
LOGIN
software

software

ORACLE Gold Partner

# Alen Prodan

## ModSecurity za administratore baze podataka

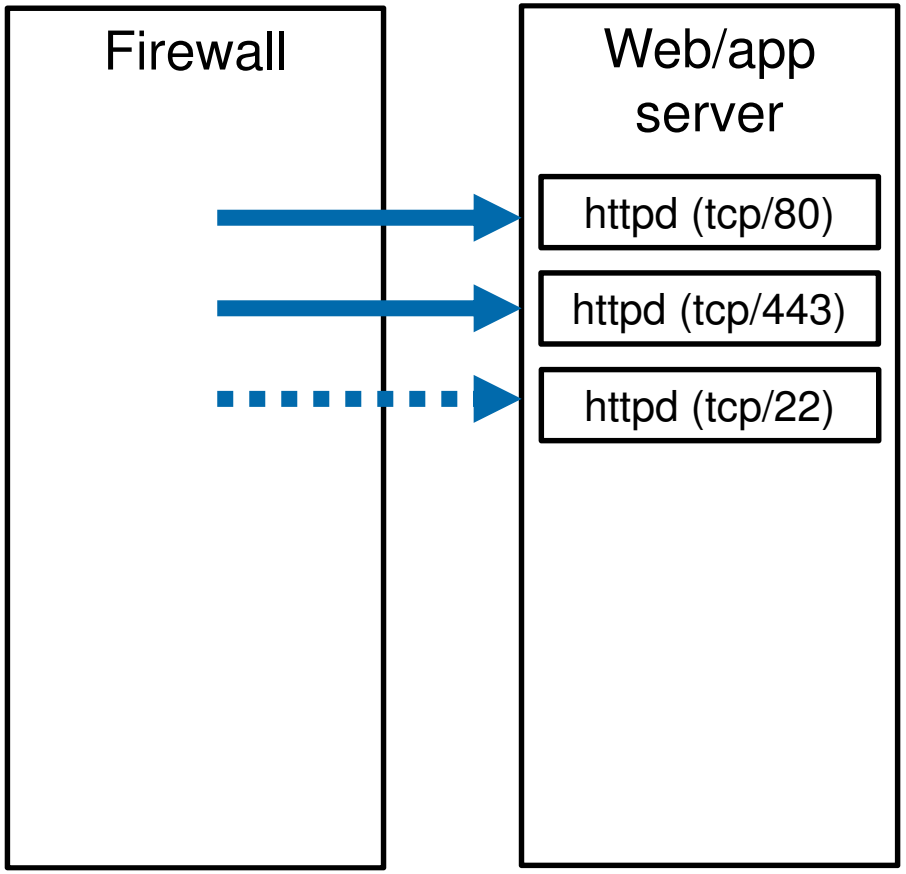
software

# Agenda

- Sigurnost okruženja web aplikacija - uvod
- Što je Web Application Firewall ?
- ModSecurity WAF – dizajn i implementacija
- Prikaz identifikacije i prevencije SQL Injection i Information Leakage napada pomoću ModSecurity WAF uređaja

# Uvod

## Topologija mreže - tradicionalni firewall




- HTTP(s) protokol potpuno otvoren
- SSH (tcp/22) filtriran

# Uvod

## ... ili zašto Firewall nije dovoljna zaštita

- Firewall uređaj propušta/blokira mrežni promet na temelju unaprijed definiranih pravila
- Tradicionalno firewall uređaji rade na OSI razinama 3 i 4, iako nove generacije u određenoj mjeri podržavaju inspekciju prometa na višim razinama OSI stoga
- Firewall provjerava smije li mrežni promet sa Računala_A:PortX dospijeti do Računala_B:PortY,
- Firewall ne provjerava sadržaj mrežnog prometa
- Dakle, pristup je u potpunosti omogućen ili nema pristupa

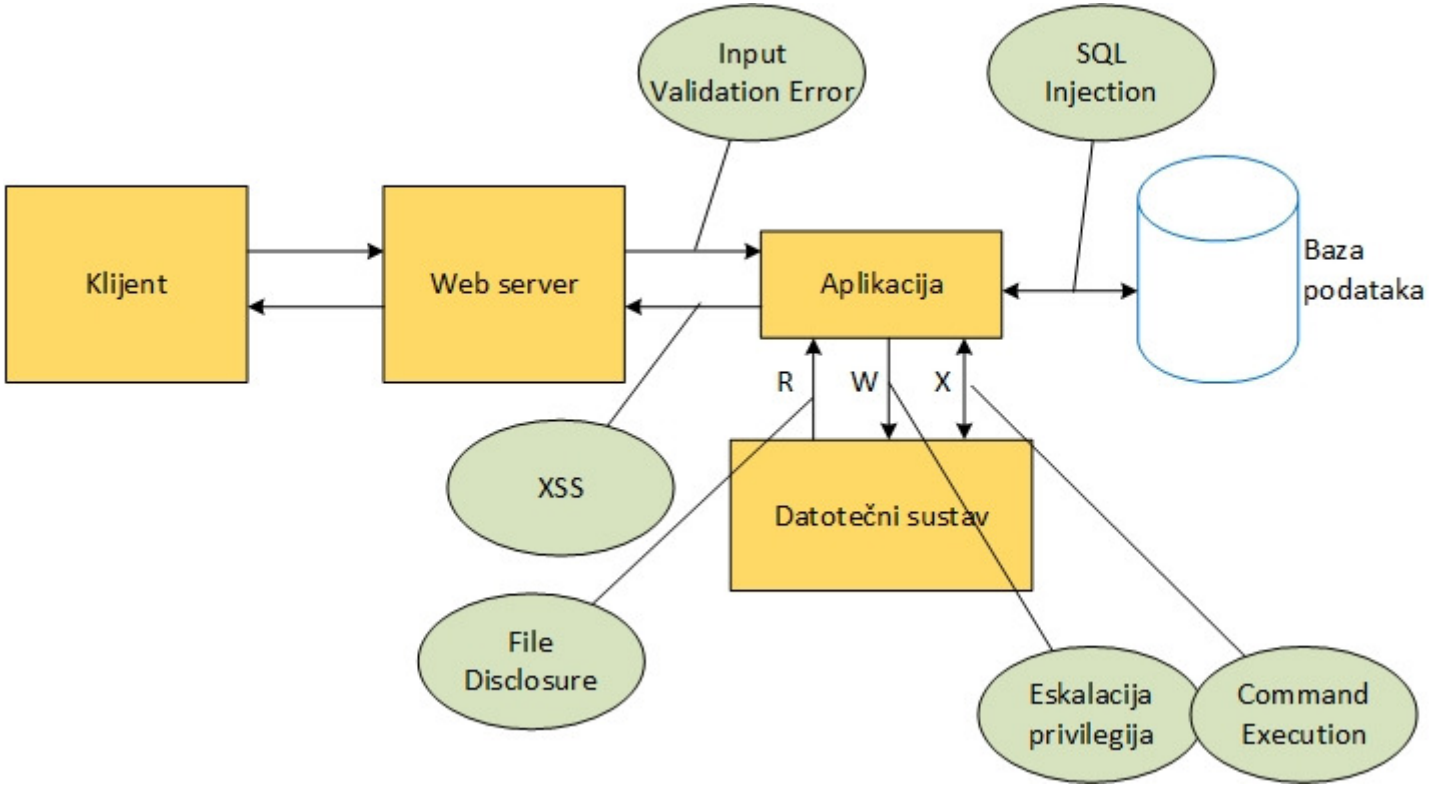
# Uvod

## ... ili zašto Firewall nije dovoljna zaštita

- Pretpostavimo da imamo samo otvoren port 80 i 443
- Pretpostavimo da se sigurnosne zakrpe redovno apliciraju
- Vulnerability scanner ne pokazuje ranjivosti pogodne za napad
- HTTP promet je kriptiran (SSL/TLS)
- Da li je stvarno sustav siguran ?

