MODSECURITY

Firewall de Aplicação WEB Open Source

Pedro Henrique C. Sampaio
UFBA - CRI

Quem sou eu?

UFBA

Pedro Sampaio

- Bolsista do CRI/UFBA (Equipe de segurança)
- Membro do Raul Hacker Club
- Organizador da Nullbyte Security Conference

STI 40 anos
Superintendência de Tecnologia da Informação | UFBA

Raul HackerClub

Roteiro

1. O que é?
2. Por que usar?
3. Como é usado?
4. Estatísticas
5. Perguntas

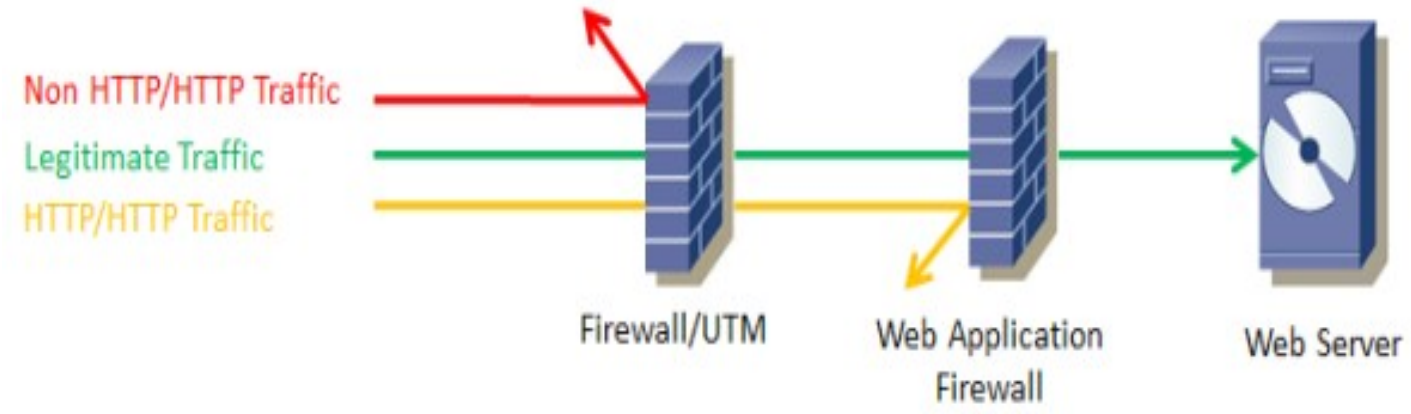
O que é

Web Application Firewall (WAF):

- Analisa e filtra mensagens enviadas ao servidor WEB.
- Atua principalmente sobre o protocolo HTTP
- Pode analisar toda a mensagem HTTP
- Funciona independente da aplicação subjacente

O que é

Web Application Firewall (WAF):



Por que usar WAFs?

- Hoje em dia tudo é web.
- Melhora o tratamento de incidentes.
- Incentiva atitudes pró-ativas.

Modsecurity

modsecurity

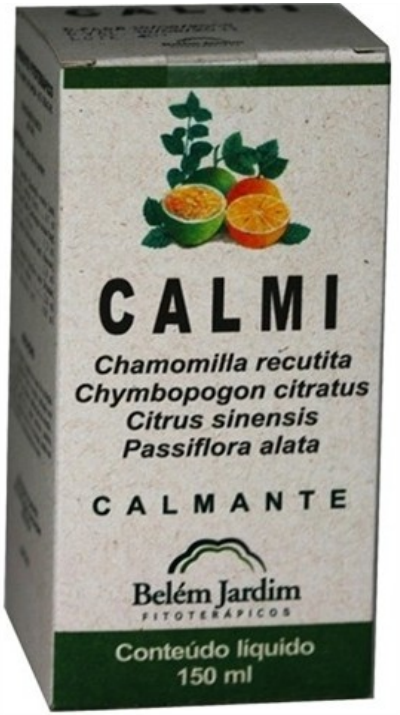
Open Source Web Application Firewall

- WAF criado por Ivan Ristic
- Hoje mantido pela SpiderLabs

Por que usar Modsecurity?

Um Calmante:

- Aumenta a visibilidade
- Flexível
- Virtual Patching
- Comunidade madura
- Sensor/Honeypot



Alternativas

ZORP

Funções

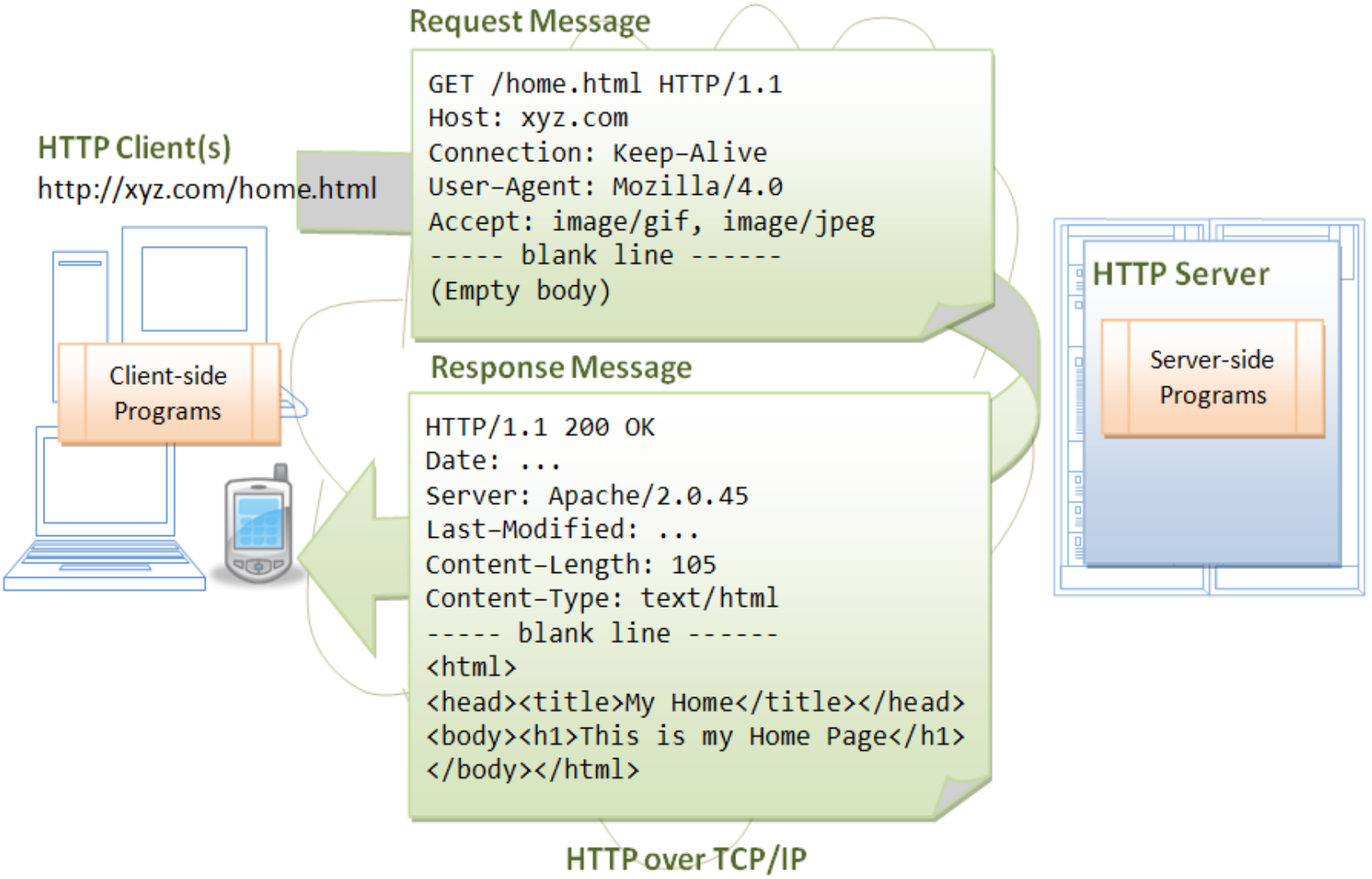
HTTP Intrusion Detection Tool:

- Permite uso de scripts de resposta
- Linguagem extensiva para escrita de regras
- Respostas customizadas (bloqueio, redirecionamento, customização de pacotes, alerta, logging)

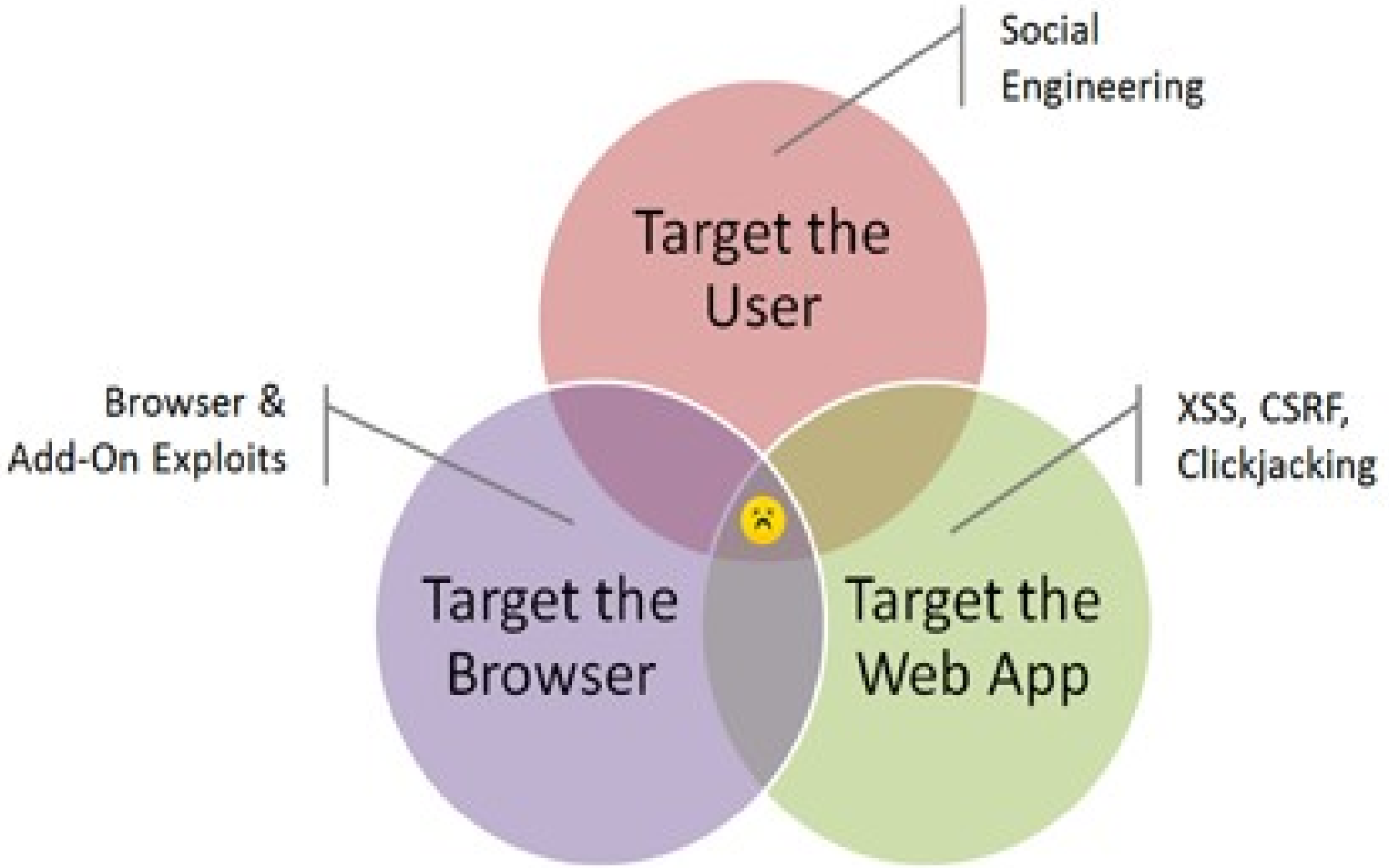
Funções

- Parsing
- Tenta reconhecer o máximo de dados possível, usando uma mentalidade de segurança
- Buffering
- Armazena as mensagens para analisar o contexto de uma transação
- Logging
- Registra de forma extensiva todas as partes de uma transação
- Rule Engine
- Processa os dados da transação e aplica ações

Transação HTTP

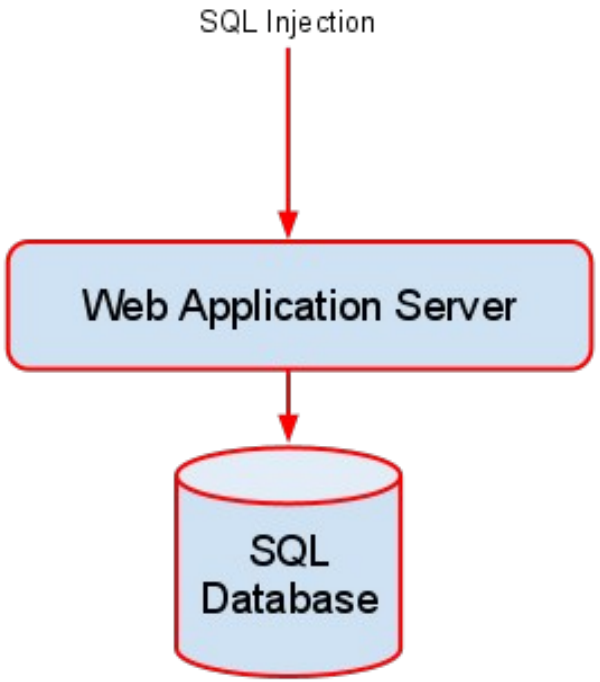


Vetores de Ataque



Vetores de Ataque

SQL Injection:



