Introduction to the OWASP ModSecurity Core Rule Set Project

Andrew Howe

OWASP Dorset

Thursday 1 June 2023
Talk Overview

• Why use a WAF? (What is a WAF?)
• WAF engines
• WAF rules: Enter the Core Rule Set (CRS)
• How CRS works
• Other bits we do as a project
Who am I and Why am I Here?

Andrew Howe

Technical Author/Architect

LOADBALANCER
Why Use a WAF?
Why Use a WAF?
Why Use a WAF?

- Network firewalls
- DMZ / network segmentation
- WAF
- Host firewall
- Data validation
Engine

modsecurity
Open Source Web Application Firewall
Engine

“SecLang”

SecRule VARIABLES OPERATOR ACTIONS
Engine

“SecLang”

SecRule VARIABLES OPERATOR ACTIONS

SecRule REQUEST_HEADERS "@rx pear|apple" "id:1,deny"
Engine

[Coraza logo]

WEB APPLICATION FIREWALL
Rules

OWASP ModSecurity Core Rule Set

THE 1ST LINE OF DEFENSE
Rules

- REQUEST-911-METHOD-ENFORCEMENT.conf
- REQUEST-913-SCANNER-DETECTION.conf
- REQUEST-920-PROTOCOL-ENFORCEMENT.conf
- REQUEST-932-APPLICATION-ATTACK-RCE.conf
- REQUEST-933-APPLICATION-ATTACK-PHP.conf
Rules

REQUEST-941-APPLICATION-ATTACK-XSS.conf
REQUEST-942-APPLICATION-ATTACK-SQLI.conf
REQUEST-944-APPLICATION-ATTACK-JAVA.conf
REQUEST-949-BLOCKING-EVALUATION.conf
Rules

- RESPONSE-951-DATA-LEAKAGES-SQL.conf
- RESPONSE-953-DATA-LEAKAGES-PHP.conf
- RESPONSE-954-DATA-LEAKAGES-IIS.conf
- RESPONSE-955-WEB-SHELLS.conf
Rules

Include modsecurity.conf-recommended
Include coreruleset-3.3.4/crs-setup.conf
Include coreruleset-3.3.4/rules/*\.conf
SecRule REQUEST_HEADERS:Content-Length "!@rx ^\d+$" \\ 
\"id:920160,\\
phase:1,\\
block,\\
msg:'Content-Length HTTP header is not numeric',\\
logdata:'%{MATCHED_VAR}',\\
tag:'paranoia-level/1',\\
ver:'OWASP_CRS/4.0.0-rc1',\\
severity:'CRITICAL',\\
setvar:'tx.inbound_anomaly_score_pl1=+%{tx.critical_anomaly_score}''
Rules

SecRule REQUEST_HEADERS:Content-Length "!@rx ^\d+$" \
  "id:920160,\nphase:1,\nblock,\nmsg:'Content-Length HTTP header is not numeric',\nlogdata:'%{MATCHED_VAR}',\ntag:'paranoia-level/1',\nver:'OWASP_CRS/4.0.0-rc1',\nseverity:'CRITICAL',\nsetvar:'tx.inbound_anomaly_score_pl1=+%{tx.critical_anomaly_score}''
Rules

SecRule REQUEST_HEADERS:Content-Length "!@rx ^\d+$" \n  "id:920160,\n  phase:1,\n  block,\n  msg:'Content-Length HTTP header is not numeric',\n  logdata:'${MATCHED_VAR}',\n  tag:'paranoia-level/1',\n  ver:'OWASP_CRS/4.0.0-rc1',\n  severity:'CRITICAL',\n  setvar:'tx.inbound_anomaly_score_pl1=+%{tx.critical_anomaly_score}''
Rules

SecRule REQUEST_HEADERS:Content-Length "!*@rx ^\d+$" \
 "id:920160,\n phase:1,\n block,\n msg:'Content-Length HTTP header is not numeric',\n logdata:'%{MATCHED_VAR}',\n tag:'paranoia-level/1',\n ver:'OWASP_CRS/4.0.0-rc1',\n severity:'CRITICAL',\n setvar:'tx.inbound_anomaly_score_pl1=+%{tx.critical_anomaly_score}''
Rules

SecRule REQUEST_HEADERS:Content-Length "!@rx ^\d+$" \
"id:920160,\nphase:1,\nblock,\nmsg:'Content-Length HTTP header is not numeric',\nlogdata:'%{MATCHED_VAR}',\ntag:'paranoia-level/1',\nver:'OWASP_CRS/4.0.0-rc1',\nseverity:'CRITICAL',\nsetvar:'tx.inbound_anomaly_score_pl1=+%{tx.critical_anomaly_score}'''
The Humans Behind the Rules!
Who Uses CRS?

OWASP ModSecurity Core Rule Set
THE 1ST LINE OF DEFENSE
Who Uses CRS?

OWASP ModSecurity Core Rule Set
THE 1ST LINE OF DEFENSE
Why is CRS So Widely Used?

OWASP ModSecurity Core Rule Set
THE 1ST LINE OF DEFENSE
How CRS Works

OWASP ModSecurity Core Rule Set

THE 1ST LINE OF DEFENSE
Anomaly Scoring
Anomaly Scoring
Anomaly Scoring

Rule 1
CRITICAL
MATCH (Add 5)

Rule 2
NOTICE
MATCH (Add 2)

Rule 3
NOTICE
NO MATCH

Blocking evaluation
DENY

Inbound anomaly score threshold: 5
Rule Set Configuration
Paranoia Levels

PL 4

Very aggressive rules
False positives likely

PL 3

Less aggressive rules
False positives rare

PL 2

PL 1
False Positives and Tuning
False Positives and Tuning

01234567896 andy.smith@company.co.uk
False Positives and Tuning

01234567896 andy.smith@company.co.uk
False Positives and Tuning

01234567896 andy.smith@company.co.uk
Rule Exclusion Packages

- Drupal
- WordPress
- Nextcloud
- DokuWiki
- cPanel
- XenForo
- phpBB
- phpMyAdmin
Plugins

• Automatic (opportunistic) character decoding
• Anti-User Agent bot spoofing (e.g. attackers pretending to be a Google bot)
• Legacy DoS protection
Docker Containers

- Apache
- Nginx
CRS Sandbox

- https://sandbox.coreruleset.org/


930120  PL1 OS File Access Attempt
932160  PL1 Remote Command Execution: Unix Shell Code Found
949110  PL1 Inbound Anomaly Score Exceeded (Total Score: 10)
980130  PL1 Inbound Anomaly Score Exceeded (Total Inbound Score: 10 - SQLI=0,XSS=0,RFI=0,LFI=5,RCE=5,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 10, 0, 0, 0
And More Cool Stuff We Do!

• Google Summer of Code
• Documentation and PR
• Tooling for crazy regular expressions
• Go-FTW
• CRS Status Page
The Future

- CRS 4
- CRS 3.3.5
Conclusion