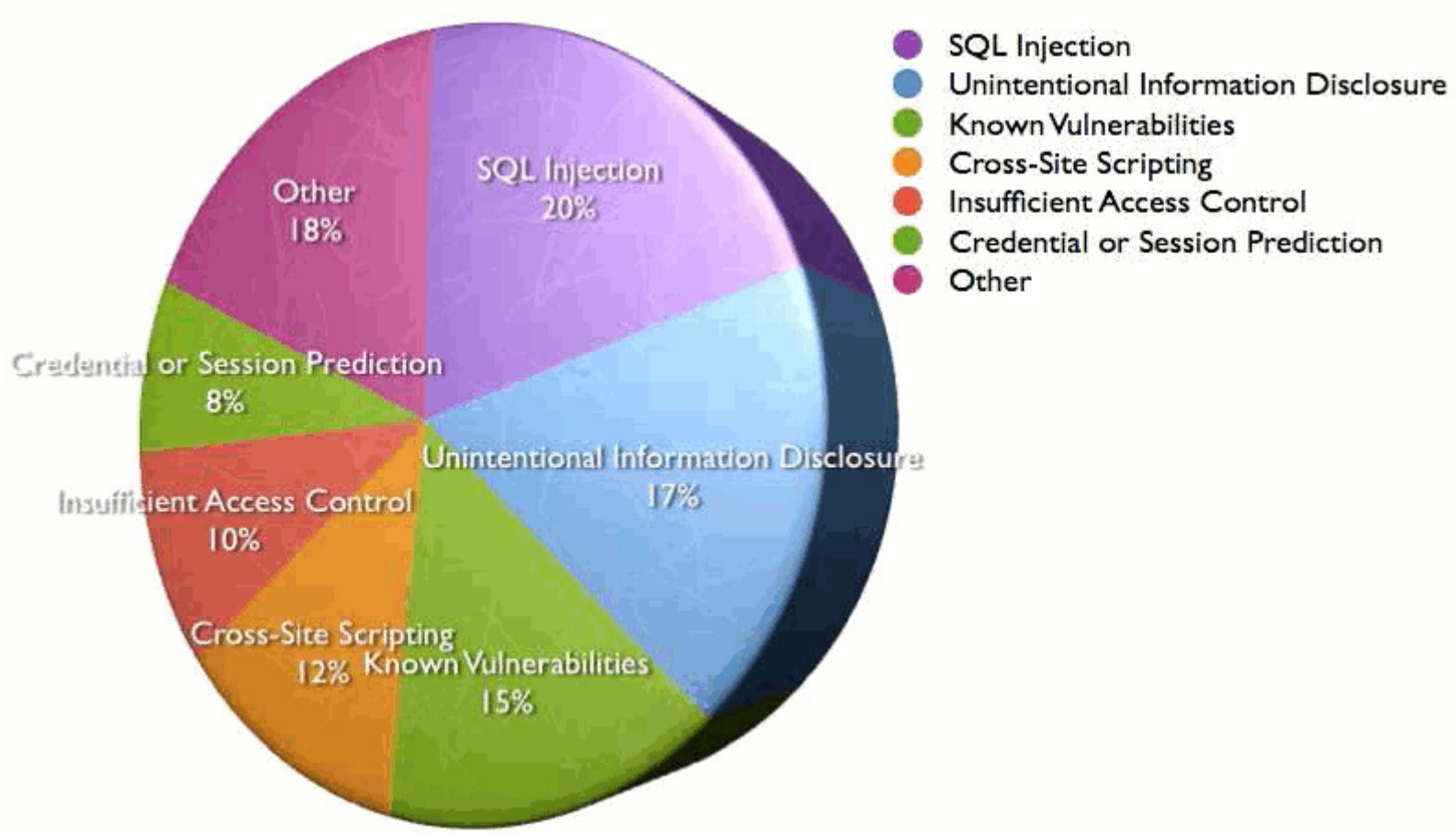
# Uvod

## Problem sigurnosti web aplikacija



# Uvod

## Korištene ranjivosti za napad na sustave




Izvor: http://project67555.appspot.com/security.html

# Rješenja

## Da li je to sve ?

- Pravovremena instalacija zakrpi za server softver
- Razvoj vlastitog programskog koda vodeći računa o sigurnosti
- Hardening mrežne i serverske infrastrukture

# ModSecurity Web Application Firewall

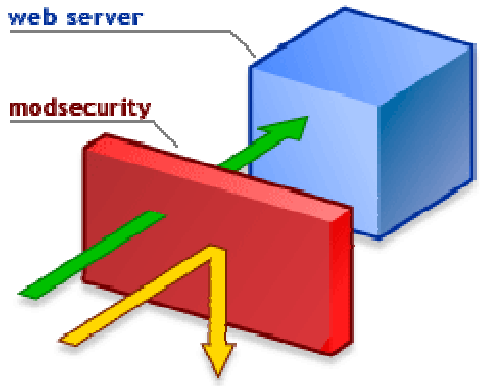
## Što je ModSecurity ?

- ModSecurity je open-source web application firewall
- Slobodan (besplatan) za korištenje
- WAF je softver koji vrši inspekciju HTTP prometa koristeći unaprijed definirani skup pravila (rules)
- Pravila spriječavaju poznate napade kao npr. SQL Injection, Information Leakage, XSS …
- Prilagođavajući pravila vlastitim aplikacijama mnogi napadi mogu biti identificirani i blokirani
- Dostupan na različitim platformama i za različite HTTP servere (Apache, IIS, Nginx)
- Najzastupljenija inačica je modsecurity module za Apache 2.x (70% instalacija)
- Trenutna verzija ModSecurity 2.8.0 (15.04.2014)

# ModSecurity Web Application Firewall

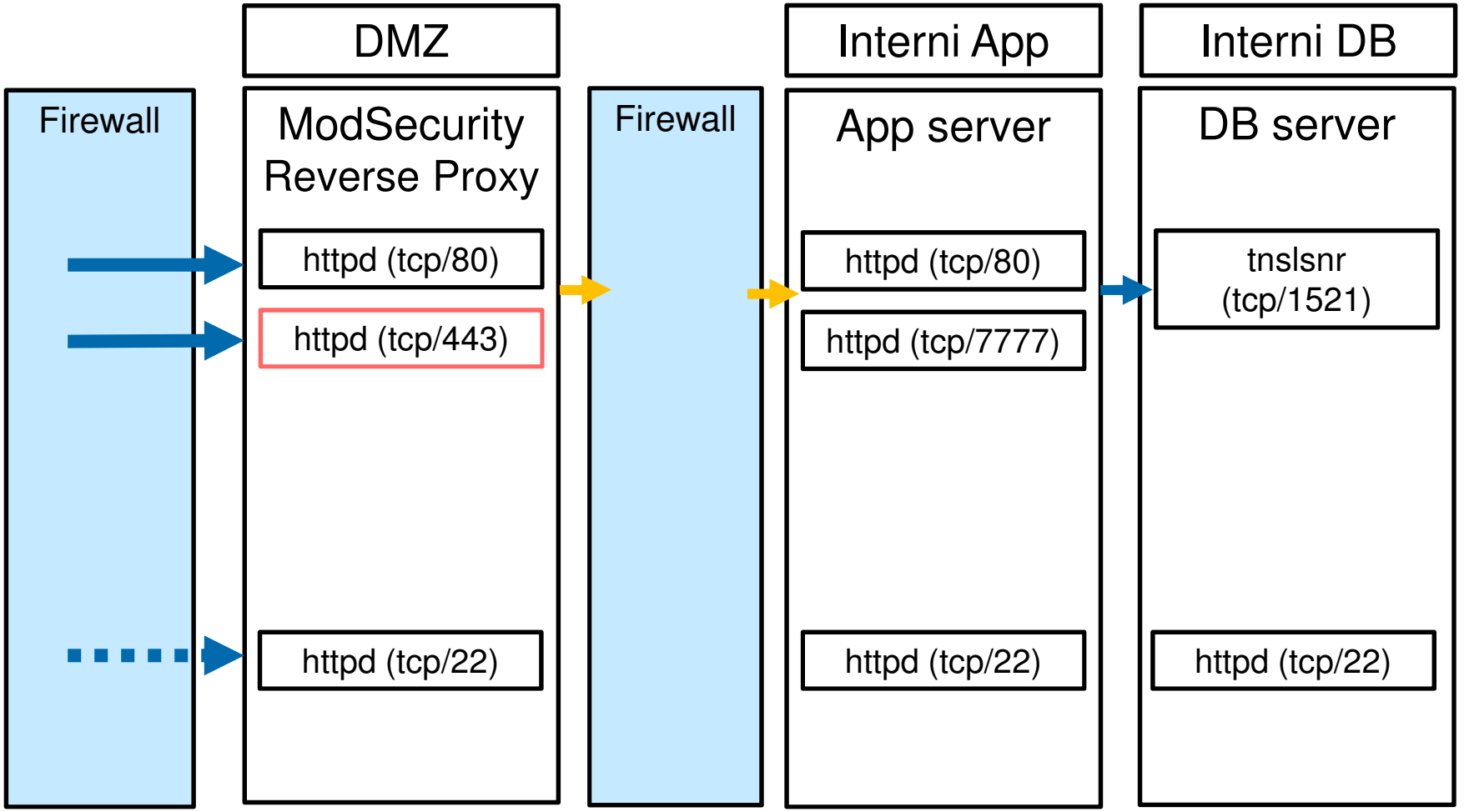
## ModSecurity – glavne prednosti u zaštiti web aplikacija

- Nadzor HTTP prometa i kontrola pristupa web aplikacijama u realnom vremenu
- Virtualne zakrpe (virtual patching)
- Potpuno logiranje HTTP prometa
- Kontinuirana procjena sigurnosti sustava
- Snažnija zaštita (hardening) web aplikacija
- Podržani modaliteti instalacije: Embedded i Reverse Proxy