Login Information

Login ID : test@test.com' or 1=1--

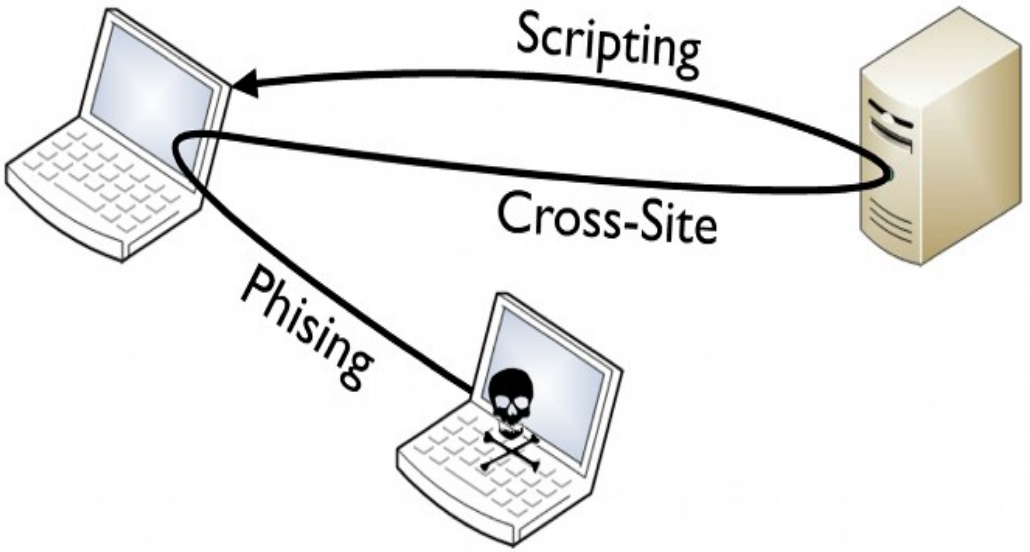
Password :

Login successful

Login Clear

Vetores de Ataque

Cross-Site Scripting (XSS):



http://somepage.com/users.php?register=<script>alert('hacked')</script>

Link

Malicious code

Inspeção

O servidor Apache entrega os dados da transação para o mod security assim que elas fiquem disponíveis.

Cinco fases:

1)Request Header
2)Request Body
3)Response Header
4)Response Body
5)Logs

Inspeção

Anatomia de uma regra:

```
SecRule VARIABLES OPERATOR [TRANSFORMATION_FUNCTIONS, ACTIONS]
```

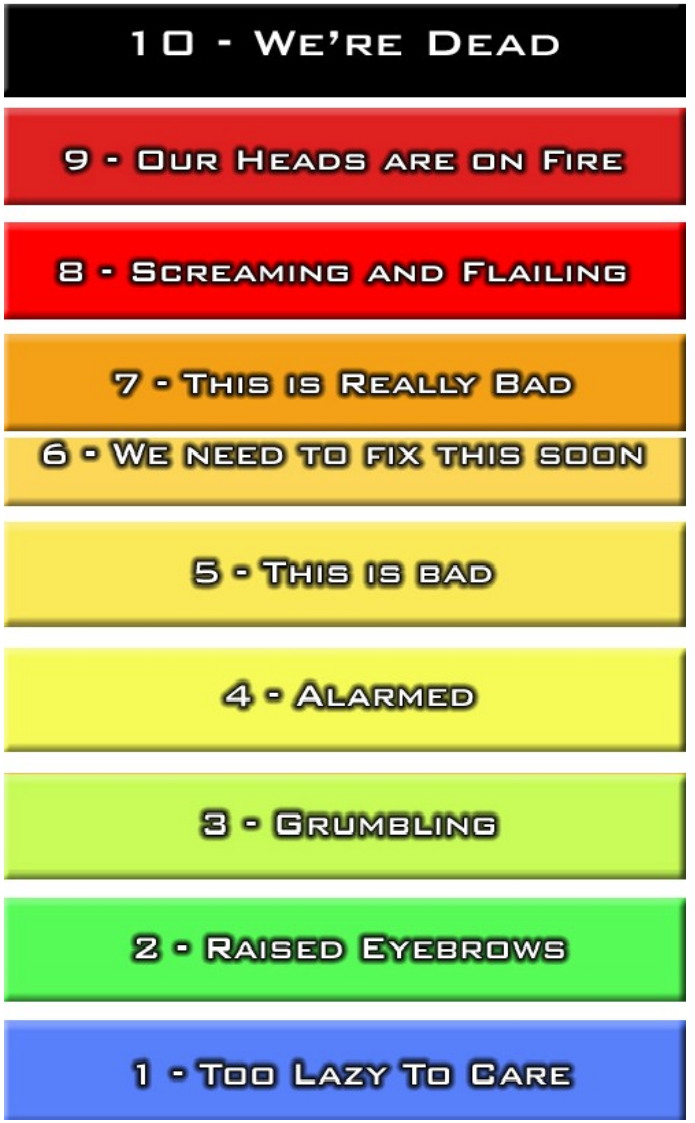
```
#
# -=[ XSS Filters - Category 1 ]=-
# script tag based XSS vectors, e.g., <script> alert(1)</script>
#
SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "(?i)(<script[^>]*>
[\s\S]*?)" \
   "msg:'XSS Filter - Category 1: Script Tag Vector',\
   id:'973336',\
   phase:request,\
   severity:'2',\
   rev:'2',\
   ver:'OWASP_CRS/3.0.0',\
   maturity:'4',\
   accuracy:'9',\
   t:none,t:removeNulls,t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,\
   block,\
   capture,\
   tag:'OWASP_CRS/WEB_ATTACK/XSS',\
   tag:'WASCTC/WASC-8',\
   tag:'WASCTC/WASC-22',\
   tag:'OWASP_TOP_10/A2',\
   tag:'OWASP_AppSensor/IE1',\
   tag:'PCI/6.5.1',\
   logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',\
   setvar:'tx.msg=%{rule.msg}',\
   setvar:tx.xss_score=+%{tx.critical_anomaly_score},\
   setvar:tx.anomaly_score=+%{tx.critical_anomaly_score},\
   setvar:tx.%{rule.id}-OWASP_CRS/WEB_ATTACK/XSS-%{matched_var_name}=%{tx.0}"
```

Inspeção

Tipos de Bloqueio:

- Bloqueio Imediato
- O evento é bloqueado na primeira regra acionada.

