Securing your Web Applications for free with ModSecurity

The FOSS WAF | 07/07/2022 | Anthony Vaccaro

ABOUT

- I’m Anthony Vaccaro, a.k.a. @WaryWolf on twitter
- Systems Engineer on APNIC’s Infrastructure team
- Previous employers – AusCERT, University of Queensland
- Grew up around computers, since the early 90s
- I.T. interests:
  - Self-hosting, decentralisation
  - Linux, FreeBSD, Open Source
  - Security (both offensive and defensive)
- Personal interests:
  - Going fast on two or four wheels
  - Badminton (although I’m not any good at it...)

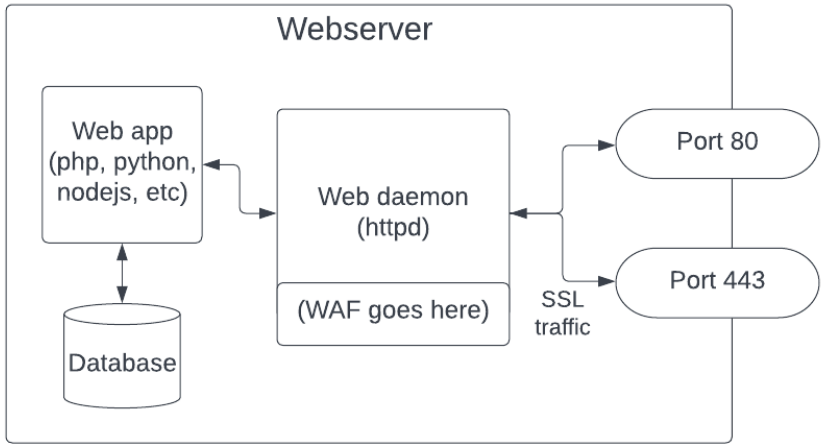
Topics Covered

- Introduction
  - What is a WAF? Do you need one?
- ModSecurity – the FOSS WAF
  - Concepts – rules, tags, scores
  - Understanding rules
  - Writing your own rules
  - Using the OWASP Core Rule Set
- Demo – Linux webserver with vulnerable webapp
  - Reading ModSecurity logs
  - Blocking malicious requests
  - Testing effectiveness with offensive tools
  - Customisation
- How to start using ModSec
- Should you use ModSec?
- Further reading
- Q & A

What is a WAF?

Web Application Firewall

- Operates on requests/responses, not packets/connections
- “Bad” content can be in a request or a response
- Needs to operate on unencrypted traffic – after SSL/TLS termination
- Separate to web application itself
  - There are application-specific WAFs, and generic WAFs



Do I need a WAF?