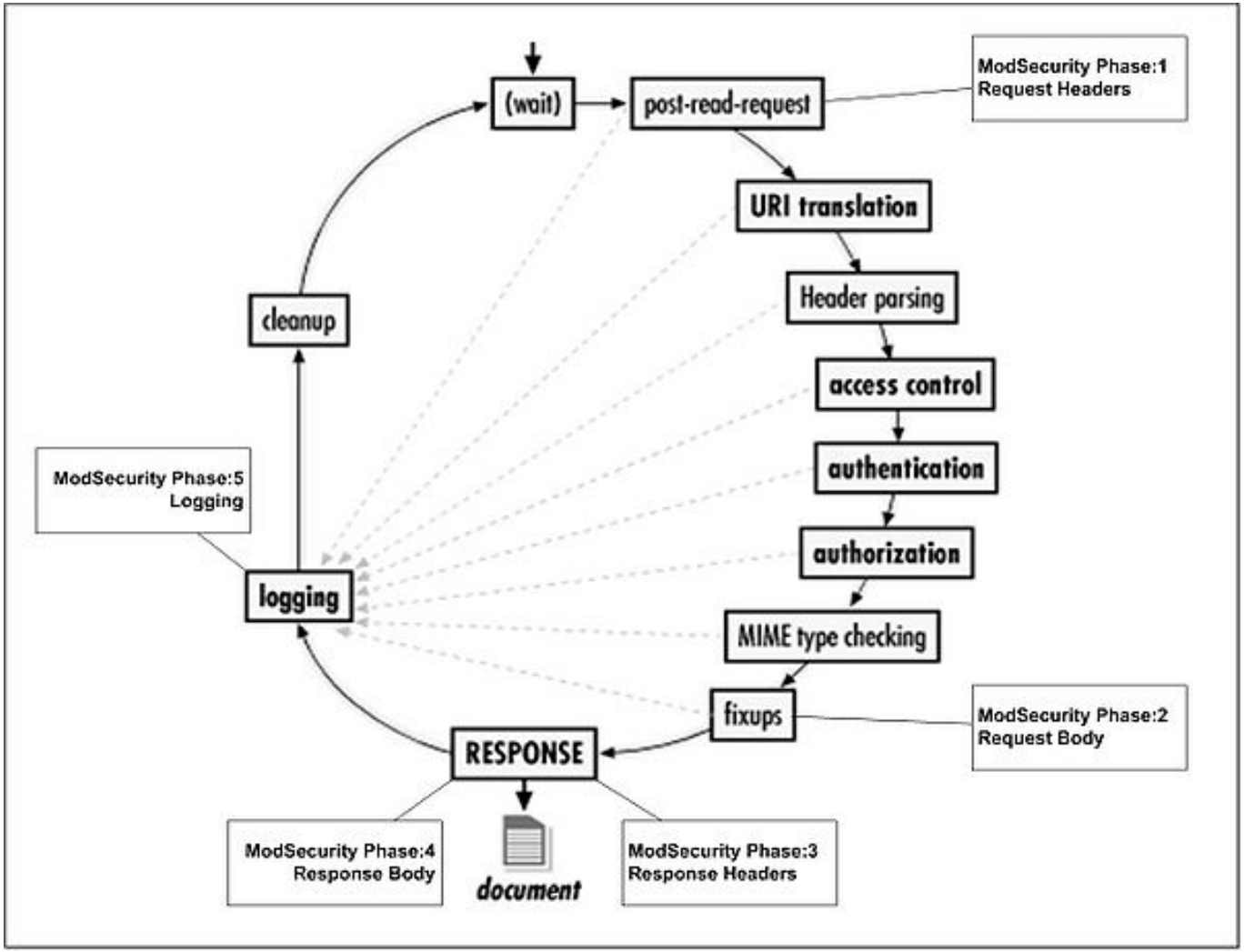
# Web Application Firewall (WAF)

## Topologija mreže - Web application firewall



# ModSecurity Web Application Firewall

## Životni ciklus HTTP transakcije



# ModSecurity Web Application Firewall

## Konfiguracijske postavke i pravila (rules)

- Konfiguracijske postavke i pravila (rules) su temelj funkcioniranja ModSecurity sustava
- Konfiguracijske postavke određuju način na koji ModSecurity procesira elemente HTTP prometa
- Pravila (rules) odlučuju što napraviti sa procesiranim podacima
- Konfiguracijske postavke i pravila pohranjuju se u tekstualne .conf datoteke koje se učitavaju/inicijaliziraju prilikom pokretanja Apache servera putem Include direktive

# ModSecurity Web Application Firewall

## Konfiguracijske postavke

**httpd.conf:**

```
<IfModule security2_module>
 Include conf/crs/*.conf
</IfModule>
```

**modsecurity.conf:**

```
SecRuleEngine On
SecRequestBodyAccess On
SecResponseBodyAccess On
SecAuditEngine On

SecDebugLog /usr/local/apache2/logs/modsec_debug.log
SecDebugLogLevel 9
SecComponentSignature "OWASP_CRS/2.2.9"
SecDefaultAction "phase:1,deny,log"
SecServerSignature "Microsoft-IIS/6.0"

SecAuditLog /usr/local/apache2/logs/modsec_audit.log
SecAuditLogParts ABCDEFGHIJKZ
SecAuditLogRelevantStatus "^(?:5|4(?!04))"
SecAuditLogType Serial
SecDataDir /usr/local/apache2/logs/data

SecGeoLookupDb /usr/local/geoip/GeoIP.dat
...
```

# ModSecurity Web Application Firewall

## Pravila (rules)

```
SecRule VARIABLES OPERATOR ACTIONS
```

- VARIABLES – određuje element HTTP transakcije nad kojim se vrši inspekcija
- OPERATOR – određuje način/mehanizam za analizu elemenata HTTP transakcije (regular expressions najpopularniji izbor)
- ACTIONS – određuje što treba napraviti ukoliko pravilo prepozna traženi uzorak

Primjer:

```
SecRule REQUEST_URI "f?p=4550" \
"t:lowercase,deny,log,auditlog,phase:2,status:404,msg:
'Neovlasteni pristup APEX_ADMIN',tag:'NEOVL.PRISTUP
f?p=4550',severity:'4'"
```

# ModSecurity Web Application Firewall

## SQL Injection i Information Leakage ranjivosti - definicija

- SQL Injection ranjivosti nastaju kada razvojni programeri koriste neprovjerene podatke za izradu dinamičkih SQL i PL/SQL naredbi
- Information Leakeage ranjivost nastaje kada sistemski podaci ili debugging informacije nekontrolirano izlaze iz sustava koristeći izlazni tok podataka (output stream) ili logging funkcionalnosti

```
Primjer ranjivog SQL upita:

sql = SELECT id, naziv FROM proizvodi WHERE id = <LITERAL>;
```

Potencijalna šteta:

- Gubitak podataka ili korupcija
- Curenje informacija
- DoS
- Reputacijski rizik

