

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

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

Kolegij: Sigurnost informacijskih sustava

Akademski godina: 2025./2026.

Sadržaj

- Cilj projekta
- Arhitektura sustava
- Mrežna konfiguracija
- WebGoat Aplikacija
- WAF konfiguracija
- Reverse proxy
- Testiranje
- Zaključak
- Literatura

Cilj projekta

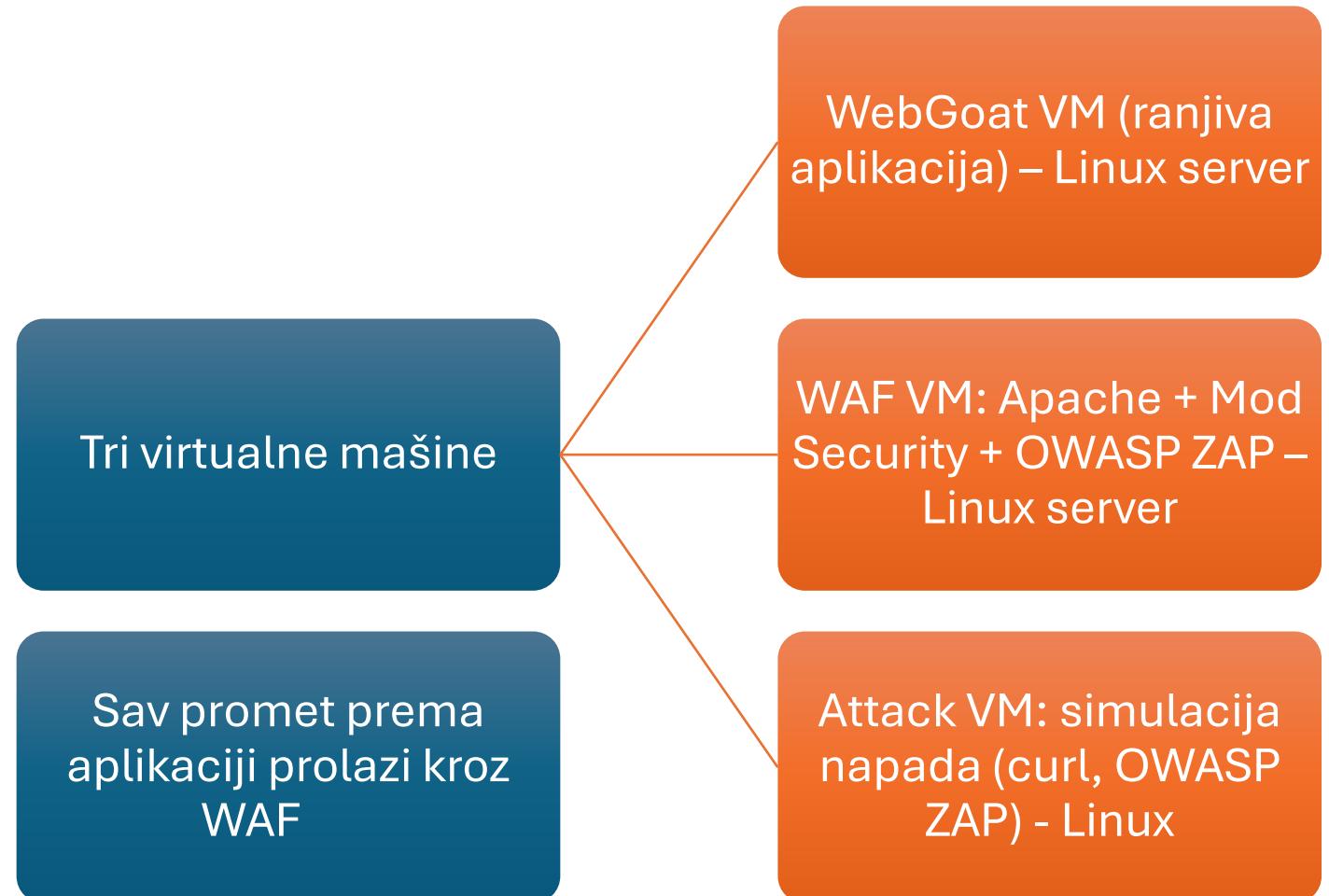
Implementirati WAF koristeći Apache + ModSecurity + OWASP CRS

