-om	Bez WAF-a
XSS i SQL injection blokiran	XSS i SQL injection prolazi
Aktivna zaštita	Nema filtriranja
Zaštićen pristup	Ranjiva aplikacija

Literatura

- OpenJDK(bez dat.) *OpenJDK*. Preuzeto 27.12.2025. s https://openjdk.org/
- OWASP (bez dat.) OWASP WebGoat. Preuzeto 27.12.2025. s https://owasp.org/www-project-webgoat/
- WebGoat (bez dat.) WebGoat: A deliberately insecure Web Application. Preuzeto 27.12.2025. s https://github.com/WebGoat/WebGoat
- CRS (bez dat.) OWASP CRS Project. Preuzeto 27.12.2025 s https://coreruleset.org/
- OWASP ModSecurity (bez dat.) ModSecurity documentation. Preuzeto 27.12.2025. s https://github.com/owasp-modsecurity/ModSecurity/wiki
- Apache (bez dat.) Apache HTTP Server Documentation. Preuzeto 27.12.2025. s https://httpd.apache.org/docs/

Literatura

- Apache (bez dat.) Apache Module mod_proxy. Preuzeto 10.01.2026. s https://httpd.apache.org/docs/current/mod/mod_proxy.html
- Apache (bez dat.) Apache Module mod_proxy_http. Preuzeto 10.01.2026. s https://httpd.apache.org/docs/current/mod/mod_proxy_http.html
- Curl (bez dat.) Documentation Overview. Preuzeto 10.01.2026. s https://curl.se/docs/