OWASP

The Open Web Application Security Project

whoami

OWASP
The Open Web Application Security Project

თემურ მაისურაძე სისტემური ადმინისტრატორი

თემა

modsecurity
Open Source Web Application Firewall

GRENA
GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION

Figure 1. Magic Quadrant for Web Application Firewalls

Source: Gartner (August 2018)

რა არის WAF

OWASP
The Open Web Application Security Project

- What is ModSecurity
- History
  - first version: November 2002
  - ModSecurity 2.0 – 2006
  - ModSecurity from GPLv2 to Apache Software License (ASLv2) - 2011
- Web Server Support
  - Apache
  - LiteSpeed (LSWS)
  - Nginx
  - IIS

GRENA
GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION

OWASP
The Open Web Application Security Project

- How ModSecurity works
- What Can ModSecurity Do?
  - Real-time application security monitoring and access control
  - Virtual patching
  - Full HTTP traffic logging
  - Continuous passive security assessment
  - Web application hardening
- Working Modes, SecRuleEngine
  - Off
  - DetectionOnly
  - On

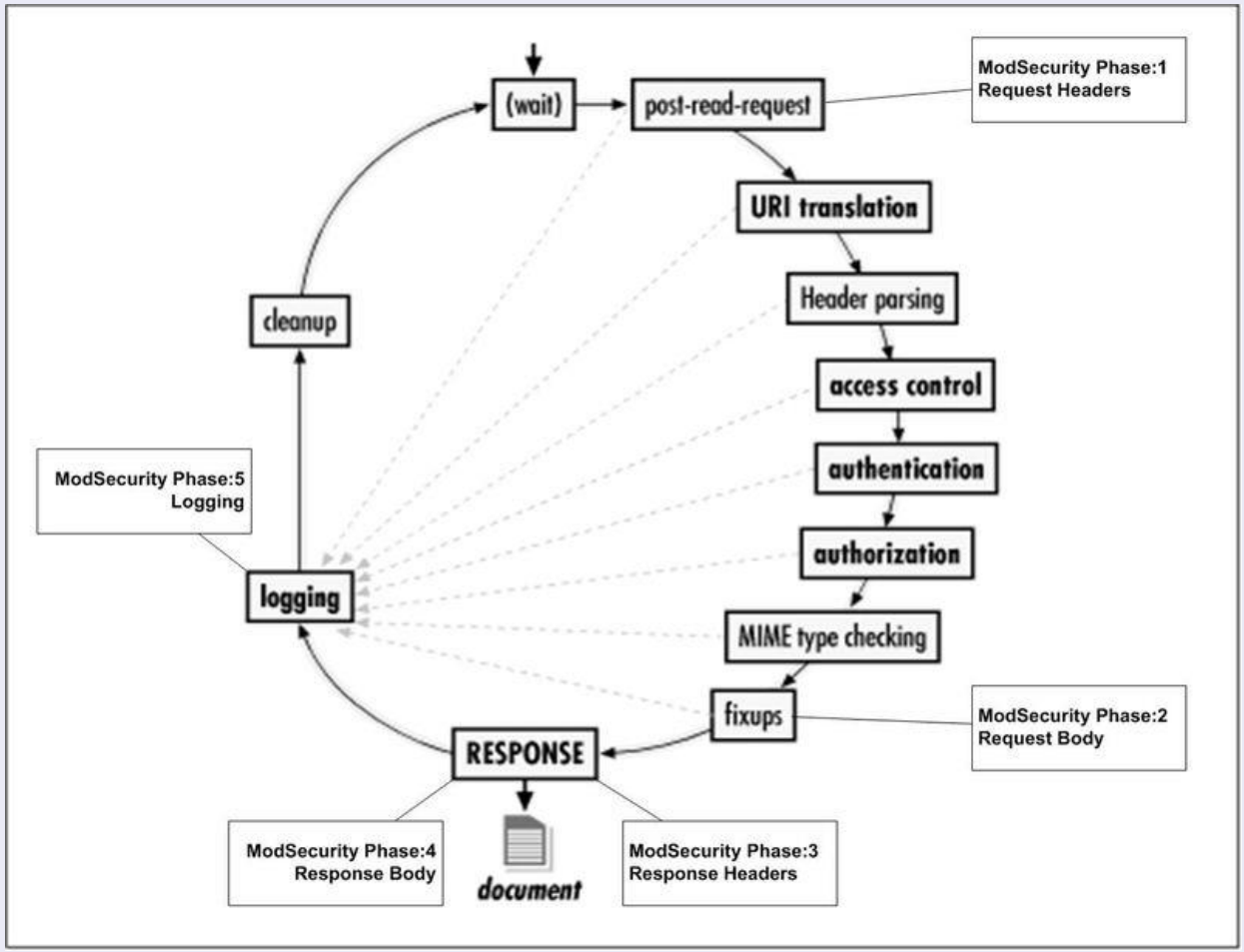
GRENA
GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION

OWASP
The Open Web Application Security Project

- Deployment Options
  - Embedded
  - Reverse proxy
- Main Areas of Functionality
  - Parsing
  - Buffering
  - Logging
  - Rule engine

GRENA
GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION

- ModSecurity Phases
  - Phase 1
  - Phase 2
  - Phase 3
  - Phase 4
  - Phase 5



OWASP
The Open Web Application Security Project

- Rules
  - Vendor specific rules
  - OWASP Core rule set
  - Aplication specific rules
  - Custom rules
  - SecRemoteRules

GRENA
GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION

OWASP
The Open Web Application Security Project

•OWASP Core rule set

Core Rules Content

In order to provide generic web applications protection, the Core Rules use the following techniques:

- **HTTP Protection** - detecting violations of the HTTP protocol and a locally defined usage policy.
- **Real-time Blacklist Lookups** - utilizes 3rd Party IP Reputation
- **Web-based Malware Detection** - identifies malicious web content by check against the Google Safe Browsing API.
- **HTTP Denial of Service Protections** - defense against HTTP Flooding and Slow HTTP DoS Attacks.
- **Common Web Attacks Protection** - detecting common web application security attack.
- **Automation Detection** - Detecting bots, crawlers, scanners and other surface malicious activity.
- **Integration with AV Scanning for File Uploads** - detects malicious files uploaded through the web application.
- **Tracking Sensitive Data** - Tracks Credit Card usage and blocks leakages.
- **Trojan Protection** - Detecting access to Trojans horses.
- **Identification of Application Defects** - alerts on application misconfigurations.
- **Error Detection and Hiding** - Disguising error messages sent by the server.