Postaviti izolirano testno okruženje

Testirati reakciju WAF-a na zlonamjerne zahtjeve

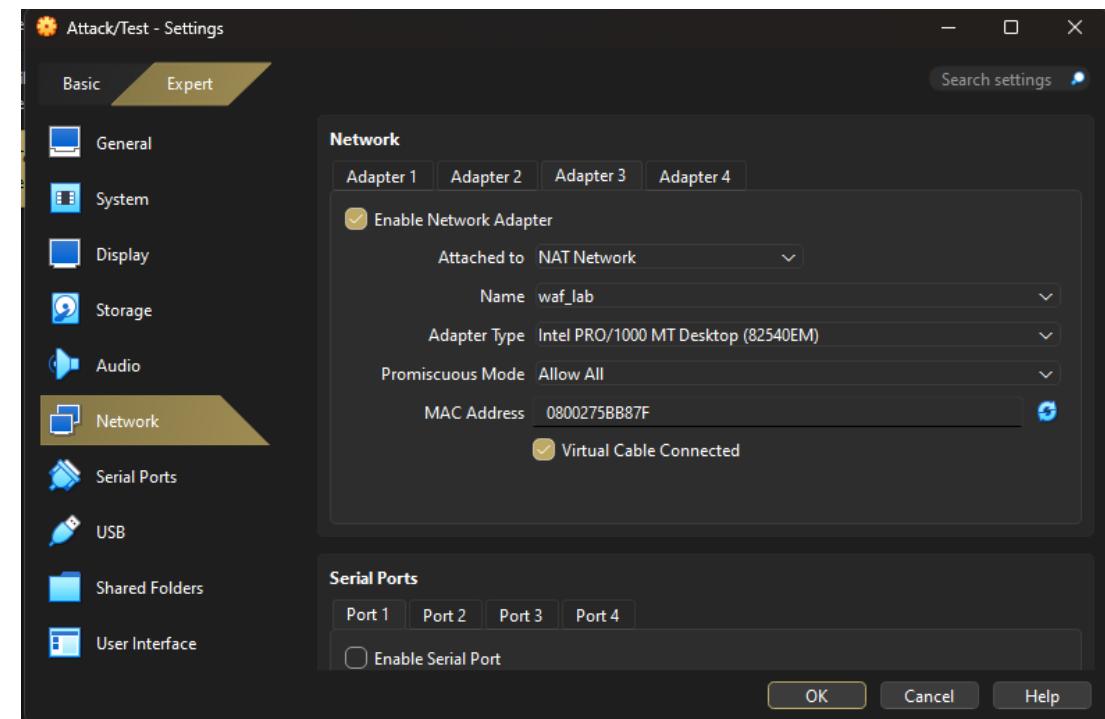
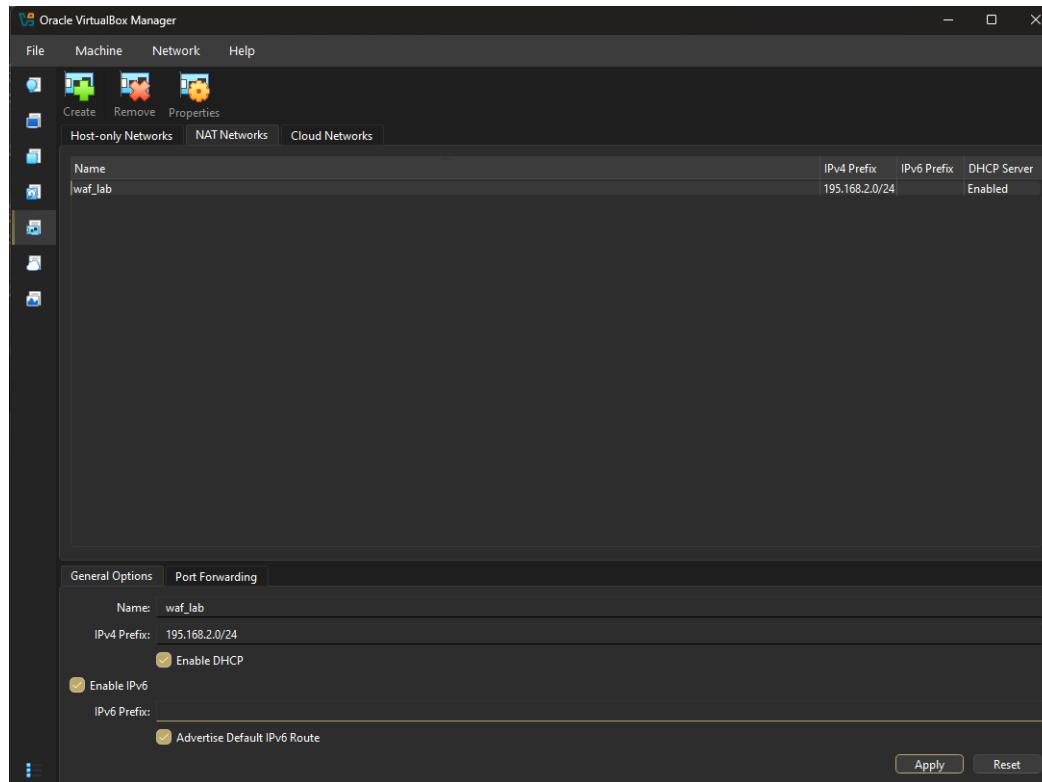
Usporediti ponašanje sustava sa i bez WAF-a