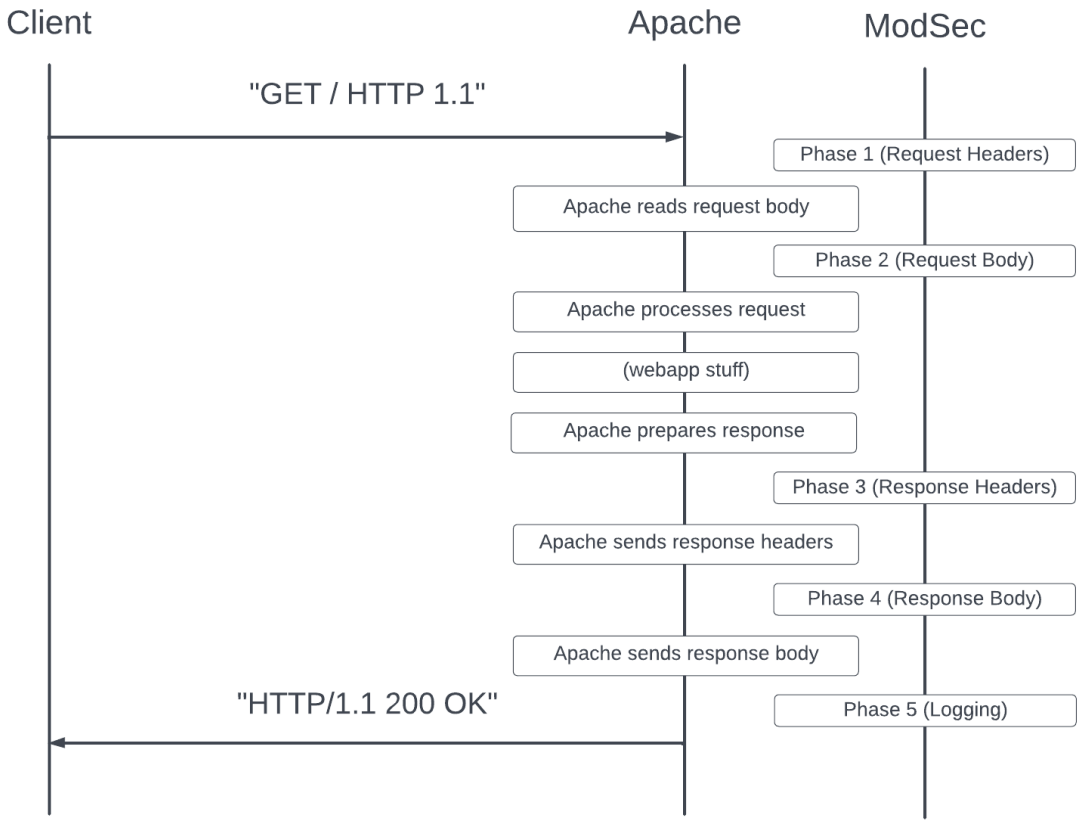
- Most of the time!
- Any form of external input is potential for exploitation
  - Search bar
  - Comments
  - User details (name, email, etc)
- Static websites will benefit less from a WAF
  - Static sites can still leak sensitive information (e.g. config files)
  - If you don’t need dynamic content (e.g. a blog without comments), convert your site to static for increased security & speed

ModSecurity

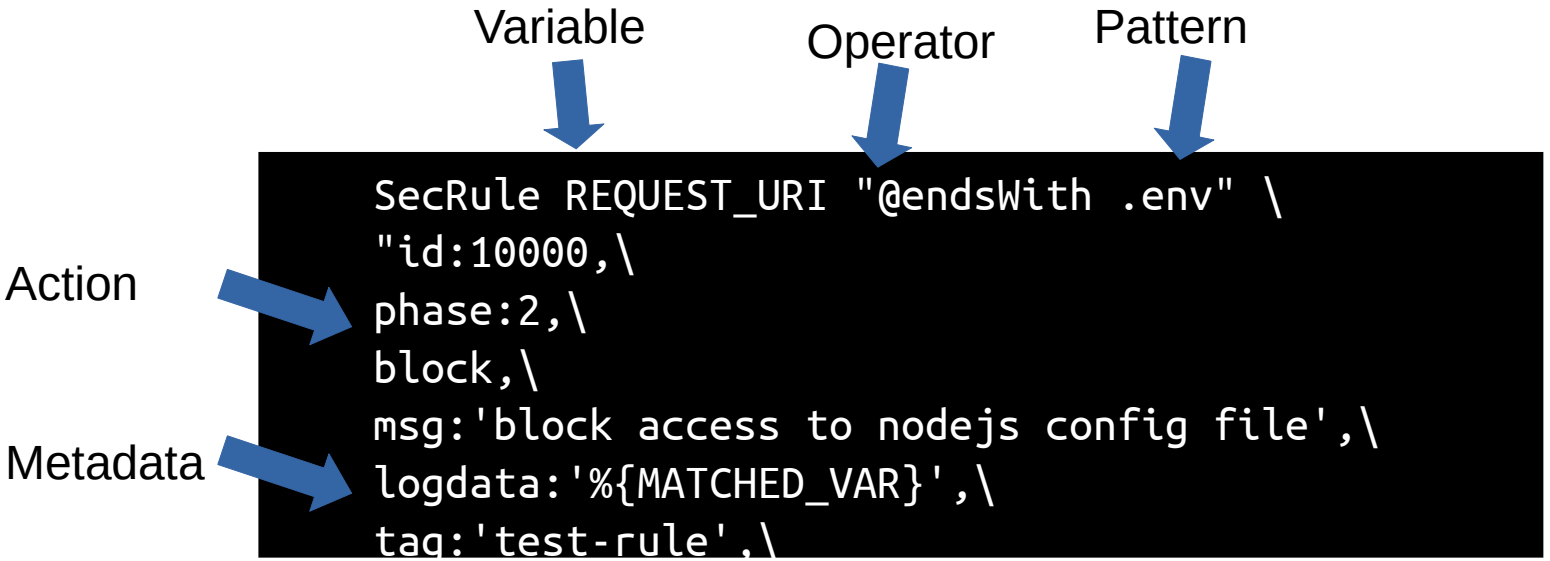
- Free, open source WAF, designed to be used with Apache HTTPD
  - Version 3 of ModSecurity is compatible with IIS & nginx
- Project started in 2002, latest release (3.0.7) on 31st may 2022
- Provides a framework for inspecting web requests & responses
- Rules are based on regular expressions powered by PCRE
- Professional support from TrustWave ending in 2024
  - Community support will continue