OWASP

The Open Web Application Security Project

- Rule Example 1

```
SecRule REQUEST_HEADERS|!REQUEST_HEADERS:User-Agent|!REQUEST_HEADERS:Referer|!REQUEST_HEADERS:Cookie \
  "@validateByteRange 32,34,38,42-59,61,65-90,95,97-122" \
  "phase:request,\
   rev:'2',\
   ver:'OWASP_CRS/3.0.0',\
   maturity:'9',\
   accuracy:'9',\
   block,\
   msg:'Invalid character in request headers (outside of very strict set)',\
   id:920274,\
   severity:'CRITICAL',\
   t:none,t:urlDecodeUni,\
   tag:'application-multi',\
   tag:'language-multi',\
   tag:'platform-multi',\
   tag:'attack-protocol',\
   tag:'OWASP_CRS/PROTOCOL_VIOLATION/EVASION',\
   tag:'paranoia-level/4',\
   setvar:'tx.msg=%{rule.msg}',\
   setvar:tx.anomaly_score=+%{tx.critical_anomaly_score},\
   setvar:tx.%{rule.id}-OWASP_CRS/PROTOCOL_VIOLATION/EVASION-%{matched_var_name}=%{matched_var}"
```

OWASP

The Open Web Application Security Project

0	48	`	96		144	À	192
1	49	a	97	'	145	Á	193
2	50	b	98	'	146	Â	194
3	51	c	99	"	147	Ã	195
4	52	d	100	"	148	Ä	196
5	53	e	101	•	149	Å	197
6	54	f	102	–	150	Æ	198
7	55	g	103	—	151	Ç	199
8	56	h	104	˜	152	È	200
9	57	i	105	™	153	É	201
:	58	j	106	š	154	Ê	202
;	59	k	107	›	155	Ë	203
<	60	l	108	œ	156	Ì	204
=	61	m	109		157	Í	205
>	62	n	110	ž	158	Î	206
?	63	o	111	Ÿ	159	Ï	207

GRENA

GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION

- Rule Example 2

```
SecRule REQUEST_URI|ARGS \
        "\/etc\/(passwd|group|gshadow|shadow|motd|shells|hosts|issue|ba
sh|profile|pam|sudoers|rsyslog.conf|syslog.conf|sysctl.conf|inetd.conf|
xinetd.conf)" \
        "id:1111,log,deny,auditlog,logdata:%{matched_var},phase:1,statu
s:403,severity:2,tag:'PATH_TRAVERSAL/ATTACK',msg:'Someone tries to read
 passwd or shadow'"
```

OWASP
The Open Web Application Security Project

•Exeptions

–SecRuleRemoveById

–SecRuleUpdateTargetById 11111 !ARGS:key

–SecRuleUpdateTargetByTag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION" !ARGS:key

–SecRuleUpdateTargetByMsg "Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters" !ARGS:key

–SecRule REMOTE_ADDR "^1\.1\.1\.1$" phase:1,nolog,id:1,allow,ctl:ruleEngine=Off,ctl:auditEngine=Off

–SecRule REMOTE_HOST "@ipmatch 1.1.1.1,2.2.2.2" \

–"id:12345,phase:2,t:none,pass,nolog,noauditlog,ctl:ruleRemovebyID=11111,ctl:ruleRemovebyID=22222,ctl:ruleRemovebyID=33333"

–SecRule REQUEST_URI "^/index\.php "id:10,phase:2,t:none,pass,nolog,noauditlog,ctl:ruleRemovebyID=11111,ctl:ruleRemoveByTag=event-correlation"

GRENA
GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION

- Scan uploaded files with external script (antivirus)

–SecRule FILES_TMPNAMES "@inspectFile /usr/local/bin/modsec-clamscan.pl" "id:351000,rev:1,severity:2,msg:'Malicious File upload attempt',log,deny,auditlog,status:403,t:none"

- Run external program after rule mutch

–SecRule REQUEST_HEADERS:User-Agent "@pmFromFile modsecurity_35_scanners.data" \

–"phase:2,rev:'2.2.5',t:none,t:lowercase,deny,msg:'Request Indicates a Security Scanner Scanned the Site',id:'990002',tag:'AUTOMATION/SECURITY_SCANNER',tag:'WASCTC/WASC-21',tag:'OWASP_TOP_10/A7',tag:'PCI/6.5.10',severity:'4',setvar:'tx.msg=%{rule.msg}',setvar:tx.anomaly_score=+%{tx.warning_anomaly_score},setvar:tx.automation_score=+%{tx.warning_anomaly_score},setvar:tx.%{rule.id}-AUTOMATION/SECURITY_SCANNER-%{matched_var_name}=%{matched_var},exec:/usr/local/bin/modsec2iptables"

OWASP
The Open Web Application Security Project

მადლობა ყურადღებისთვის!

კითხვები?

GRENA
GEORGIAN RESEARCH AND EDUCATIONAL NETWORKING ASSOCIATION