Arhitektura sustava



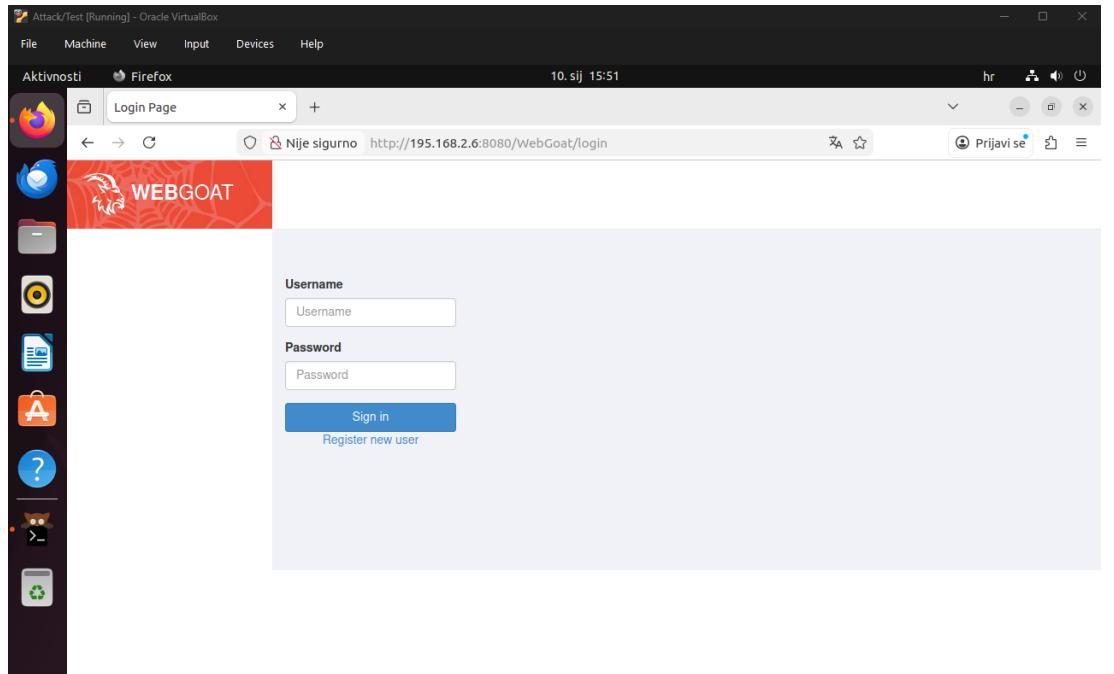
Mrežna konfiguracija

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



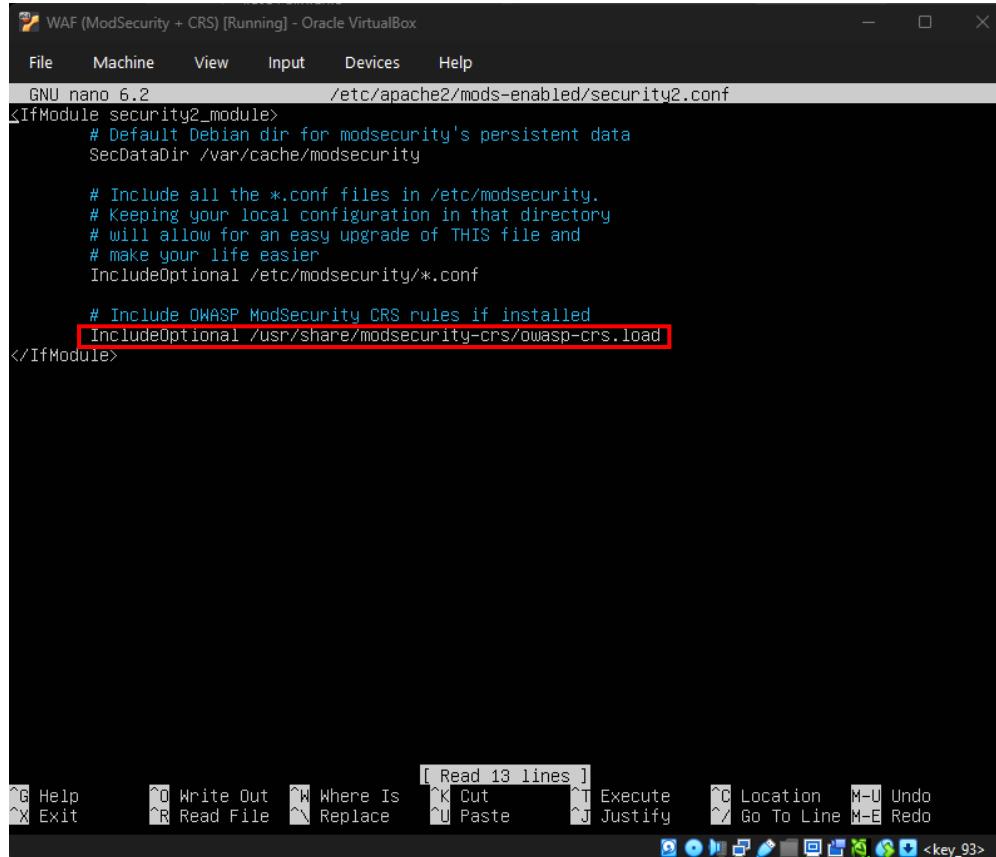
WebGoat aplikacija

- 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



```
GNU nano 6.2 /etc/apache2/mods-enabled/security2.conf
<IfModule security2_module>
    # Default Debian dir for modsecurity's persistent data
    SecDataDir /var/cache/modsecurity

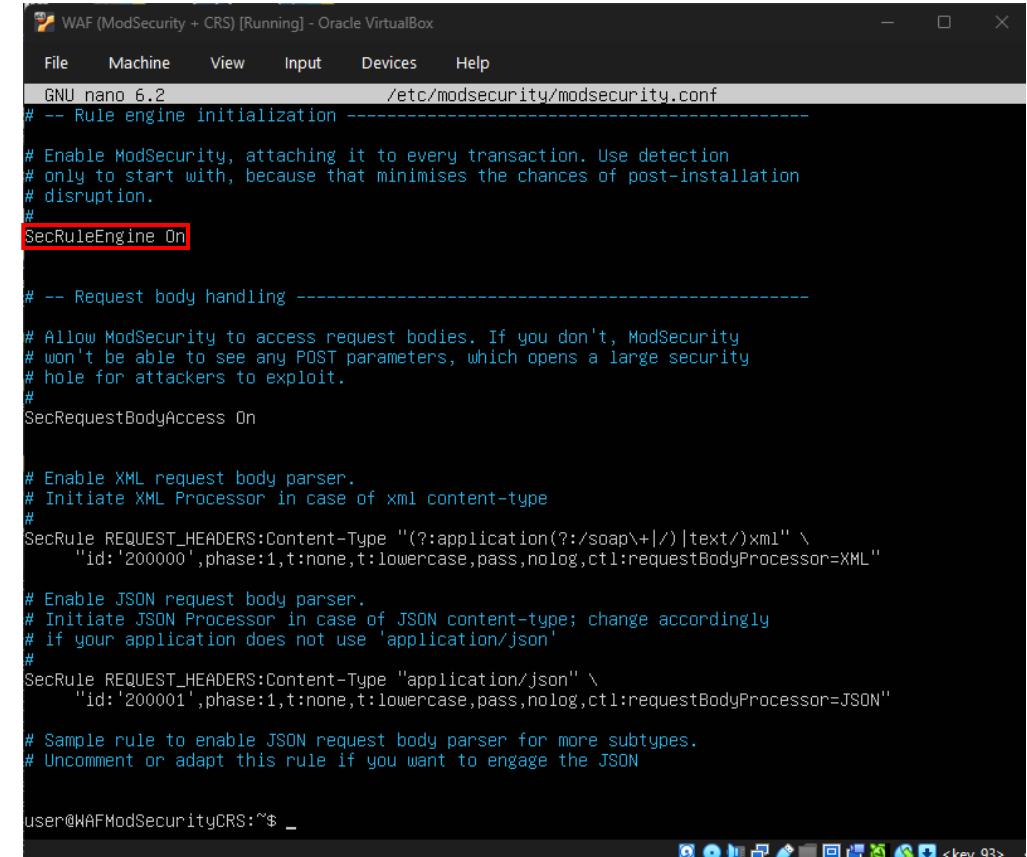
    # Include all the *.conf files in /etc/modsecurity.
    # Keeping your local configuration in that directory
    # will allow for an easy upgrade of THIS file and
    # make your life easier
    IncludeOptional /etc/modsecurity/*.conf

    # Include OWASP ModSecurity CRS rules if installed
    IncludeOptional /usr/share/modsecurity-crs/owasp-crs.load
</IfModule>
```

File Machine View Input Devices Help

^G Help ^D Write Out ^W Where Is ^C Cut ^J Execute ^C Location M-U Undo
^X Exit ^R Read File ^Y Replace ^P Paste ^L Justify ^I Go To Line M-E Redo