# ModSecurity Web Application Firewall

## SQL Injection ranjivost

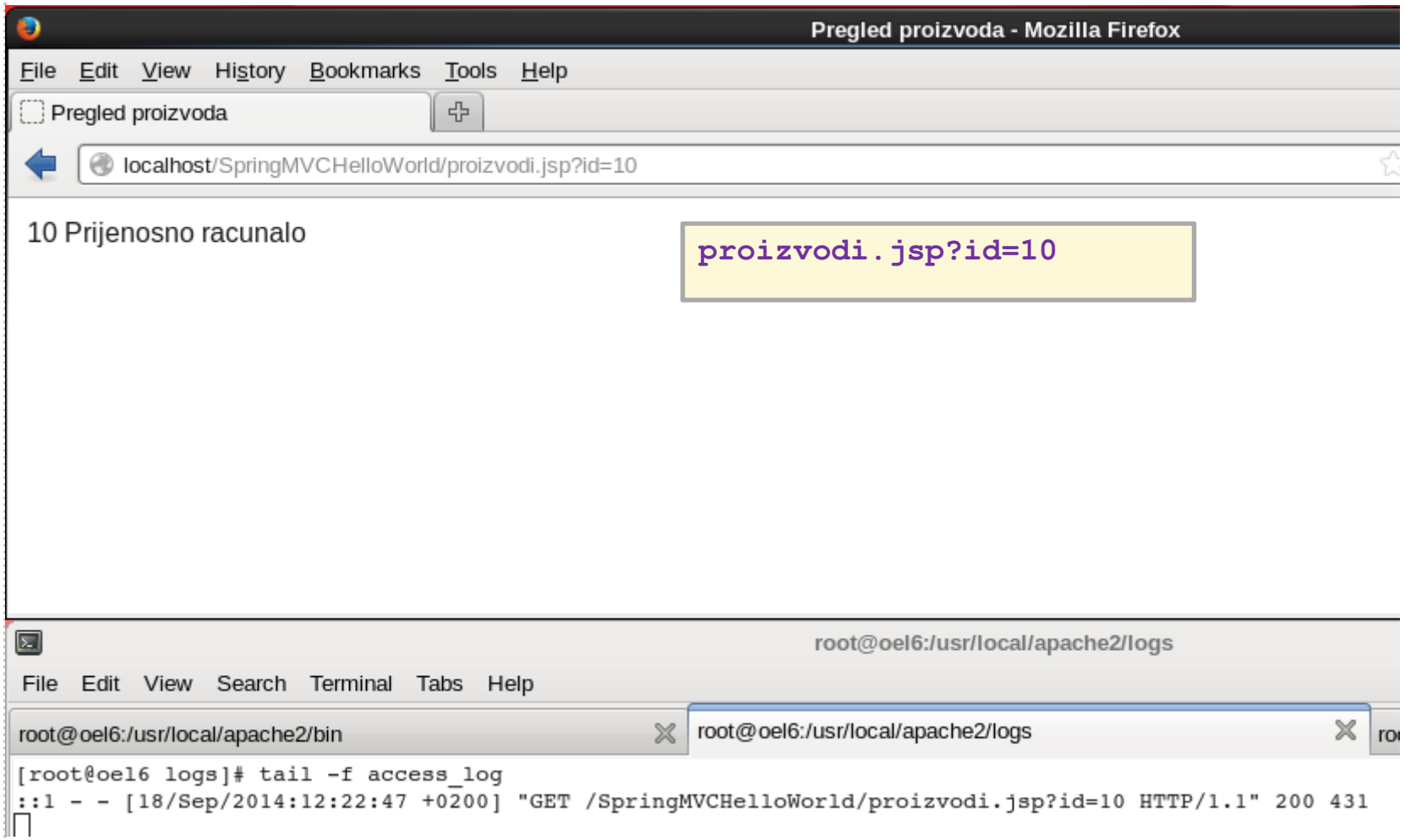
**Primjer ranjivog Java koda:**

```
Connection connection = null;
try {
 connection =
DriverManager.getConnection("jdbc:oracle:thin:@testhost:1521:orcl",
"test", "test");
  Statement statement = connection.createStatement();
  String id = request.getParameter("id");
  String sql = "SELECT id, naziv FROM proizvodi WHERE id = " + id;

  ResultSet resultSet = statement.executeQuery(sql);
  while (resultSet.next()) {
    resultSet.getString("id");
    resultSet.getString("naziv");
}
catch(Exception exception) {
 exception.printStackTrace();
     out.println("Exception : " + exception.getMessage());
}
```

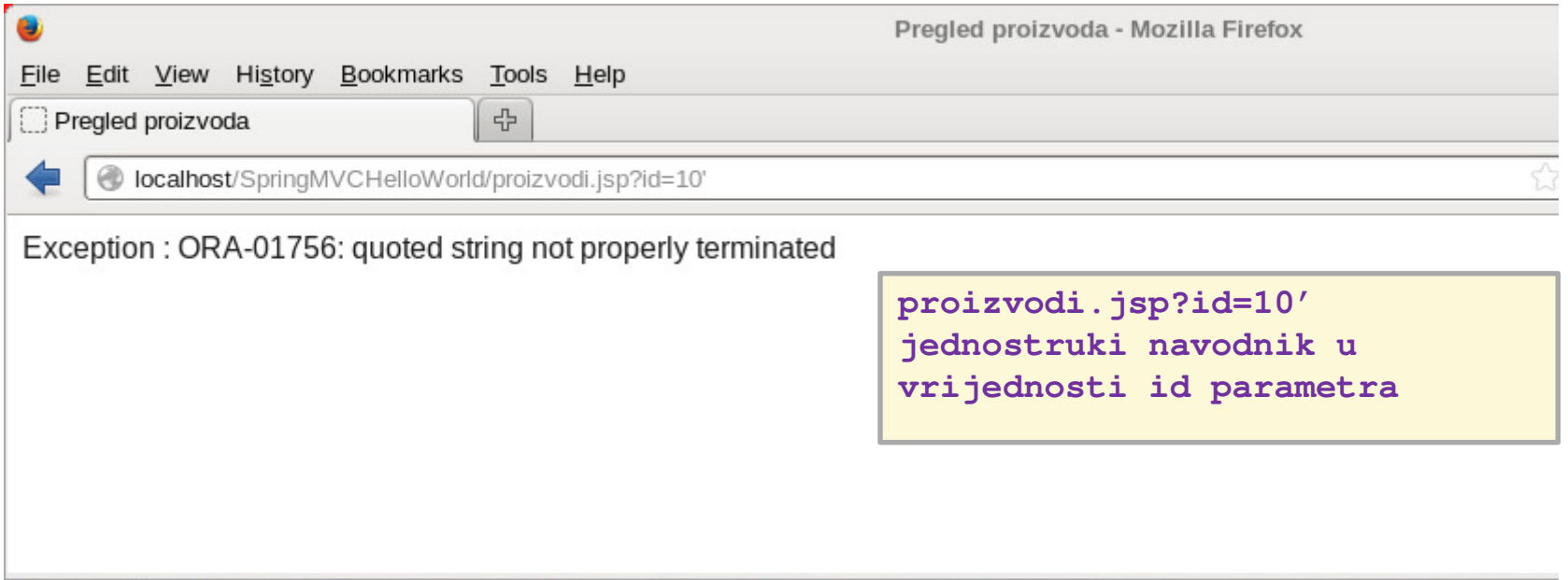
# ModSecurity Web Application Firewall

## SQL Injection ranjivost – planirano korištenje aplikacije



# ModSecurity Web Application Firewall

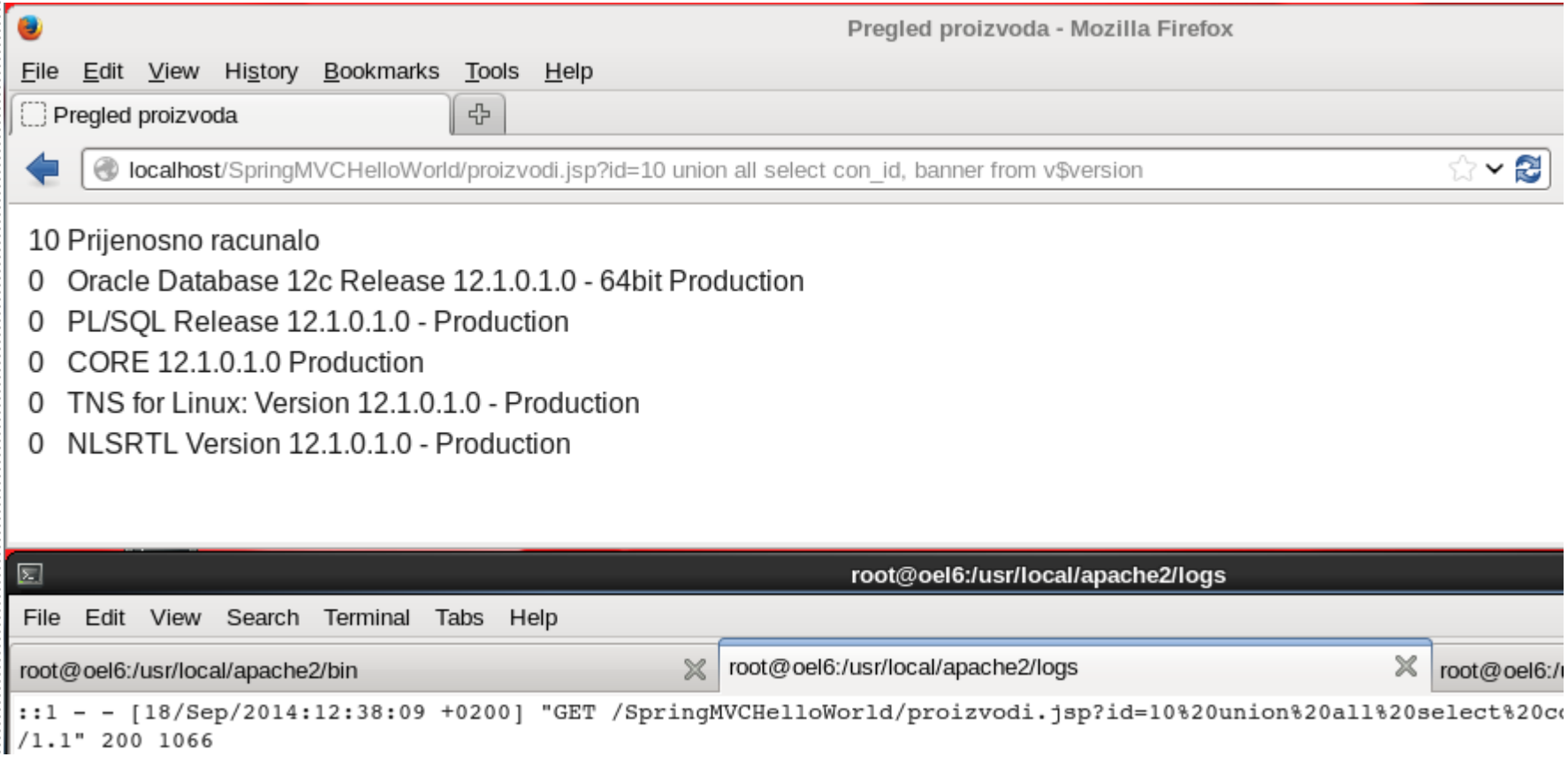
## Ispitivanje aplikacije na SQL Injection ranjivost




```
SELECT id, naziv, kolicina FROM proizvodi WHERE id = 10'
```

