verizon
digital media services

OWASP
Open Web Application Security Project

Core Rule Set for the Masses

Lessons from taming ModSecurity rules at massive scale

Tin Zaw, Verizon
Robert Whitley, Verizon

Goals

- Understanding ModSecurity
- Setting realistic expectations
- Tuning, tuning and continuous tuning

By practitioners, for practitioners and the curious

Agenda

- Web Application Firewalls
- ModSecurity
- Getting Ready for WAF
- Core Rule Set
- Fine-tuning Process
- Safe Exclusion Techniques
- Core Rule Set 3.0

Verizon Edgecast Network

40 Tbps
Network Capacity

100+
PoPs

5
Continents

3K+
Interconnects

Web Application Firewalls

- Operate at HTTP layer
- Address application level security issues
    - E.g., OWASP Top 10 risks
- Also operate on network level information

WAF Benefits

- Attack Detection
- Attack Mitigation
- Virtual Patching
- Policy Enforcement

Can be minimally effective in mitigating automated attacks (by dumb bots)

ModSecurity - A brief history

- Open Source
- Developed by Ivan Ristić in 2002
- First created for Apache® 1.3.x
    - Later ported to Windows® IIS and NGINX
- Uses SecRules language
- Allows modular rule sets to be added
- Core Rule Set
    - The standard for WAF rules

ModSecurity Architecture

- **Two Components**
  - Engine (2.9.2, 3.0.0-RC1)
  - Core Rule Set (Latest: 3.0.2)
- **Two Deployment Modes**
  - Embedded
  - Reverse Proxy

ModSecurity Principles

- Flexibility
- Passiveness
- Predictability

ModSecurity Capabilities

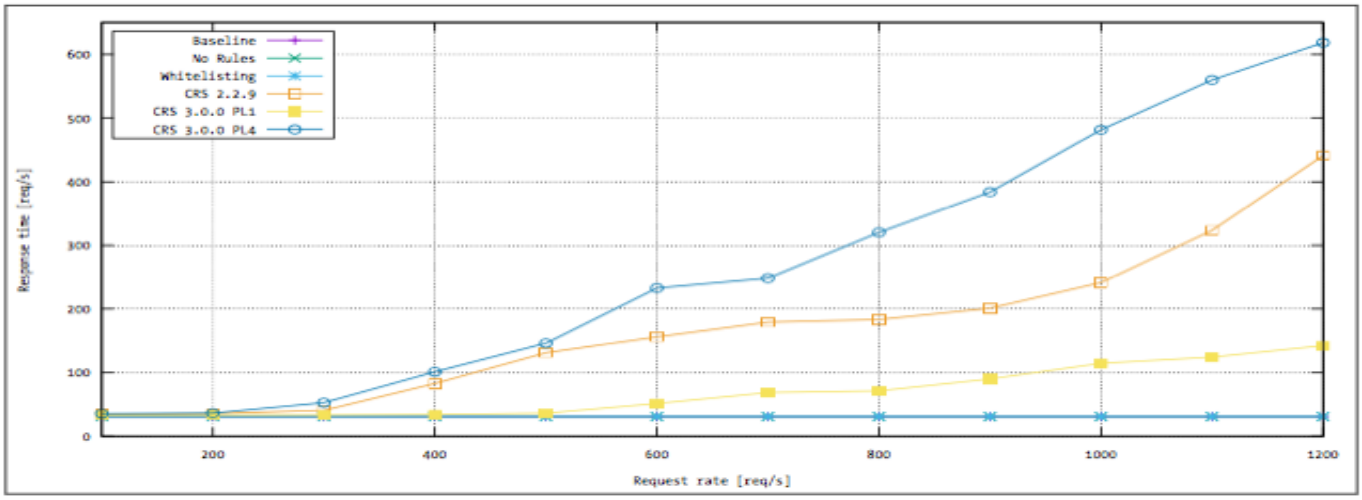
- Monitoring
- Full HTTP Logging
- Attack Detection & Mitigation
- Virtual Patching
- Access Control
    - Black/whitelisting of URLs/IPs
- Attack Surface Reduction
    - Restricting HTTP versions, verbs

Performance Considerations

- Understand time-intensive activities
    - File scans, parsing, external operations, noisy rules, excessive logs
- Minimize false positives
- Scale linearly
    - Leverage load balancer, cloud, CDN, etc.
- Quick propagation of configuration changes and events

Holy Grail: Fixed and minimal performance impact per transaction as your traffic grows