[Read 13 lines] <key_93> ..



```
GNU nano 6.2 /etc/modsecurity/modsecurity.conf
# -- Rule engine initialization ----

# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On

# -- Request body handling ----

# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "(?:application(?:/soap\+|/)|text/)\xml" \
    "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"

# Enable JSON request body parser.
# Initiate JSON Processor in case of JSON content-type; change accordingly
# if your application does not use 'application/json'
#
SecRule REQUEST_HEADERS:Content-Type "application/json" \
    "id:'200001',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=JSON"

# Sample rule to enable JSON request body parser for more subtypes.
# Uncomment or adapt this rule if you want to engage the JSON
```

user@WAFModSecurityCRS:~\$..

```
WAF (ModSecurity + CRS) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
GNU nano 6.2 /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ProxyPreserveHost On
    ProxyPass / http://195.168.2.6:8080/WebGoat/
    ProxyPassReverse / http://195.168.2.6:8080/WebGoat/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

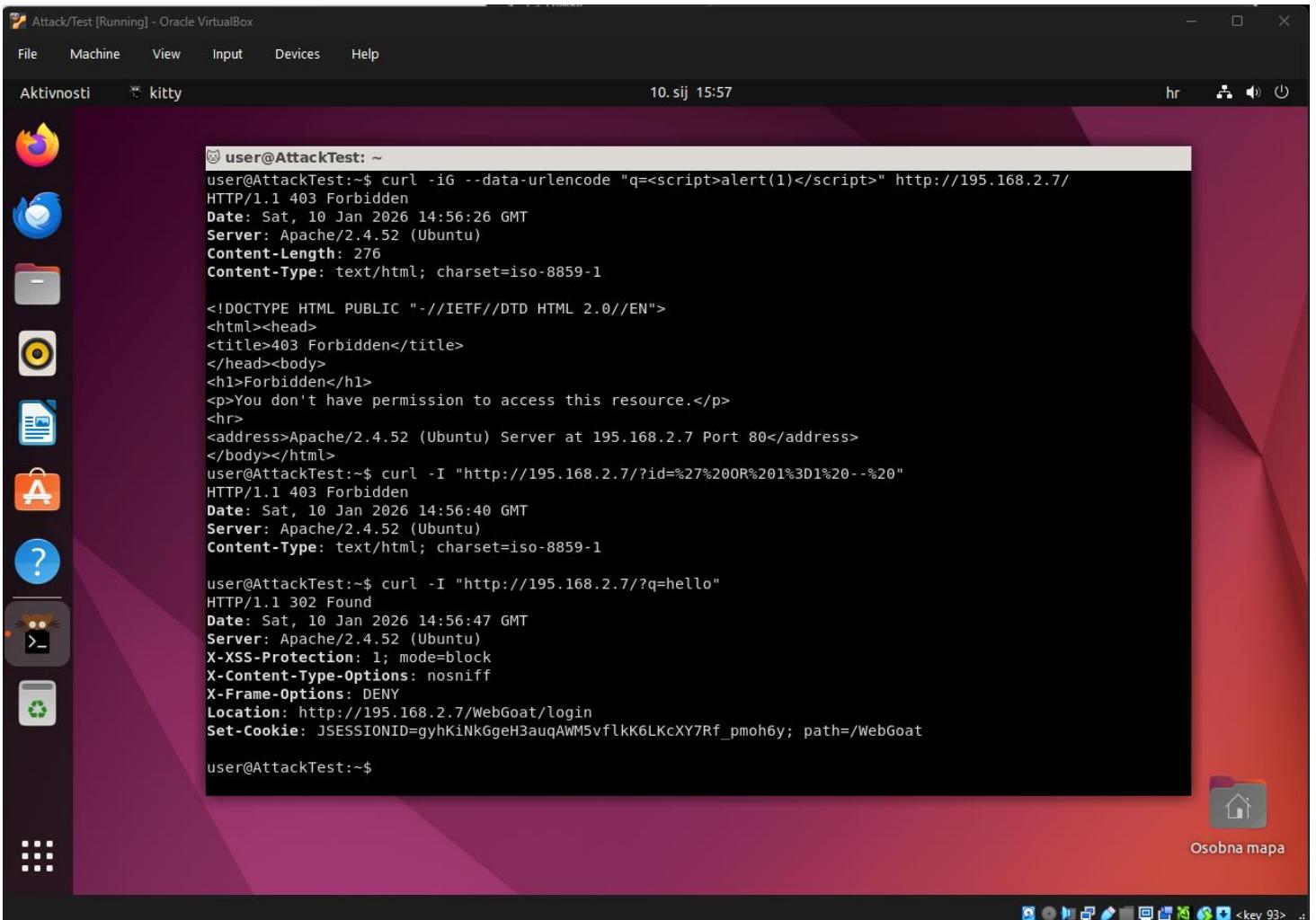
^G Help      ^O Write Out  ^W Where Is  [ Read 34 lines ]
^X Exit      ^R Read File  ^Y Replace   ^K Cut      ^T Execute  ^C Location M-U Undo
                                         ^U Paste    ^J Justify  ^G Go To Line M-E Redo
```