# ModSecurity Web Application Firewall

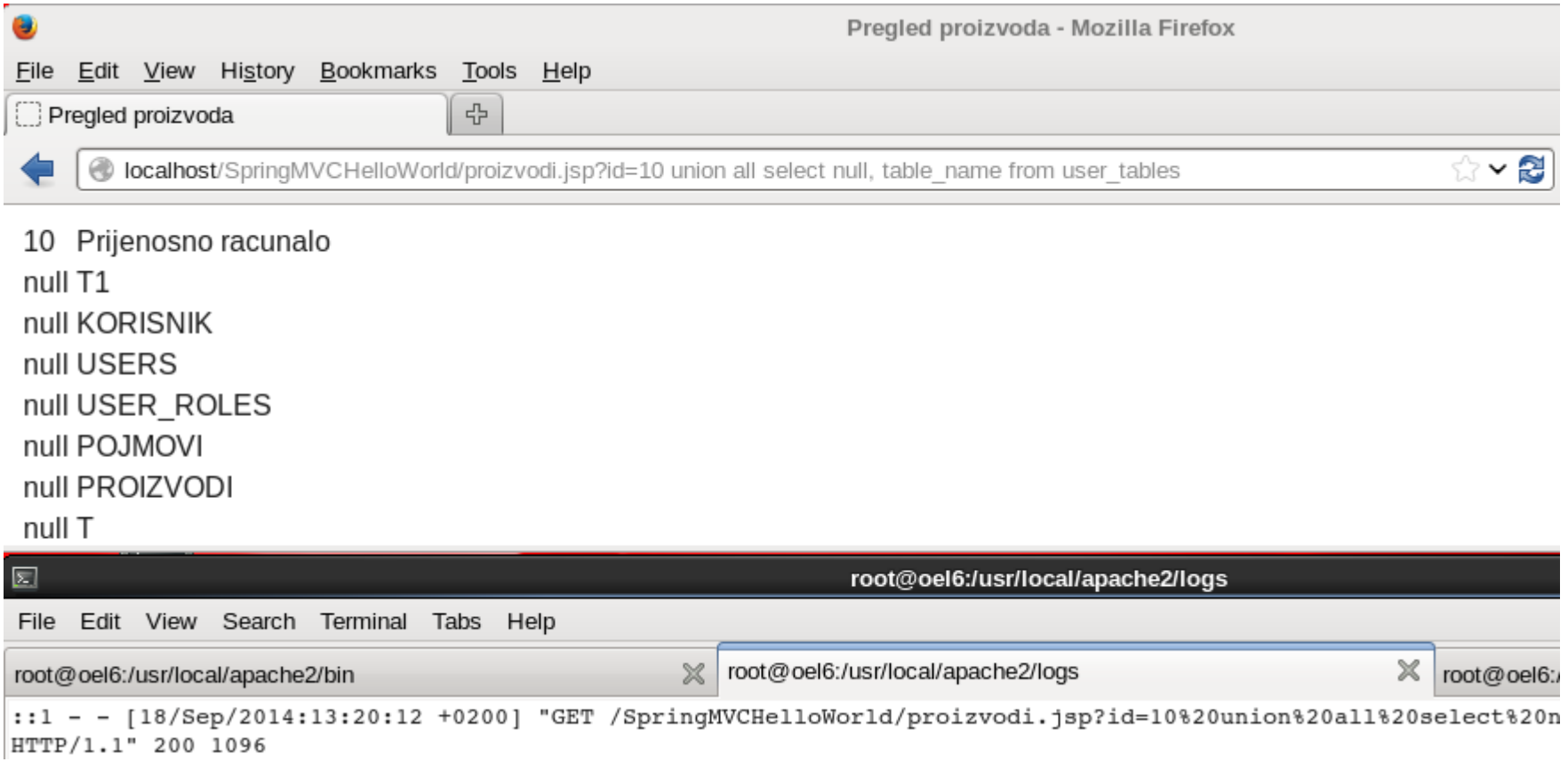
## SQL Injection ranjivost – SQL manipulacija UNION ALL




```
SELECT id, naziv, kolicina FROM proizvodi WHERE id = 10
UNION ALL
SELECT con_id, banner FROM v$version
```

# ModSecurity Web Application Firewall

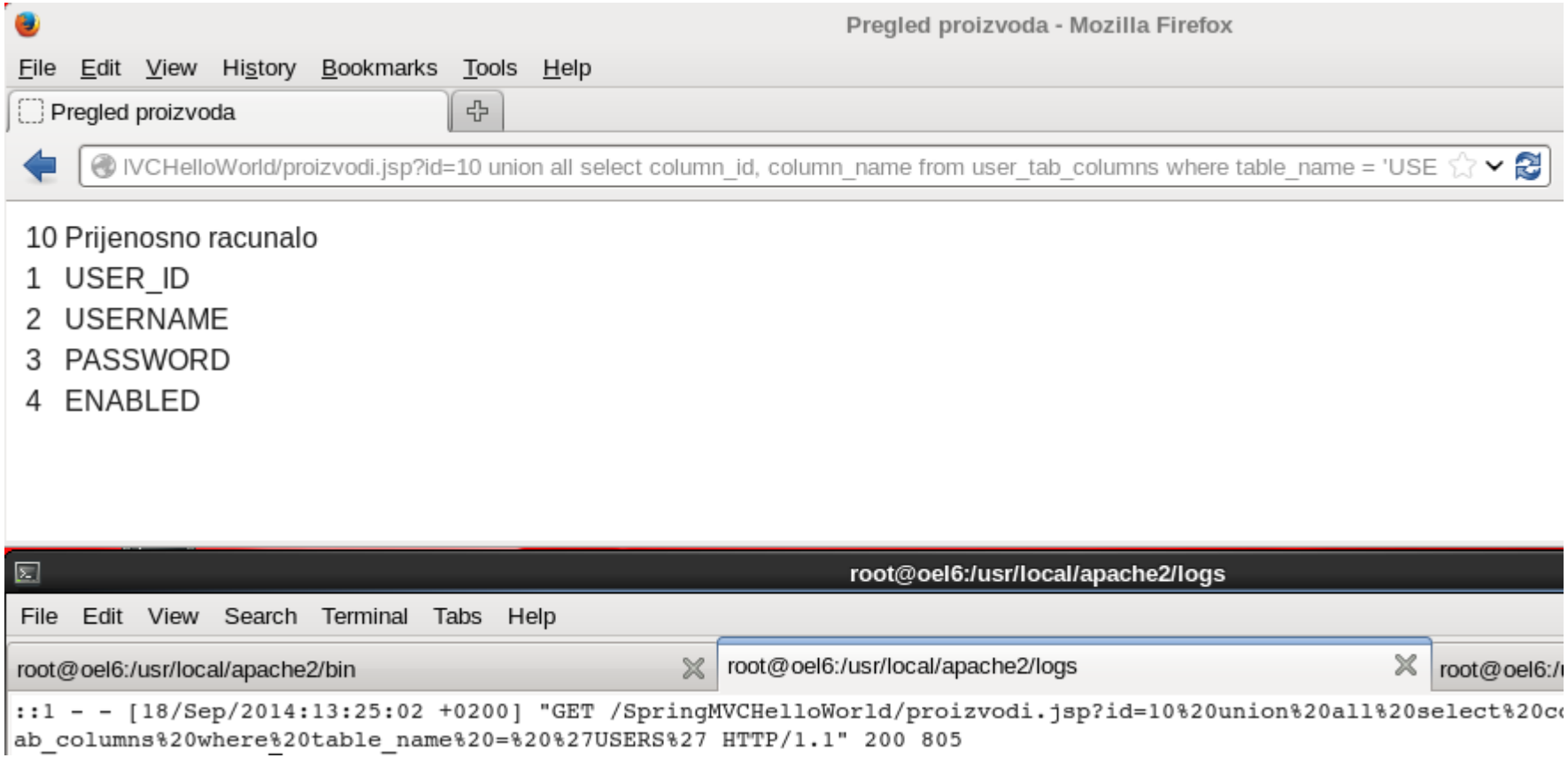
## SQL Injection ranjivost – SQL manipulacija UNION ALL




```
SELECT id, naziv, kolicina FROM proizvodi WHERE id = 10
UNION ALL
SELECT null, table_name FROM user_tables
```