Response Time Test



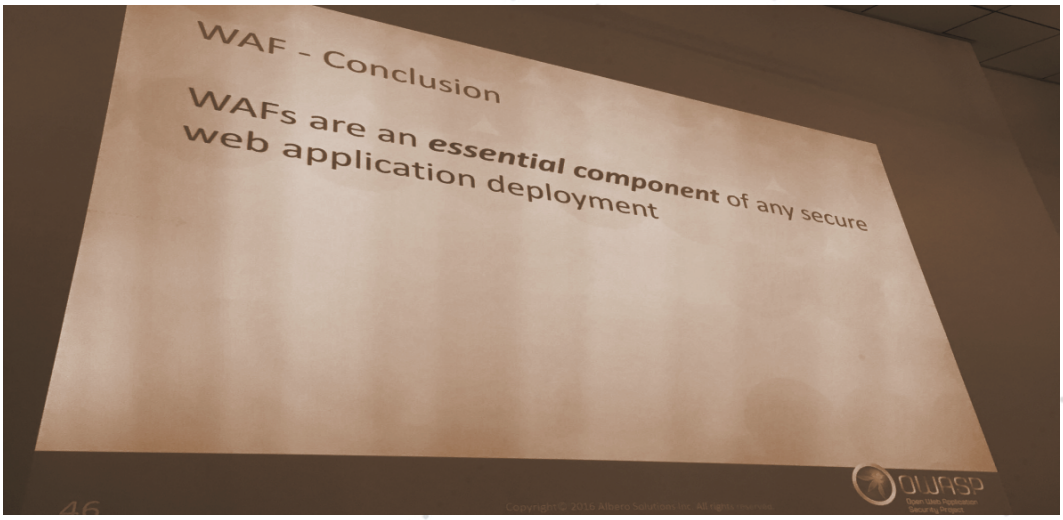
Source: ModSecurity Handbook

Limitations

ModSecurity, and WAF in general, are **NOT**:

- One box to fix ‘em all
- Set it and forget it
- Replacements for other secure development/deployment practices
- Risk free
- Cost free (even with open source)

WAFs Are Essential



©David Caissy. Used with permission.

Set Your Expectations

- Know yourself
- Know your adversary
- Know your environment

Know Yourself

- What kind of business are you in?
    - Publisher – availability
    - E-commerce – performance
    - Bank – data loss
- How much is your downtime worth?
- What are your compliance requirements?
- What is your current security posture?
- Which side do you err on?

Know Your Adversary

- Who attacked you?
    - How sophisticated are the attacks?
    - What were the consequences?
- Who and what are you afraid of?
- Who competes with you?

Know Your Environment

- Technology stack
- Network setup
- Your web application's behavior
    - Maximum file upload size
    - Maximum number and size of parameters
    - Allowed HTTP methods
    - Disallowed file extensions
- Blocking behavior desired

Let's NOT Abandon WAF

Even after WAF is purchased and deployed, some people abandon it because:

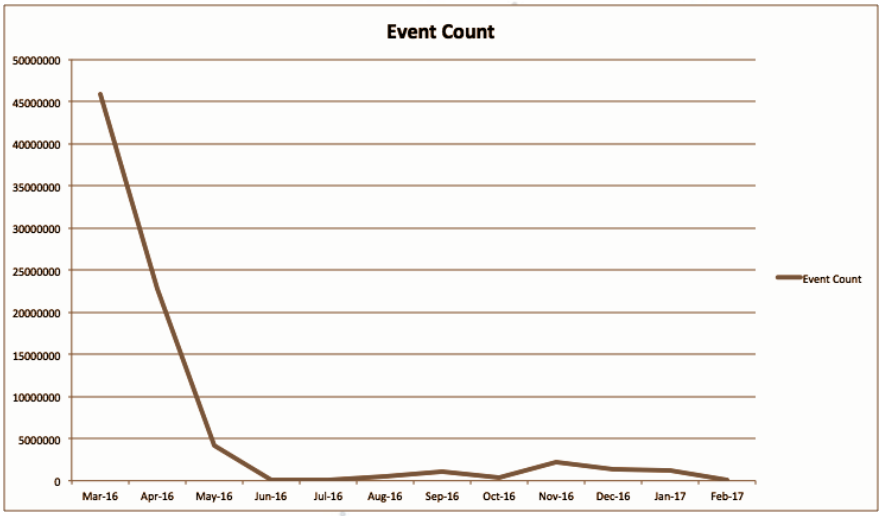
- They experience a large number of false positives
- Fine-tuning is difficult for average user
- Separating signal from noise is expensive

"Out-of-the-box" settings don't work in most cases

Core Rule Set (CRS)

- Self-Service Rule Set
- Targets OWASP Top 10
- Multiple iterations
- Regex-based Rule Set
- Most commonly deployed for ModSecurity
- Allows for lightweight inspection

The Holy Grail of Fine-tuning



Fine-tuning Your WAF

Goal: Teach WAF so that it can make correct decisions on your behalf.

