WASC/OWASP WAFEC
From industry to community project

Achim Hoffmann, sic[!]sec GmbH
Ofer Shezaf, HP ArcSight

achim@owasp.org, ofer@shezaf.com

OWASP
Hamburg, 23.08.2013

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.
WAFEC

- Stands for “Web Application Firewall Evaluation Criteria”
- Project of WASC
  - Web Application Security Consortium
    http://www.webappsec.org/
- Started in spring 2005
- As follow-up of the WAS-TC
  - Web Application Security Threat Classification
- Published January 2006
- Web Application Firewall Evaluation Criteria Response Matrix, Published May 2009
- More information at http://www.wafec.org/
WASC WAFEC vs. WASC/OWASP

WAFEC

- WASC – industry driven project
  - Primary information from most vendors
  - Very organized and disciplined project management

- OWASP – community driven project
  - Reputation for excellence and objectivity
  - Easy to join and participate in OWASP project

However:
most authors and contributors participate in both

Why not merge?
- Community is voluntary work – slower
- Industry – often mainly commercial interest

Community + industry = unbiased + widely accepted
WASC WAFEC to WASC/OWASP WAFEC

- 2006 WAFEC v 1.0
- 2009 WAFEC Evaluation Response Matrix
- 2010 Start of Work on V 2.0
- 2011 Discussion about „merge“ with OWASP
- 2012 WAFC WAFEC becomes WASC/OWASP WAFEC
  schedule to finish v 2.0
- 2013 WASC/OWASP WAFEC v 2.0 to be published
Why WAFEC 2.0: 2005 - 2013

Why a new document?

- New HTTP technologies in use (i.e. Web2.0)
- New players in the market
- New WAF functionalities
- WAF functionalities overlap with other technologies
- Customers want to compare
  - <2009: most WAF vendors prohibited benchmarks (at least publishing the results)
  - >2010: benchmarks became more popular
- 2008: OWASP Best practices: Web Application Firewalls
WAFEC 2.0
Content and challenges
We planned to announce today

But we will not
The challenges

The challenges of a volunteering project
  § Combining multiple contributions – duplication, gaps and quality.
  § Volunteering goes just as far...

Evaluation criteria are HARD!
  Let’s focus on that.
Core Security Value

Protection Methods
§ Not just signatures:
§ Cookie signing
§ Challenge/response
§ IP Reputation
  § Signatures also means different things to different people.
§ More than one way to do things.
§ Is one better than the other?
§ Many times just about naming.
§ Very vulnerable to marketing exploit.

Protection Effectiveness
§ How to define?
§ How to measure?
§ A standard test is easy to prepare for.
§ Just imagine:
  § Criteria: “Does your product protect from CSRF”?
§ Answer: YES!
Are all criteria equal?

Consider the following (generalized) requirements:
- Protect from SQL injection attacks
- Frequency of signatures update
- Support sending events to a SOC
- Support TCP based syslog

They differ in:
- Importance
  - Role: Mandatory, supporting or environment specific

Setting weights is nearly impossible
WAF and WAFEC Boundaries

What is a must for a WAF?
Single Sign On?

How to take into account the value of related features?
SSL offloading
Load balancing?

None behavioral requirements
Performance

Hardware certification
Vendor information, support contracts
Price....
Solution - WAFEC 2 structure