- Anomaly Score
- O evento será bloqueado se uma quantidade suficiente de regras seja acionada.

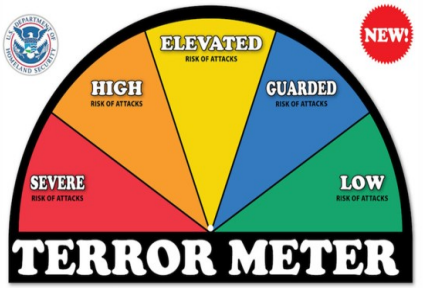


Inspeção

Bloqueio imediato:

- SecRule ARGS "(select|where|group|order|by|union)" "phase:2,t:urlDecodeUni,block,msg:'SQL Injection Attack',id:'959070'"

Inspeção



Anomaly Score

SecRule ARGS "@pm select where group by order union"
"phase:2,pass,nolog,setvar:'tx.sqli_select_statement=%{tx.sqli_select_statement} %{matched_var}'"

SecRule TX:SQLI_SELECT_STATEMENT "@containsWord select"
"phase:2,pass,nolog,setvar:tx.sqli_select_statement_count=+1,setvar:tx.sql_injection_score=+1"

SecRule TX:SQLI_SELECT_STATEMENT "@containsWord where"
"phase:2,pass,nolog,setvar:tx.sqli_select_statement_count=+1,setvar:tx.sql_injection_score=+1"

SecRule TX:SQLI_SELECT_STATEMENT "@contains group by"
"phase:2,pass,nolog,setvar:tx.sqli_select_statement_count=+1,setvar:tx.sql_injection_score=+1"

SecRule TX:SQLI_SELECT_STATEMENT "@contains order by"
"phase:2,pass,nolog,setvar:tx.sqli_select_statement_count=+1,setvar:tx.sql_injection_score=+1"

SecRule TX:SQLI_SELECT_STATEMENT "@containsWord union"
"phase:2,pass,nolog,setvar:tx.sqli_select_statement_count=+1,setvar:tx.sql_injection_score=+1"

SecRule TX:SQLI_SELECT_STATEMENT_COUNT "@ge 3" "phase:2,block,msg:'SQL SELECT Statement Anomaly Detection Alert'"

Inspeção

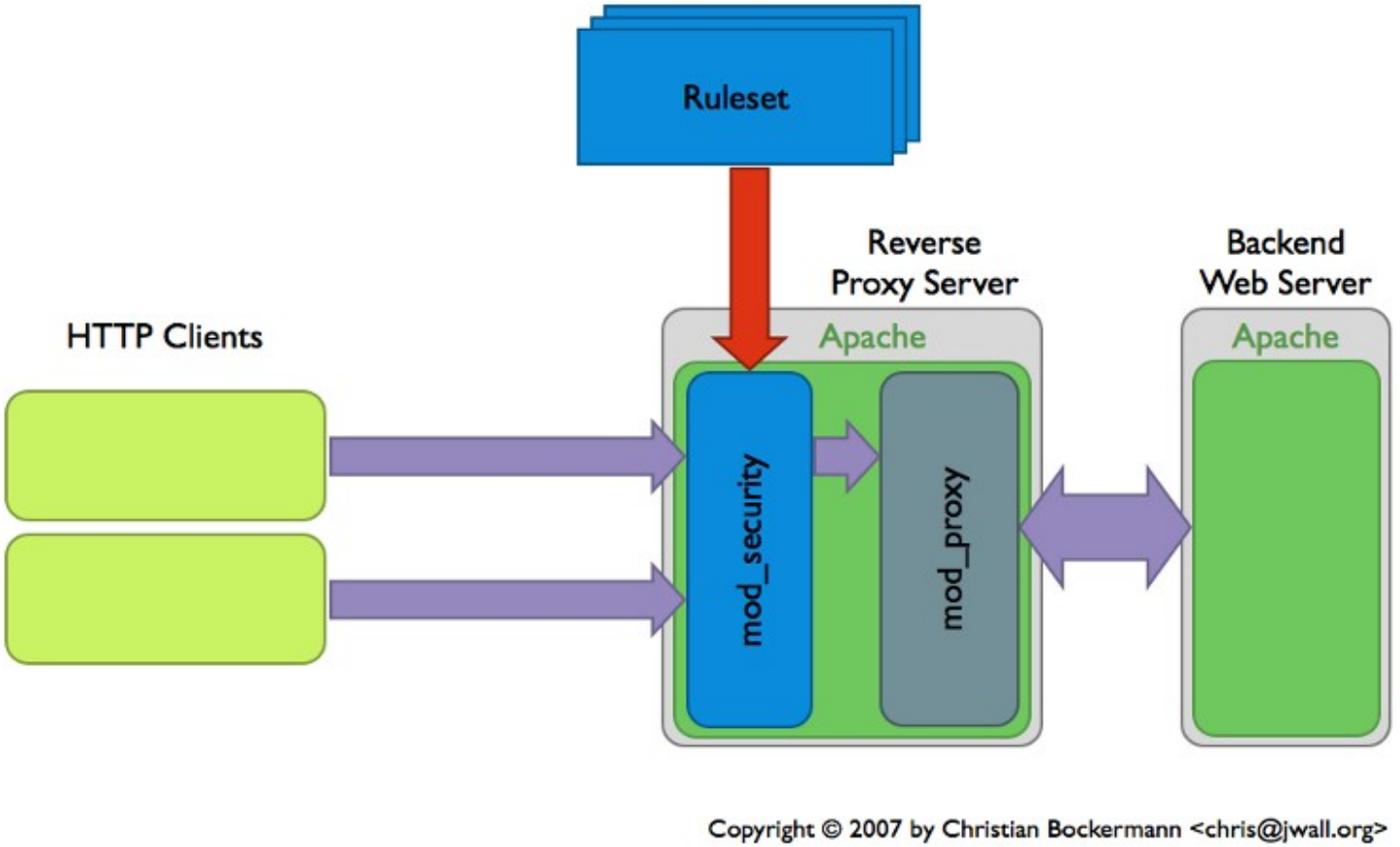
Regras OWASP – Core Rule Set

OWASP

Open Web Application Security Project

Arquitetura

Proxy Reverso ou Embarcado



Logs, Lots of Logs

Logs, Lots of Logs

Apache Logs:

File Edit View Terminal Tabs Help

james@feisty-fawn: /var/log/apache2 | james@feisty-fawn: /var/www

```
james@feisty-fawn:/var/www$ python logscroll.py
127.0.0.1 - - [27/Apr/2007:15:28:42 -0500] "GET /phpmyadmin/favicon.ico HTTP/1.1" 404 337 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:28:45 -0500] "GET /bst/index HTTP/1.1" 200 3397 "http://localhost/bst/index" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:28:46 -0500] "GET /bst/template/original/css/style.css HTTP/1.1" 304 - "http://localhost/bst/index" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:28:52 -0500] "GET / HTTP/1.1" 200 2747 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:14 -0500] "GET /phpmyadmin/favicon.ico HTTP/1.1" 404 337 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:13 -0500] "GET /phpmyadmin/ HTTP/1.1" 200 13610 "http://localhost/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:14 -0500] "GET /phpmyadmin/css/phpmyadmin.css.php?token=bcfc0591b6082a5ad821d4c7491659e1&js_frame=right HTTP/1.1" 200 20339 "http://localhost/phpmyadmin/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:15 -0500] "GET /phpmyadmin/css/print.css?token=bcfc0591b6082a5ad821d4c7491659e1 HTTP/1.1" 200 1063 "http://localhost/phpmyadmin/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:15 -0500] "GET /phpmyadmin/favicon.ico HTTP/1.1" 404 337 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:15 -0500] "GET /phpmyadmin/favicon.ico HTTP/1.1" 404 337 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:18 -0500] "GET /phpmyadmin/ HTTP/1.1" 200 13610 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:18 -0500] "GET /phpmyadmin/favicon.ico HTTP/1.1" 404 337 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:18 -0500] "GET /phpmyadmin/css/phpmyadmin.css.php?token=bcfc0591b6082a5ad821d4c7491659e1&js_frame=right HTTP/1.1" 200 20339 "http://localhost/phpmyadmin/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:19 -0500] "GET /phpmyadmin/favicon.ico HTTP/1.1" 404 337 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
127.0.0.1 - - [27/Apr/2007:15:29:19 -0500] "GET /phpmyadmin/favicon.ico HTTP/1.1" 404 337 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.3) Gecko/20061201 Firefox/2.0.0.3 (Ubuntu-feisty)"
```

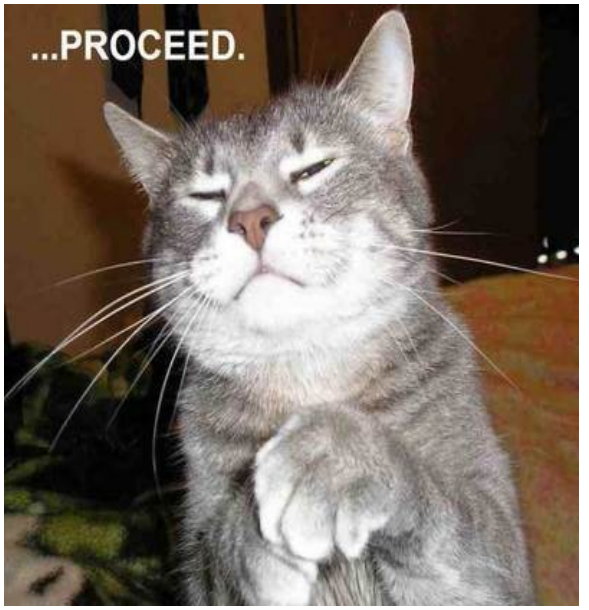
Logs, Lots of Logs

```
--00aee77f-A--
[11/Sep/2012:14:13:41 +0200] UE8q9X8AAQEAADtgIhEAAAAD              55654
--00aee77f-B--
GET /modern-classic HTTP/1.1
User-Agent: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)
Host: www.[redacted].co.za
Accept: */*
Accept-Encoding: deflate, gzip
Range: bytes=0-40960
Connection: keep-alive

--00aee77f-F--
HTTP/1.1 403 Forbidden
Vary: Accept-Encoding
Last-Modified: Sat, 28 Apr 2012 11:34:20 GMT
Accept-Ranges: bytes
Content-Encoding: gzip
Content-Length: 813
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

--00aee77f-H--
Message: Access denied with code 403 (phase 2). String match "bytes=0-" at REQUEST_HEADERS:Range. [file "/etc/modse
curity/activated_rules/modsecurity_crs_20_protocol_violations.conf"] [line "248"] [id "958291"] [rev "2.2.5"] [msg
"Range: field exists and begins with 0."] [data "bytes=0-40960"] [severity "NOTICE"] [tag "RULE_MATURITY/5"] [tag "
RULE_ACCURACY/7"] [tag "https://www.owasp.org/index.php/ModSecurity_CRS_RuleID-958291"] [tag "PROTOCOL_VIOLATION/IN
VALID_HREQ"] [tag "http://www.bad-behavior.ioerror.us/documentation/how-it-works/"]
Action: Intercepted (phase 2)
Stopwatch: 1347365621305848 3649 (- - -)
Stopwatch2: 1347365621305848 3649; combined=193, p1=129, p2=36, p3=0, p4=0, p5=28, sr=31, sw=0, l=0, gc=0
Producer: ModSecurity for Apache/2.6.3 (http://www.modsecurity.org/); OWASP_CRS/2.2.5.
Server: Apache/2.2.22 (Ubuntu)
```

Modsecurity Audit Logs:



Logs, Lots of Logs

WAF-FLE:

WAF-FLE

HOME | EVENTS | FILTER | MANAGEMENT

Logged User: Admin | Logout

Delete Preserve

< Previous 10 of 334 Next >

Rules Match

ID	Severity	Message
960015		Event: Operator EQ matched 0 at REQUEST_HEADERS. Message: Request Missing an Accept Header Tags: | Broken Authentication and Session Management | Failure to restrict URL access | Insufficient Anti-automation
990002		Event: Matched phrase "nikto" at REQUEST_HEADERS:User-Agent. Message: Request Indicates a Security Scanner Scanned the Site Tags: AUTOMATION/SECURITY_SCANNER | Broken Authentication and Session Management | Failure to restrict URL access | Insufficient Anti-automation
990012		Event: Pattern match "(?i(?:c(?:o(?:n(?:t(?:entsmartz|actbot/)|cealed defense|veracrawler)|mpatible(?: ;(?: msie|\\.)|-)|py(?:rightcheck|guard)|re-project/1.0)|h(?:ina(?: local browse 2\\.|claw)|e(?:rrypicker|esebot))|rescent internet toolpak)|w(?:e(?:b(?: (?:downloader|by ..." at REQUEST_HEADERS:User-Agent. Message: Rogue web site crawler Data: Nikto Tags: AUTOMATION/MALICIOUS | Broken Authentication and Session Management | Failure to restrict URL access | Insufficient Anti-automation
981173		Event: Operator GE matched 4 at TX:restricted_sqli_char_count. Message: Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded Data: 7
981176		**Event: Pattern match "(.*)" at TX:960015-PROTOCOL_VIOLATION/MISSING_HEADER-REQUEST_HEADERS. Message: Inbound Anomaly Score Exceeded (Total Score: 26, SQLi=13, XSS=10): Last Matched Message: XSS Attack Detected Data: Last Matched Data: 0**
981204		Event: Operator GE matched 20 at TX:inbound_anomaly_score. Message: Inbound Anomaly Score Exceeded (Total Inbound Score: 26, SQLi=13, XSS=10): XSS Attack Detected

Transaction ID 207303

Sensor	teste
Unique ID	Tpm@@38AAAEAAHhm0woAAAAY
Action	Access denied with code 403 (phase 2)
Score	Total: 26, SQLi: 13, XSS: 10
Source	127.0.0.1 / 54369
Destination	127.0.0.1 / 80
Web App Info	-
Session ID	-
User ID	-
Timestamp	2011-10-15 14:12:28 --0300 (received at 2011-10-15 14:12:28)
Duration	341.035 msec
Server	Apache/2.2.16 (Ubuntu)
Producer	ModSecurity for Apache/2.6.1 (http://www.modsecurity.org/)
Rule Set	core ruleset/2.2.1.