Reverse proxy

- Apache prima sve HTTP zahtjeve
- Prosljeduje 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



The screenshot shows a Linux desktop environment with a terminal window open in the foreground. The terminal window has a dark background and displays the following command-line session:

```
user@AttackTest:~$ curl -iG --data-urlencode "q=<script>alert(1)</script>" http://195.168.2.7/
HTTP/1.1 403 Forbidden
Date: Sat, 10 Jan 2026 14:56:26 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 276
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at 195.168.2.7 Port 80</address>
</body></html>
user@AttackTest:~$ curl -I "http://195.168.2.7/?id=%27%20OR%201%3D1%20--%20"
HTTP/1.1 403 Forbidden
Date: Sat, 10 Jan 2026 14:56:40 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1

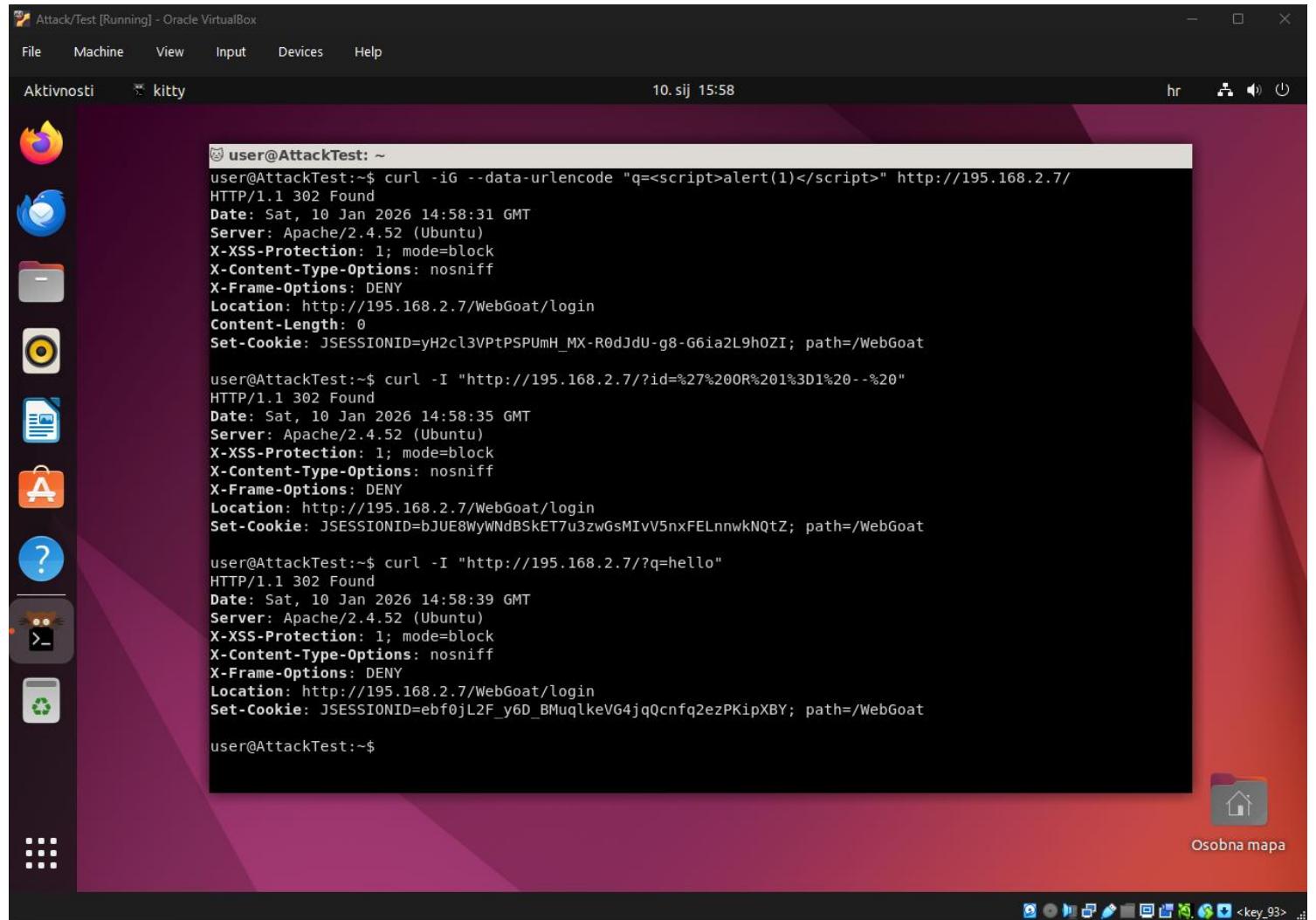
user@AttackTest:~$ curl -I "http://195.168.2.7/?q=hello"
HTTP/1.1 302 Found
Date: Sat, 10 Jan 2026 14:56:47 GMT
Server: Apache/2.4.52 (Ubuntu)
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Location: http://195.168.2.7/WebGoat/login
Set-Cookie: JSESSIONID=gyhKiNkGgeH3auqAWM5vflkk6LKcXY7Rf_pmoh6y; path=/WebGoat

user@AttackTest:~$
```