https://github.com/SpiderLabs/ModSecurity

How ModSecurity works



Example of a ModSecurity rule



Demo: Example rule

ModSecurity Logs

- Debug log
- Audit logs
- Performance logs
- Apache logs

```
SecDebugLog       /var/log/modsec/debug.log
SecDebugLogLevel  3

SecAuditEngine                RelevantOnly
SecAuditLogRelevantStatus     "^(?:5|4(?!04))"
SecAuditLogParts              ABEFHIJKZ

SecAuditLogType               Concurrent
SecAuditLog                   /var/log/modsec/audit.log
SecAuditLogStorageDir         /var/log/modsec/modsec-audit

LogFormat "[%{%Y-%m-%d %H:%M:%S}t.%{usec_frac}t] %h \"%r\" %>s \"%
{Referer}i\" %v %p %R [%I %O %{ratio}n%%] [%D %{ModSecTimeIn}e %
{ApplicationTime}e %{ModSecTimeOut}e]  [%{ModSecAnomalyScoreIn}e %
{ModSecAnomalyScoreOut}e]" extended
```

```
[2022-07-06 19:50:52] 10.0.2.2 "GET /.env HTTP/1.1" 403 "-" modsecdemo 80 [669 469] [5729 2178 0 0]  [5 0]
[2022-07-06 19:50:59] 10.0.2.2 "GET /index.html HTTP/1.1" 404 "-" modsecdemo 80 [647 468] [7861 4783 536 457]  [0 0]
```

Writing rules looks hard...

- “I don’t want to create hundreds of rules like that!”
- “I don’t know what kinds of exploits I need to be protecting against…”
- “Hasn’t someone done this already? I’m just running Wordpress after all”
- “Can’t I just download a pre-written list of rules?”
- Actually…. Yes, you can!

The OWASP Core Rule Set

OWASP - The Open Web Application Security Project

- Pre-written rules (over 600) to protect against all common web exploits
- Generic, application-specific & OS/platform-specific rules
  - Rules are well-organised & categorised
  - Modsec lets you disable groups of rules as needed
- Free! Open source! Ready to download!

https://coreruleset.org

The OWASP Core Rule Set

```
REQUEST-901-INITIALIZATION.conf
REQUEST-903.9001-DRUPAL-EXCLUSION-RULES.conf
REQUEST-903.9002-WORDPRESS-EXCLUSION-
RULES.conf
REQUEST-903.9003-NEXTCLOUD-EXCLUSION-
RULES.conf
REQUEST-903.9004-DOKUWIKI-EXCLUSION-RULES.conf
REQUEST-905-COMMON-EXCEPTIONS.conf
REQUEST-910-IP-REPUTATION.conf
REQUEST-911-METHOD-ENFORCEMENT.conf
REQUEST-912-DOS-PROTECTION.conf
REQUEST-913-SCANNER-DETECTION.conf
REQUEST-920-PROTOCOL-ENFORCEMENT.conf
REQUEST-921-PROTOCOL-ATTACK.conf
REQUEST-930-APPLICATION-ATTACK-LFI.conf
REQUEST-931-APPLICATION-ATTACK-RFI.conf
REQUEST-932-APPLICATION-ATTACK-RCE.conf
REQUEST-933-APPLICATION-ATTACK-PHP.conf
REQUEST-934-APPLICATION-ATTACK-NODEJS.conf
REQUEST-941-APPLICATION-ATTACK-XSS.conf
REQUEST-942-APPLICATION-ATTACK-SQLI.conf
REQUEST-944-APPLICATION-ATTACK-JAVA.conf
RESPONSE-950-DATA-LEAKAGES.conf
RESPONSE-952-DATA-LEAKAGES-JAVA.conf
```

```
SecRule REQUEST_FILENAME "@pmFromFile restricted-files.data" \
    "id:930130,\
    phase:2,\
    block,\
    capture,\
    t:none,t:utf8toUnicode,t:urlDecodeUni,\
    t:normalizePathWin,t:lowercase,\
    msg:'Restricted File Access Attempt',\
    logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %
{MATCHED_VAR}',\
    tag:'application-multi',\
    tag:'language-multi',\
    tag:'platform-multi',\
    tag:'attack-lfi',\
    tag:'paranoia-level/1',\
    tag:'OWASP_CRS',\
    tag:'capec/1000/255/153/126',\
    tag:'PCI/6.5.4',\
    ver:'OWASP_CRS/3.3.2',\
    severity:'CRITICAL',\
    setvar:'tx.lfi_score=+%{tx.critical_anomaly_score}',\
    setvar:'tx.anomaly_score_pl1=+%{tx.critical_anomaly_score}'"
```