RAW Transaction download

Request Details

HEADER

GET /zorum/index.php?method=<script>alert('Vulnerable')</script> HTTP/1.0
Connection: Keep-Alive
Content-Length: 0
User-Agent: Mozilla/4.75 (Nikto/2.1.1) (Evasions:None) (Test:001454)
Content-Type: application/x-www-form-urlencoded
Host: localhost

Response Details

HEADER

HTTP/1.1 403 Forbidden
Vary: Accept-Encoding
Content-Length: 292
Keep-Alive: timeout=15, max=100
Connection: Keep-Ali
Content-Type: text/html; charset=iso-8859-1

BODY

```
<!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 /zorum/index.php
on this server.</p>
<hr>
<address>Apache/2.2.16 (Ubuntu) Server at localhost Port 80</address>
</body></html>
```

WAF-FLE, version 0.5.1. Released under GNU General Public License, version 2.

Logs, Lots of Logs

- Audit Log:
  - Cada entrada registra uma transação inteira
- Apache Log:
  - Cada linha é uma única requisição
  - Não loga as respostas

Logs, Lots of Logs

Audit Log Parts:

- A Audit log header (mandatório)
- B Request headers
- C Request body
- E Response body
- F Response headers
- H Audit log trailer, informações extras
- I Compact request body, alternativo ao C), exclui arquivos
- K Contém uma lista das regras relacionadas
- Z Seguimento final (mandatório)

Bloqueio

```
--60c21a51-A--
[27/Sep/2013:19:50:25 +0200] aef128f30aa1b043130b5930907f7e575377 127.0.0.1 80 127.0.0.1 80
--60c21a51-B--
POST http://localhost:8080/WebGoat/attack?Screen=31&menu=900 HTTP/1.1
host: localhost:8080
user-agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.24) Gecko/20111109 CentOS/3.6.24-3.el6.centos Firefox/3.6.24
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-us,en;q=0.5
accept-encoding: gzip,deflate
accept-charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
keep-alive: 115
connection: keep-alive
referer: http://localhost:8080/WebGoat/attack?Screen=31&menu=900
cookie: JSESSIONID=C84C0A866BA2234B64C33C383CB1F5EF
authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
content-type: application/x-www-form-urlencoded
content-length: 134

--60c21a51-C--
QTY1=1&QTY2=1&QTY3=1&QTY4=1&field2=4128+3214+0002+1999&field1=111%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&SUBMIT=
Purchase
```

