Ofer Shezaf
WAFEC 2.0 Project Leader
March 2009

The roadmap for WAFEC 2.0

WHY WAFs FAIL?

Xiom: the WAF experts

- Focus on real time web application security solutions.
- Free & unbiased expert information about web application firewalls and related technologies.
- Help in making WAFs deliver:
  - Selecting the correct WAF solution for you.
  - Optimizing your WAF implementation.
  - Write rules to ensure effective security.
  - Analyze alerts to understand risk and vulnerabilities of your web application.
  - Implementing ModSecurity based solutions.

www.xiom.com

modsecurity
Open Source Web Application Firewall

WAF: Many Definitions

- An appliance, server plug-in, or filter that **applies a set of rules to an HTTP conversation** (OWASP).
- An intermediary device, sitting between a web-client and a web server, **analyzing OSI Layer-7 messages** for violations in the programmed security policy (WASC)
- **A security policy enforcement point** positioned between a web application and the client end point … designed **to inspect the contents of the application layer** of an IP packet (PCI)
- A security technology designed to protect web sites from attack which **do not require modification of the application source code** (WAFEC 1.0)

Xiom Definition

Simply put, A WAF is an **operational security control** which monitors **HTTP traffic** in order to protect **web applications** from attacks.

Protects applications in real time, rather than hardening them or fixing them in advance.

analyzes the traffic between the untrusted client and the web server.

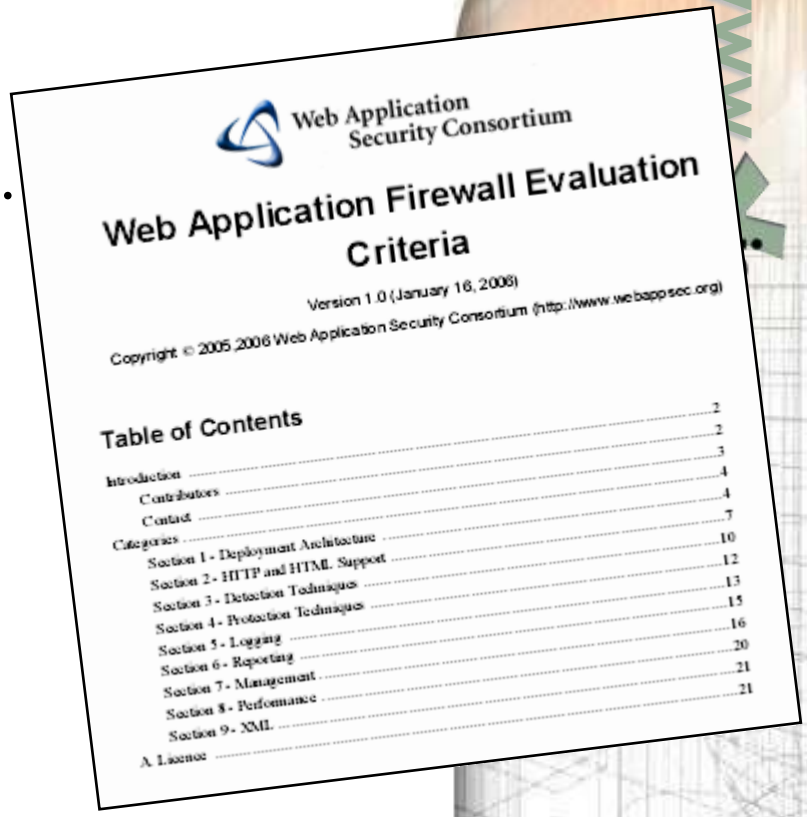
Mostly custom written and very dynamic, web applications are in many cases vulnerable and not well protected by other solutions.

How is it Different?

- Intimate understanding of HTTP
- Provide a positive security model
- Application layer rules
- Session based protection
- Allow fine grained policy management
  - most notably exceptions.

What is WAFEC?

- The Web Application Firewall Evaluation Criteria, the premier resource defining what a WAF is.
- A Web Application Security Consortium project
- Where?
  - Version 1, published in 2006: www.webappsec.org/projects/wafec
  - Version 2, under development: www.xiom.com/wafec



Web Application Security Consortium

Web Application Firewall Evaluation Criteria

Version 1.0 (January 16, 2006)

Table of Contents

What WAFEC 1.0 is not?

- A comparison of products.
- Neither benchmark nor a check list:
  - No weighting.
  - Many alternatives for same feature.
  - No indication of preferred solution for each feature.
- Dated:
  - Rudimentary XML, Performance sections
  - No sufficient discussion of the required security benefits of a WAF and how to test it for them

The WAF Paradox

- The application security Need is well understood.
- Solution has clear advantage over code review and testing:
  - Less depended on manual work and expertise.
  - Provides an immediate mitigation.
  - Handles code that is not, or cannot be tested and fixed: 3rd party, ad-hoc etc.
  - Therefore cheaper.
- But still a tiny niche market:
  - Around $50M a year
  - Led by small players: Imperva, Breach, F5.

Why?

- Not mature enough?
  - WAFs exist since 1997..
- Hard to use?
  - Ever tried to use a source code analysis tool?
- Cultural resistance?
  - Sure, but over time shouldn't sure economics win?

Xiom Take on Why

"We use a WAF to help clients virtually patch issues found in pen tests when changes to the source code is not an option or will take too long.

However WAFs cover only about half of the issues we find."

Insufficient Security

- Insufficient Anti-Automation:
  - Denial of service
  - Mass information retrieval
  - Cheating: Gaming, Queues
- Insufficient Authentication:
  - Easy to guess passwords
  - Brute force attacks
  - Stolen passwords
- Cross Site Request Forgery
- Predicable resource identifiers

All of these can be done by a WAF, is hard to do in code, and yet WAFs don't do it.

Still Difficult to Operate

- Learning limited to positive input validation model.
- Other areas where learning could be applied:
  - Automatic exceptions creation.
  - Rate based detection.
  - Session flow & Normal user behavior.

WAFEC 2.0

- Will include a list of threats a WAF should protect from.
- Will differentiate between operational features and security features.
- Will define “must features”.

Conclusion

- Real time web application security controls are important.
- Existing solutions provide value, but fall short of clearly winning over re-coding.
- Major technical advances are needed to move WAFs to the main stream.
- Such advancement is needed to ensure better security to our web applications.
- WAFEC 2.0 might help client require more and push vendors to provide more value.