# ModSecurity Web Application Firewall

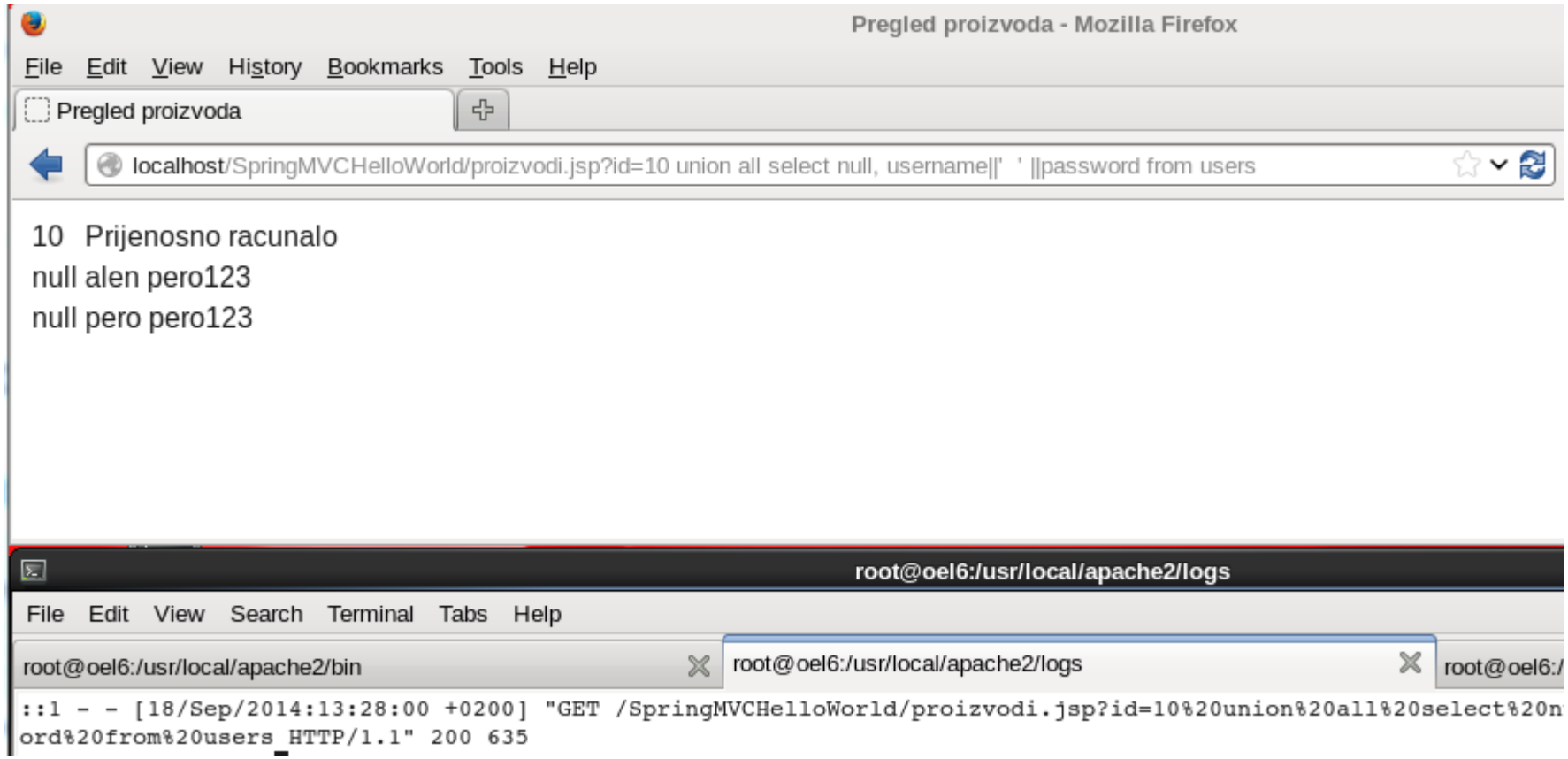
## SQL Injection ranjivost – SQL manipulacija UNION ALL




```
SELECT id, naziv, kolicina FROM proizvodi WHERE id = 10
UNION ALL
SELECT column_id, column_name FROM user_tab_columns where table_name ='USERS'
```

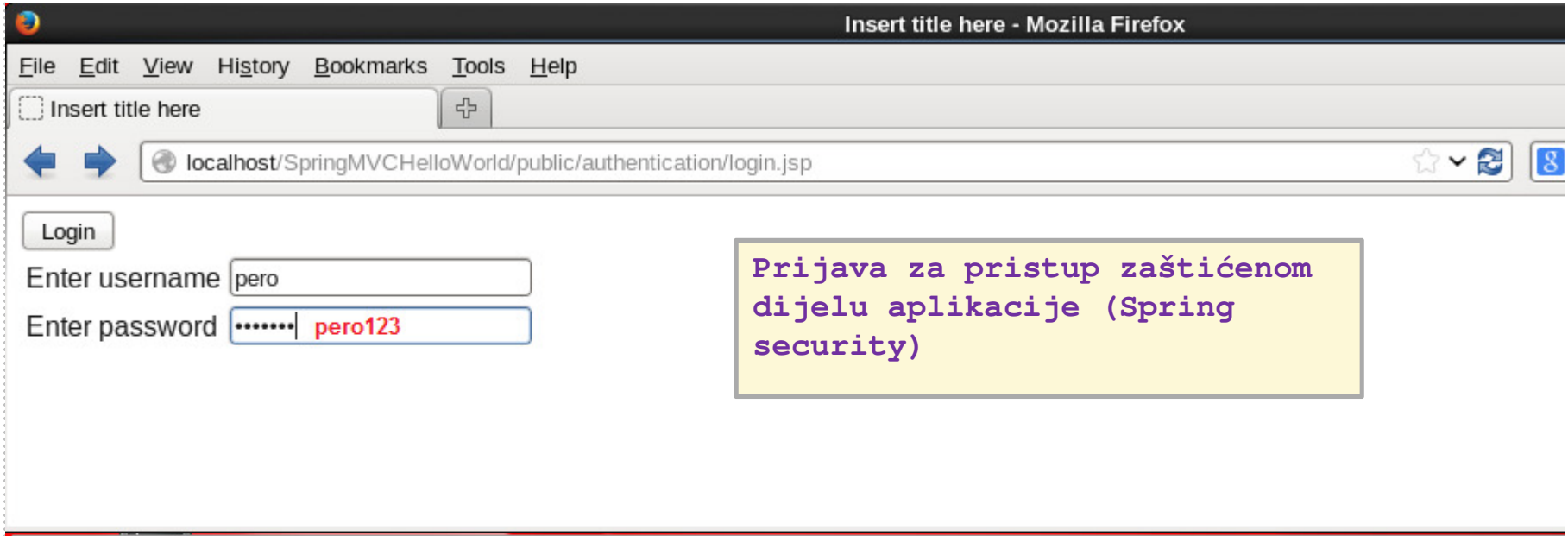
# ModSecurity Web Application Firewall

## SQL Injection ranjivost – SQL manipulacija UNION ALL

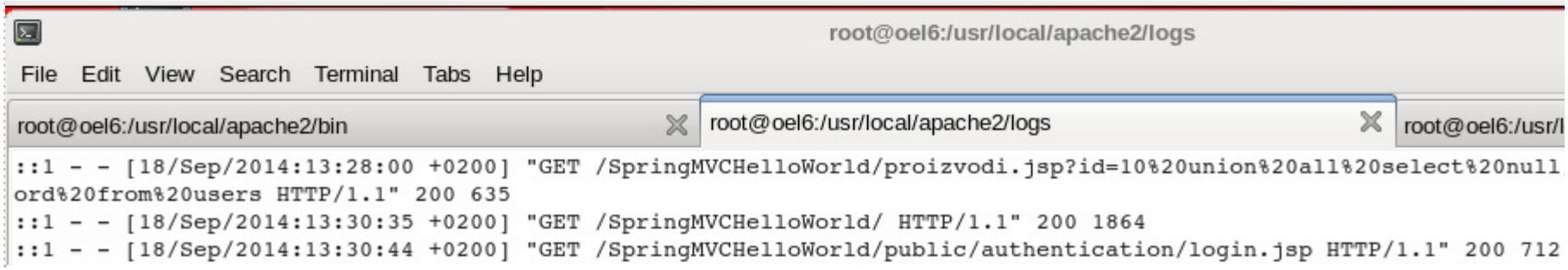



```
SELECT id, naziv, kolicina FROM proizvodi WHERE id = 10
UNION ALL
SELECT null, username||' `||password FROM users
```