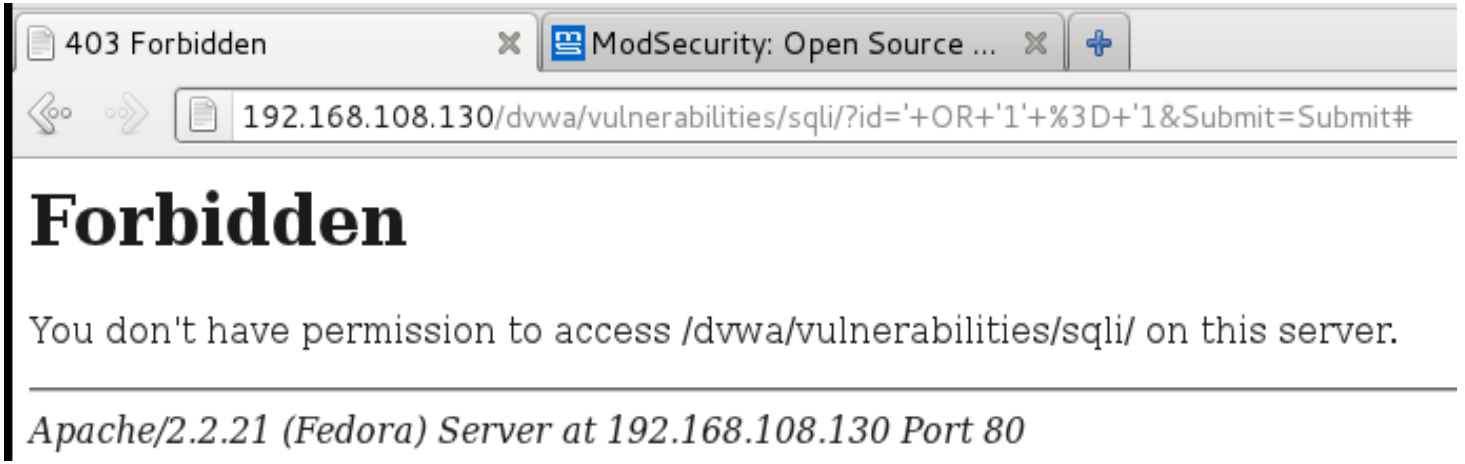
Bloqueio

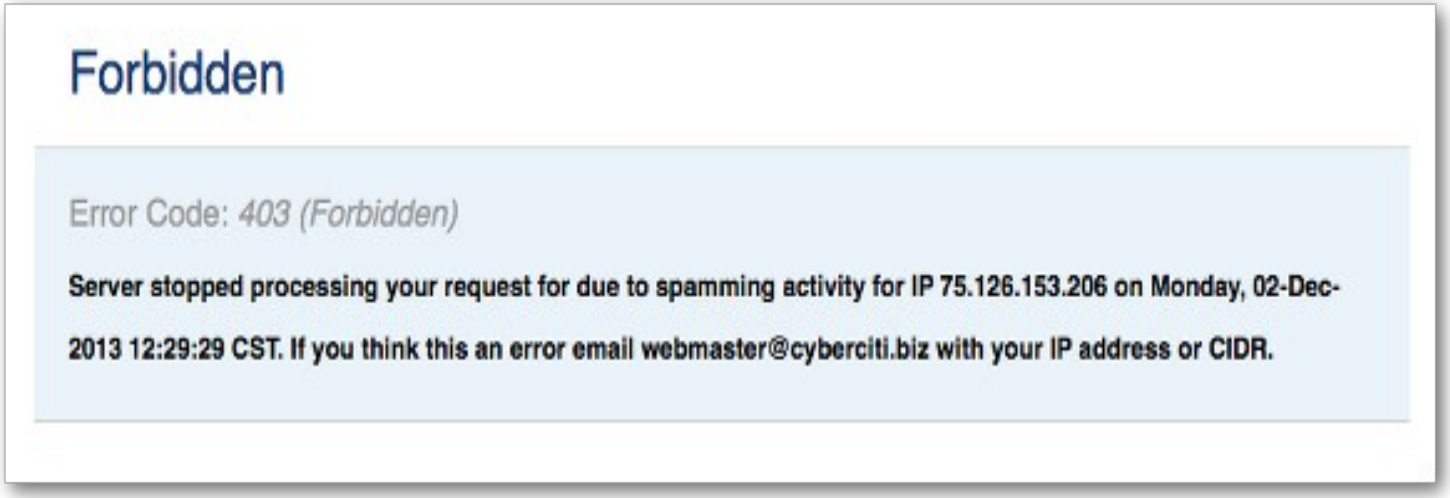
```
--2aabd000-F--
HTTP/1.1 403 Forbidden
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

--2aabd000-H--
Message: Pattern match "^[\d.:]+$" at REQUEST_HEADERS:Host. [file "/etc/httpd/modsecurity.d/base_rules/modsecurity_crs_21_pro
tocol_anomalies.conf"] [line "97"] [id "960017"] [rev "2.0.5"] [msg "Host header is a numeric IP address"] [severity "CRITICA
L"] [tag "PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [tag "http://technet
.microsoft.com/en-us/magazine/2005.01.hackerbasher.aspx"]
Message: Pattern match "\b(\d+) ?(?:=|<>|<=>|<|>) ?\1\b|[\'"\`\´\’\‘](\d+)[\'"\`\´\’\‘] ?(?:=|<>|<=>) ?[\'"\`\´\’\‘]\2\b|[\'"
\`\´\’\‘](\w+)[\'"\`\´\’\‘] ?(?:=|<>|<=>) ?[\'"\`\´\’\‘]\3\b" at ARGS:id. [file "/etc/httpd/modsecurity.d/base_rules/modsecur
ity_crs_41_sql_injection_attacks.conf"] [line "425"] [id "950001"] [rev "2.0.5"] [msg "SQL Injection Attack"] [data "'1' = '1
"] [severity "CRITICAL"] [tag "WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSenso
r/CIE1"] [tag "PCI/6.5.2"]
Message: Pattern match "\b(\d+) ?(?:=|<>|<=>|<|>) ?\1\b|[\'"\`\´\’\‘](\d+)[\'"\`\´\’\‘] ?(?:=|<>|<=>) ?[\'"\`\´\’\‘]\2\b|[\'"
\`\´\’\‘](\w+)[\'"\`\´\’\‘] ?(?:=|<>|<=>) ?[\'"\`\´\’\‘]\3\b" at ARGS:id. [file "/etc/httpd/modsecurity.d/base_rules/modsecur
ity_crs_41_sql_injection_attacks.conf"] [line "425"] [id "950001"] [rev "2.0.5"] [msg "SQL Injection Attack"] [data "'1' = '1
"] [severity "CRITICAL"] [tag "WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSenso
r/CIE1"] [tag "PCI/6.5.2"]
Message: Access denied with code 403 (phase 2). [file "/etc/httpd/modsecurity.d/base_rules/modsecurity_crs_49_enforcement.con
f"] [line "25"] [msg "Anomaly Score Exceeded (score 45): SQL Injection Attack"]
Action: Intercepted (phase 2)
Stopwatch: 1314807605870630 8213 (1041 5312 -)
Producer: ModSecurity for Apache/2.5.12 (http://www.modsecurity.org/); core ruleset/2.0.5.
Server: Apache/2.2.21 (Fedora)

--2aabd000-Z--
```

Bloqueio


403 Forbidden
ModSecurity: Open Source ...
192.168.108.130/dvwa/vulnerabilities/sqli/?id='+OR+'1'+%3D+'1&Submit=Submit#
Forbidden
You don't have permission to access /dvwa/vulnerabilities/sqli/ on this server.
Apache/2.2.21 (Fedora) Server at 192.168.108.130 Port 80


Forbidden
Error Code: 403 (Forbidden)
Server stopped processing your request for due to spamming activity for IP 75.126.153.206 on Monday, 02-Dec-2013 12:29:29 CST. If you think this an error email webmaster@cyberciti.biz with your IP address or CIDR.

Estatísticas

Testes no ambiente UFBA:

- Amostra de 2187 requisições
- Sendo 650 de ataques SQL Injection conhecidos
- Infra com mais de 300 sites

Configuração:

- Modo de bloqueio imediato
- Regras OWASP Core Rule Set

Resultados:

- 1300 eventos bloqueados
- 60% de falsos positivos – 717
- 10% de falsos Negativos – 67
- 587 Ataques legítimos bloqueados

Estatísticas

Testes no ambiente UFBA:

- Amostra de 2187 requisições
- Sendo 650 de ataques SQL Injection conhecidos
- Infra com mais de 300 sites

Configuração:

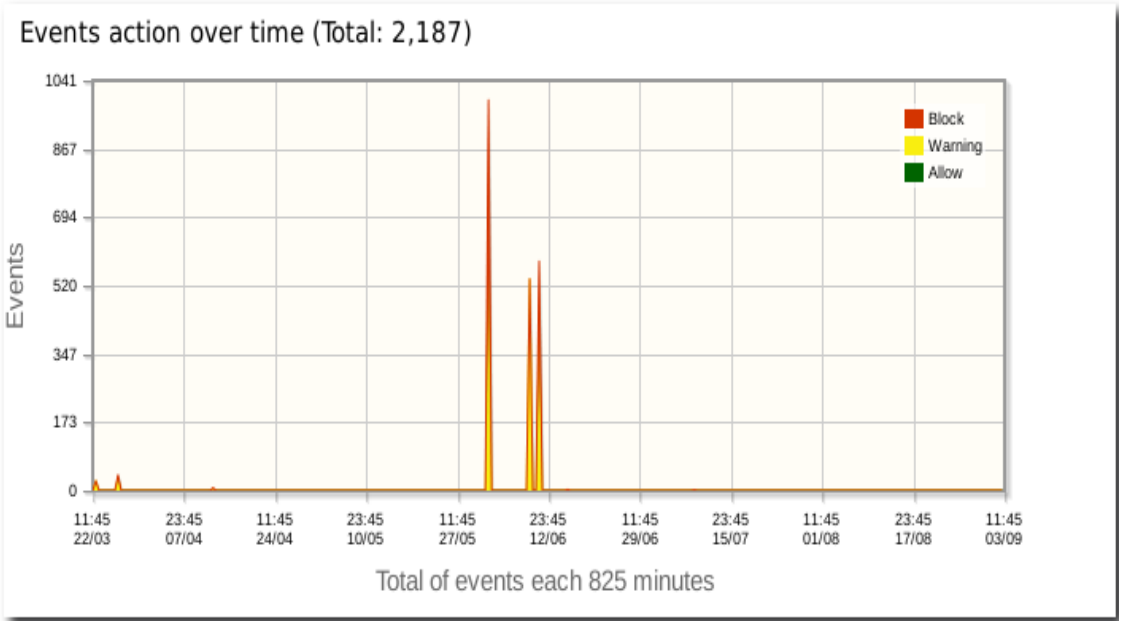
- Modo anomaly + *Bloqueio imediato*
- Regras OWASP Core Rule Set + *Customização scores*