Anomaly scoring

- Anomaly scoring is part of the Core Rule Set
- Each rule has a severity
- Each severity has a score (0 to 5)
- It’s possible to block requests or responses above a score
- Separate scores for requests and responses

```
SecAction \
 "id:900110,\
  phase:1,\
  nolog,\
  pass,\
  t:none,\
  setvar:tx.inbound_anomaly_score_threshold=10,\
```

Whitelisting

- What if you want to disable a rule? Perhaps temporarily?

- You find the rule ID or tag (by looking at the source or through the debug log)
- In your modsecurity.conf file (after CRS includes), add the following:
  - `SecRuleRemoveById <RULE-ID>`
  - `SecRuleRemoveByTag “<TAG>”`

```
# Disabled, too many false positives
SecRuleRemoveById 953110

# Disabled, we are using linux
SecRuleRemoveByTag "platform-windows"
```

Advanced Whitelisting

- What if you only want a rule to run *sometimes?*

- e.g. you have a page where legitimate traffic trips rules
  - But you don’t want to disable the rule everywhere...
- In modsecurity.conf, after CRS includes, add:

```
SecRule REQUEST_URI "@beginsWith /old-site/" \
    "phase:1,nolog,pass,id:10003,ctl:ruleRemoveById=953110"
```

(yes, this is a rule that disables another rule)

Demo – running ModSecurity on Linux

- Pray to demo gods...

Easing yourself in

- How to start using modsec?

- Install on your test/dev infra first
- `SecRuleEngine DetectionOnly`
- Observe logs & whitelist rules as needed
  - `grep -v \[0 0\] httpd-modsec.log`
  - `SecRuleRemoveByTag`
- Install on prod, copy your prepared config over
- Observe & whitelist against prod traffic
- Choose an anomaly threshold
- `SecRuleEngine On`

Easing yourself in

- How to start using modsec?

- Worried about blocking everything?
  - Set '`SecRuleEngine DetectionOnly`' on first run – no blocking, just logging
- Busy site? Worried about server load?
  - '`sampling_percentage`' in crs-setup.conf
  - Enable perf logging
- Blocking thresholds – start high
  - You can generally set request threshold lower than response
  - Pay attention to which rules are triggering in the debug log

Should you use ModSecurity?

- If you have:

- Dynamic, self-hosted websites (e.g. Wordpress)
- Limited budget
- Basic sysadmin knowledge
- Some free time (both initial & ongoing)

Then yes!

- If you have:

- No self-hosted websites (e.g. SaaS/static only)
- Existing Cloudflare license
- Limited free time

Then no!

Further Reading

- Where to look next?

- Official documentation for ModSec & CRS: https://modsecurity.org & https://coreruleset.org
- ModSec reference manual on Github: https://github.com/SpiderLabs/ModSecurity/wiki/
- Christian Folini's tutorials: https://www.netnea.com/cms/apache-tutorials/
- AppSec 2017 talk: Introducing CRS 3.0 by Christian Folini:
- https://www.youtube.com/watch?v=eO9gBAmKS58

QUESTIONS?

Thank You!