# ModSecurity Web Application Firewall

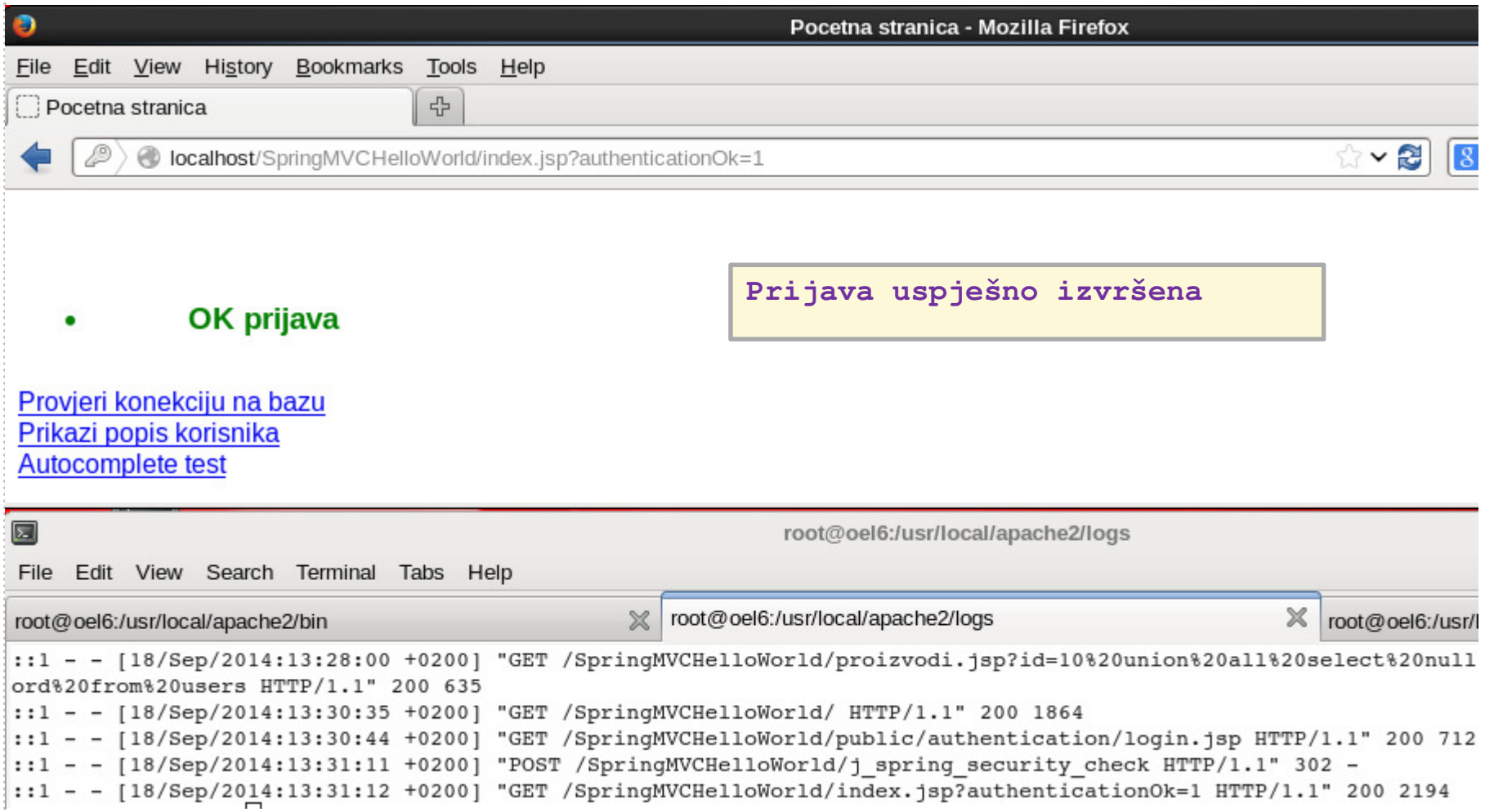



**Prijava za pristup zaštićenom dijelu aplikacije (Spring security)**



# ModSecurity Web Application Firewall

## SQL Injection ranjivost - Demo



# ModSecurity Web Application Firewall

## Pravila (rules) za zaštitu od SQL Injection napada

```
::1 - - [18/Sep/2014:13:27:28 +0200] "GET
   /SpringMVCHelloWorld/proizvodi.jsp?id=10%20union%20all%20selec
   t%20username,%20password%20from%20users HTTP/1.1" 200 380
```

**SecRule VARIABLES OPERATOR ACTIONS**

**Regex:**

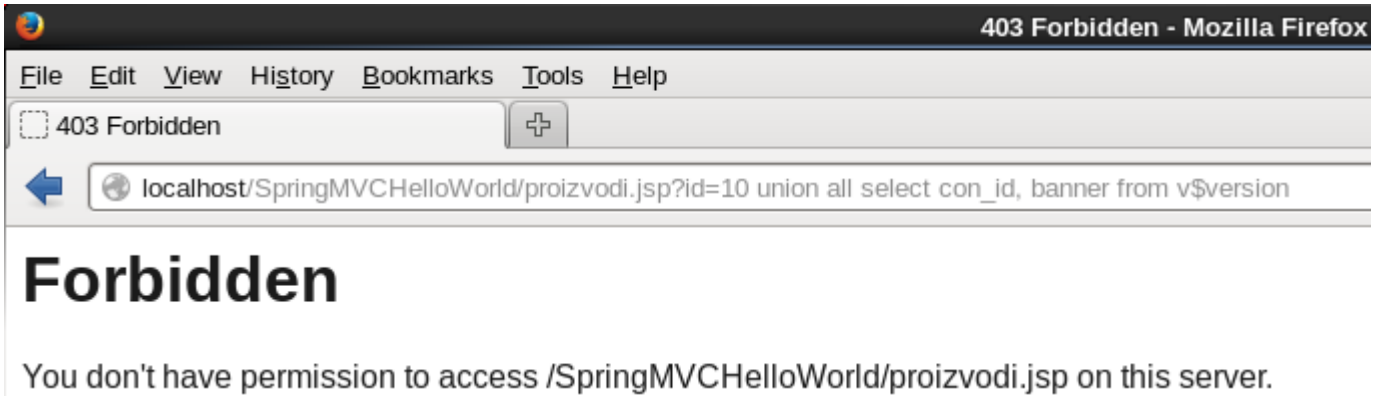
```
SecRule ARGS "union([[:space:]]+)?(all)?|(select.+from)" \
"t:lowercase,deny,log,auditlog,phase:2,status:403,msg:`SQL
Injection napad`, id:100001"
```

# ModSecurity Web Application Firewall

## Pravila (rules) za zaštitu od SQL Injection napada

```
SecRule ARGS "union([[:space:]]+)?(all)?|(select.+from)" \
"t:lowercase,deny,log,auditlog,phase:2,status:403,msg:`SQL
Injection napad`, id:100001"
```

```
::1 - - [18/Sep/2014:14:02:14 +0200] "GET
   /SpringMVCHelloWorld/proizvodi.jsp?id=10%20union%20all%20selec
   t%20con_id,%20banner%20from%20v$version HTTP/1.1" 403 235
```



# ModSecurity Web Application Firewall

## Pravila (rules) za zaštitu od SQL Injection napada

```
SecRule ARGS "union([[:space:]]+)?(all)?|(select.+from)" \
"t:lowercase,deny,log,auditlog,phase:2,status:403,msg:`SQL
Injection napad`, id:100001"
```

**modsec_debug.log:**

```
Second phase starting (dcfg 11dc328).
Input filter: This request does not have a body.
Starting phase REQUEST_BODY.
This phase consists of 1 rule(s).
Recipe: Invoking rule 11fcd60; [file "/usr/local/apache2/conf/crs/modsecurity_crs_100_oracle.conf"] [line "5"] [id "100001"].
Rule 11fcd60: SecRule "ARGS" "@rx union([[:space:]]+)?(all)?|(select.+from)" "phase:2,t:lowercase,deny,log,auditlog,status:403,

T (0) lowercase: "10 union all select con_id, banner from v$version"
Transformation completed in 17 usec.
Executing operator "rx" with param "union([[:space:]]+)?(all)?|(select.+from)" against ARGS:id.
Target value: "10 union all select con_id, banner from v$version"
Ignoring regex captures since "capture" action is not enabled.
Operator completed in 21 usec.
Rule returned 1.
Match, intercepted -> returning.
Access denied with code 403 (phase 2). Pattern match "union([[:space:]]+)?(all)?|(select.+from)" at ARGS:id. [file "/usr/local/
```