The desktop environment includes a dock with icons for various applications like a browser, file manager, terminal, and system tools. The taskbar at the bottom shows several open windows and a user profile icon.

Testiranje

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



```
user@AttackTest:~$ curl -iG --data-urlencode "q=<script>alert(1)</script>" http://195.168.2.7/
HTTP/1.1 302 Found
Date: Sat, 10 Jan 2026 14:58:31 GMT
Server: Apache/2.4.52 (Ubuntu)
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Location: http://195.168.2.7/WebGoat/login
Content-Length: 0
Set-Cookie: JSESSIONID=yH2cL3VPtPSPUmH_MX-R0dJdU-g8-G6ia2L9h0ZI; path=/WebGoat

user@AttackTest:~$ curl -I "http://195.168.2.7/?id=%27%200R%201%3D1%20--%20"
HTTP/1.1 302 Found
Date: Sat, 10 Jan 2026 14:58:35 GMT
Server: Apache/2.4.52 (Ubuntu)
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Location: http://195.168.2.7/WebGoat/login
Set-Cookie: JSESSIONID=bJUE8WyWNdBSkET7u3zwGsMIVv5nxFELnnwkNQtZ; path=/WebGoat

user@AttackTest:~$ curl -I "http://195.168.2.7/?q=hello"
HTTP/1.1 302 Found
Date: Sat, 10 Jan 2026 14:58:39 GMT
Server: Apache/2.4.52 (Ubuntu)
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Location: http://195.168.2.7/WebGoat/login
Set-Cookie: JSESSIONID=ebf0jL2F_y6D_BMuqlkeVG4jqQcnfq2ezPKipXBY; path=/WebGoat

user@AttackTest:~$
```

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/>