- Run it in alert-only mode (for a week at least)
- Identify false positives
    - Correlation of all fields is needed
- Decide on false positives
    - The “box” cannot decide for you that it does not know you or your environment
- Fine-tune it by excluding variables

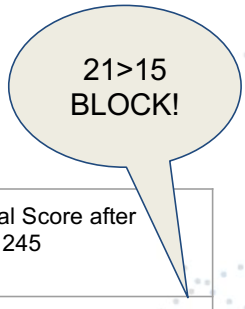
Anomaly Scoring in ModSecurity

- What is anomaly scoring?
- What is the anomaly score threshold?
- Higher threshold, more false negatives
- Lower threshold, more false positives

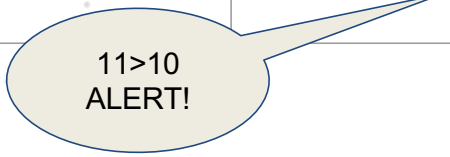
Goal: To keep total anomaly score threshold to minimum with acceptable false positives

Anomaly Scoring Explained

Two Anomaly Score Thresholds,
same HTTP transaction



Threshold	Total Score after 960024	Total Score after 981173	Total Score after 981255	Total Score after 981245
15 (Blocking Mode)	3	6	11	21
10 (Alert-only Mode)	3	6	11	



Keeping the Wall Bulletproof

Now that you have a Wall, do not blow too many holes in it

- Exclude variables that cause false positives
- Deploy exclusions carefully and methodically
    - Exclusions can reduce your level of security
- Identify the right variables to exclude

Safe Exclusions

- Consider arguments first, then cookies
    - Make sure they are used safely in the code
- Consider URL exclusions carefully
    - It blows larger holes in your wall
- Turn off rules only as last resort
    - Exception: Some very noisy rules like 981172 and 981173
    - **Better**: Use Paranoia Mode with CRS 3.0 (details later)

Exclusion Example

```
SecRuleUpdateTargetById   958895   !ARGS:email
```

- **Argument exclusions**
  - One of the safer vectors to exclude
  - Can be achieved via rule target updates in ModSecurity
  - Can be set to only exclude for specific rules

Cookie Exclusions

```
SecRuleUpdateTargetById   981243 !REQUEST_COOKIES:cookie
```

- Cookies tend to cause a large amount of false positives on WAFs
- Cookies can be easily manipulated
- Care must be taken when excluding cookies
- Can be set to only exclude for specific rules


INCLUDES:
DR. FOLINI'S
PARANOIA MODE
OWASP ModSecurity Core Rule Set
v3.0
BASED UPON A TRUE STORY!
CRS3
OWASP ModSecurity Core Rule Set v3.0
DIRECTED BY
CHAIM SANDERS
STARRING
WALTER HOP AS REGEX WIZARD, CHAIM SANDERS
ORIGINAL IDEA BY OFER SHEZAF AND RYAN BARNETT ALSO STARRING CHRISTIAN FOLINI, FRANZISKA BÜHLER, @EMPHAZER, RYAN BARNETT, FELIPE ZIMMERLE
MANUEL LEOS, VLADIMIR IVANOV, CHRISTIAN PEROZI, @YGREK, @TOBY78, @JAMUSE, MATT KOCH, ACHIM HOFFMANN, MAZIN AHMED, NOËL ZINDEL
Trustwave
COMING SOON TO A SERVER NEAR YOU!
OWASP

Core Rule Set 3.0

- First major CRS release (Nov. 2016) \ since CRS 2.2.9 (2013)
- Introduces Paranoia Mode
- “Problem” rules have been identified and combined with others to reduce the amount of false positives

Core Rule Set 3.0

- New Remote Code Execution rules are highlighted
- Large variety of SQLi and XSS rules have been dumped in favor of including Nick Galbreath's "libinjection" library
- Lots of new and great documentation!

Paranoia Mode

- Born on the back of Anomaly Scoring mode
- 4 levels of “paranoia” determine what protection is best for your environment
  - Level 1: 150 base rules, very few false positives
  - Level 2: 30 Additional Rules. Some possible false positives.
  - Level 3: 15 Additional Rules. False positives will be unavoidable and will require tuning.
  - Level 4: 6 Additional Rules. WAF should be fine-tuned before enabling PL 4

Thank you.

@TZaw

Tin Zaw resides in Santa Monica, California, where he seeks a Zen state of mind amid the chaotic mix of technology, society and cyber threats. Wanting to make the world safer online, he gave up his beloved programming job to focus on cyber security. He is a former president of OWASP Los Angeles and he currently co-leads OWASP Automated Threats project. Tin currently works to make the Internet safer and more secure at Verizon Digital Media Services.

@tzaw

@BuddyleeR

Robert Whitley lives in sunny Southern California, where he learned the basics of information security as a SOC analyst and engineer. He spends his days consulting on WAF and Rate limiting configurations at Verizon Digital Media Services. A budding professional, Robert gave up the lanes to attend engineering school, an experience he found to be as challenging as bowling a perfect game.

ModSecurity: More Than Just CRS

- More than just a way to serve 403's to malicious traffic
- Simple Access Control (IP, GEO, URL)
- Global Settings and thresholds allow for web app hardening outside of your core rule set
- Use alerts to provide feedback to developers on possible vulnerabilities

ModSecurity: More Than Just CRS

- Implement Real Time Blocking lists based on reputation rule sets
- Commercial Rule Sets help target technology specific rule sets (WordPress, Joomla!, etc.)
- Header Manipulation
- Session Management
- Serve a Custom User Friendly Response

ModSecurity: More Than Just CRS

- Honeypot Diversion
- Penalty Box
- Virtual Patching (Exploit and Vulnerability)
- Detecting Attacks with ModSecurity Persistent Storage
- Simple Rate Limiting Module