# ModSecurity Web Application Firewall

## Regex izrazi za zaštitu od SQL Injection ranjivosti

- SQL je vrlo kompleksan jezik sa različitim dijalektima i proceduralnim jezicima (625 stranica običnog (plain) teksta)
- Regex izrazi postaju izuzetno kompleksni i podložni false-positive detekcijama

```
# SQL injection
#

SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|!REQUEST_COOKIES:/_pk_ref/|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "(?i:\b(?:(?:s(?:t(?:d(?:de
v(_pop|_samp)?)?|r(?:_to_date|cmp))|u(?:b(?:str(?:ing(_index)?)?|(?:dat|tim)e)|m)|e(?:c(?:_to_time|ond)|ssion_user)|ys(?:tem_user|date)|ha(1|2)?|oun
dex|chema|ig?n|pace|qrt)|i(?:s(null|_(free_lock|ipv4_compat|ipv4_mapped|ipv4|ipv6|not_null|not|null|used_lock))?|n(?:et6?_(aton|ntoa)|s(?:ert|tr)|te
rval)?|f(null)?)|u(?:n(?:compress(?:ed_length)?|ix_timestamp|hex)|tc_(date|time|timestamp)|p(?:datexml|per)|uid(_short)?|case|ser)|l(?:o(?:ca(?:l(ti
mestamp)?|te)|g(2|10)?|ad_file|wer)|ast(_day|_insert_id)?|e(?:(?:as|f)t|ngth)|case|trim|pad|n)|t(?:ime(stamp|stampadd|stampdiff|diff|_format|_to_sec
)?|o_(base64|days|seconds|n?char)|r(?:uncate|im)|an)|m(?:a(?:ke(?:_set|date)|ster_pos_wait|x)|i(?:(?:crosecon)?d|n(?:ute)?)|o(?:nth(name)?|d)|d5)|r(
?:e(?:p(?:lace|eat)|lease_lock|verse)|o(?:w_count|und)|a(?:dians|nd)|ight|trim|pad)|f(?:i(?:eld(_in_set)?|nd_in_set)|rom_(base64|days|unixtime)|o(?:
und_rows|rmat)|loor)|a(?:es_(?:de|en)crypt|s(?:cii(str)?|in)|dd(?:dat|tim)e|(?:co|b)s|tan2?|vg)|p(?:o(?:sition|w(er)?)|eriod_(add|diff)|rocedure_ana
lyse|assword|i)|b(?:i(?:t_(?:length|count|x?or|and)|n(_to_num)?)|enchmark)|e(?:x(?:p(?:ort_set)?|tract(value)?)|nc(?:rypt|ode)|lt)|v(?:a(?:r(?:_(?:s
am|po)p|iance)|lues)|ersion)|g(?:r(?:oup_conca|eates)t|et_(format|lock))|o(?:(?:ld_passwo)?rd|ct(et_length)?)|we(?:ek(day|ofyear)?|ight_string)|n(?:
o(?:t_in|w)|ame_const|ullif)|(rawton?)?hex(toraw)?|qu(?:arter|ote)|(pg_)?sleep|year(week)?|d?count|xmltype|hour)\W*\(|\b(?:(?:s(?:elect\b(?:.{1,100}
?\b(?:(?:length|count|top)\b.{1,100}?\bfrom|from\b.{1,100}?\bwhere)|.*?\b(?:d(?:ump\b.*\bfrom|ata_type)|(?:to_(?:numbe|cha)|inst)r))|p_(?:sqlexec|sp
_replwritetovarbin|sp_help|addextendedproc|is_srvrolemember|prepare|sp_password|execute(?:sql)?|makewebtask|oacreate)|ql_(?:longvarchar|variant))|xp
_(?:reg(?:re(?:movemultistring|ad)|delete(?:value|key)|enum(?:value|key)s|addmultistring|write)|terminate|xp_servicecontrol|xp_ntsec_enumdomains|xp_
terminate_process|e(?:xecresultset|numdsn)|availablemedia|loginconfig|cmdshell|filelist|dirtree|makecab|ntsec)|u(?:nion\b.{1,100}?\bselect|tl_(?:fil
e|http))|d(?:b(?:a_users|ms_java)|elete\b\W*?\bfrom)|group\b.*\bby\b.{1,100}?\bhaving|open(?:rowset|owa_util|query)|load\b\W*?\bdata\b.*\binfile|(?:
n?varcha|tbcreato)r|autonomous_transaction)\b|i(?:n(?:to\b\W*?\b(?:dump|out)file|sert\b\W*?\binto|ner\b\W*?\bjoin)\b|(?:f(?:\b\W*?\(\W*?\bbenchmark|
null\b)|snull\b)\W*?\()|print\b\W*?\@\@|cast\b\W*?\()|c(?:(?:ur(?:rent_(?:time(?:stamp)?|date|user)|(?:dat|tim)e)|h(?:ar(?:(?:acter)?_length|set)?|r
)|iel(?:ing)?|ast|r32)\W*\(|o(?:(?:n(?:v(?:ert(?:_tz)?)?|cat(?:_ws)?|nection_id)|(?:mpres)?s|ercibility|alesce|t)\W*\(|llation\W*\(a))|d(?:(?:a(?:t(
?:e(?:(?:_(add|format|sub))?|diff)|abase)|y(name|ofmonth|ofweek|ofyear)?)|e(?:(?:s_(de|en)cryp|faul)t|grees|code)|ump)\W*\(|bms_\w+\.\b)|(?:;\W*?\b(?:
shutdown|drop)|\@\@version)\b|\butl_inaddr\b|\bsys_context\b|'(?:s(?:qloledb|a)|msdasql|dbo)'))" \
        "phase:2,rev:'2',ver:'OWASP_CRS/2.2.9',maturity:'9',accuracy:'8',capture,t:none,t:urlDecodeUni,ctl:auditLogParts=+E,block,msg:'SQL Injection
 Attack',id:'950001',tag:'OWASP_CRS/WEB_ATTACK/SQL_INJECTION',tag:'WASCTC/WASC-19',tag:'OWASP_TOP_10/A1',tag:'OWASP_AppSensor/CIE1',tag:'PCI/6.5.2',
logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',severity:'2',setvar:'tx.msg=%{rule.msg}',setvar:tx.sql_injection_sc
ore=+%{tx.critical_anomaly_score},setvar:tx.anomaly_score=+%{tx.critical_anomaly_score},setvar:tx.%{rule.id}-OWASP_CRS/WEB_ATTACK/SQL_INJECTION-%{ma
tched_var_name}=%{tx.0}"
```

# ModSecurity Web Application Firewall

## Libinjection – ModSecurity 2.7.4+

- C biblioteka
- Ne radi memorijsku alokaciju
- Ne koristi threadove
- Nema vanjske ovisnosti (dependencies)
- >100k provjera u sekundi

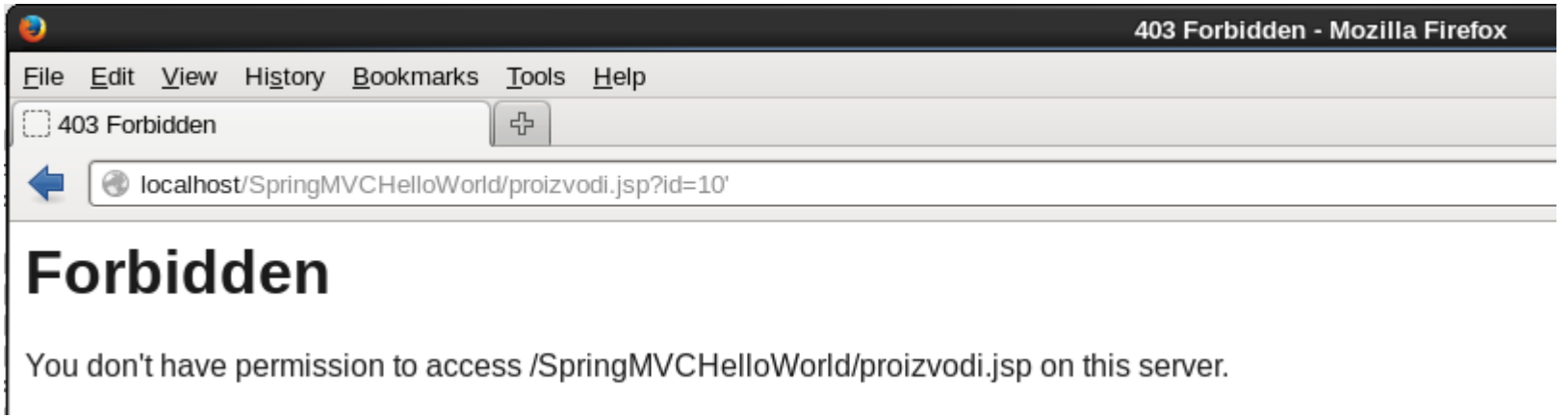
```
SecRule ARGS "@detectSQLi" \
"deny,log,auditlog,phase:2,status:403,msg:`SQL Injection
napad`, id:100002"
```

# ModSecurity Web Application Firewall

## Pravila (rules) za zaštitu od Information Leak ranjivosti

```
SecRule RESPONSE_BODY "ora-\d{5}:"
"t:lowercase,deny,log,auditlog,phase:4,status:403,msg:'Leak',
id:100004"
```

```
127.0.0.1 - - [22/Sep/2014:21:44:50 +0200] "GET
   /SpringMVCHelloWorld/proizvodi.jsp?id=10%27 HTTP/1.1" 403 235
```



LOGIN

19. hroug godišnja konferencija

# Pitanja i Odgovori



software