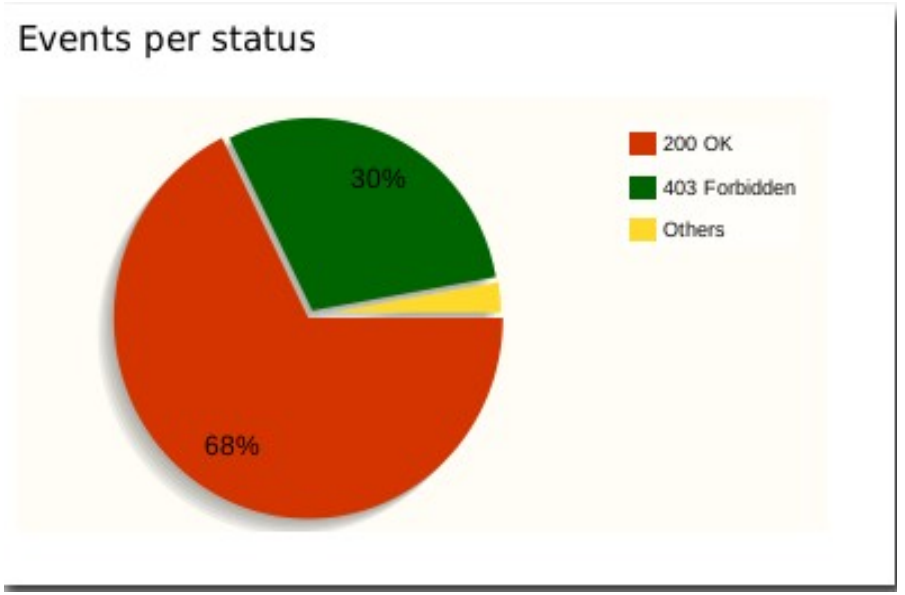
Resultados:

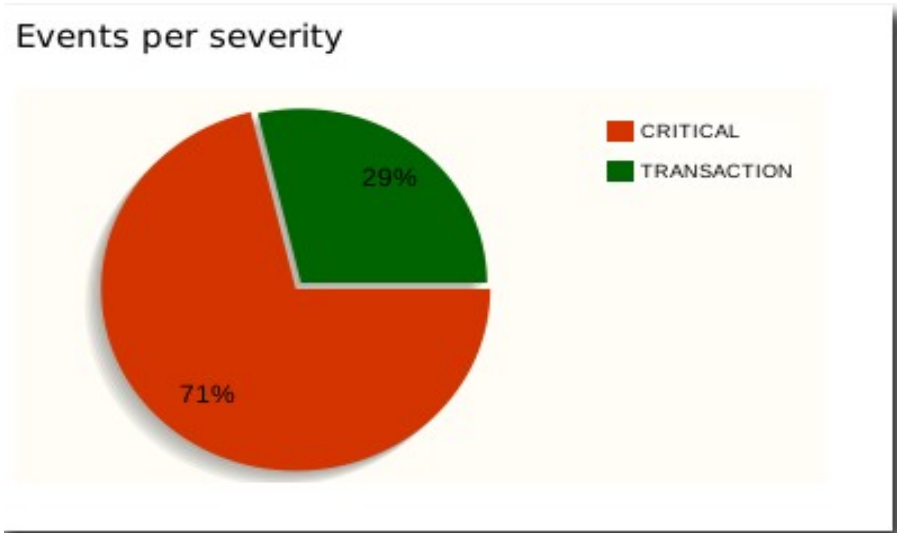
- 681 eventos bloqueados
- 5% de falsos positivos – 31
- 2% de falsos Negativos – 7
- 643 Ataques legítimos bloqueados

Estatísticas

Testes no ambiente UFBA

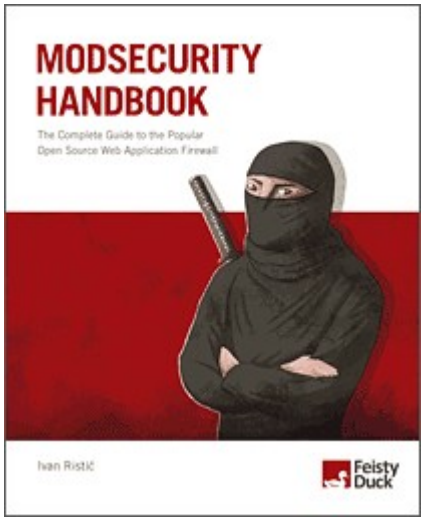


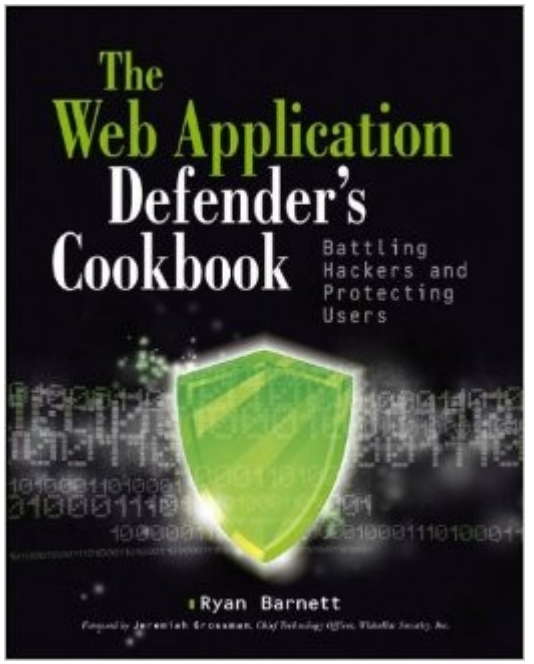




Bibliografia

• Ristic, Ivan. Mod Security handbook: The Complete Guide to the Popular Open Source Web Application Firewall. (2010)
• Barnett, Ryan. The Web Application Defender's Cookbook. (2012)





Equipe

- Pedro Sampaio
- Italo Valcy
- Emerson Macedo

Perguntas

Email: pedro.sampaio@ufba.br
Facebook: Pedro Sampaio
Twitter: @pedrocoba
IRC: irc.freenode.org / Canal #raulhc