A Year of Frustration

A RASP Deployment Story

https://www.surveymonkey.com/r/3GFHDPT
What is RASP?

Gartner says:

**Runtime application self-protection (RASP)** is a security technology that is built or linked into an application or application runtime environment, and is capable of controlling application execution and detecting and preventing real-time attacks.
But, what IS RASP?

Two Basic Types

Embedded

- USER
- APPLICATION
- Runtime Environment
- RASP
- BLOCK
- ALERT
- SEIM

Server Level

- USER
- RASP
- APPLICATION
- BLOCK
- ALERT
- SEIM OR DASHBOARD
What Can RASP Block or Monitor?

- Command Injection
- Clickjacking
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF/ XSRF)
- Database Access Violation (Advanced SQLi)
- HTML Injection
- HTTP Method Tampering
- HTTP Response Splitting
- Insecure Cookies
- Insecure Transport
- JSON Injection
- Large Requests

- Logging Sensitive Information
- Malformed Content-Types
- OGNL Injection
- Path Traversal
- SQL Injection
- Logging Sensitive Info
- Insecure Transport Protocol
- Unauthorized Network Activity
- Uncaught Exceptions
- Unvalidated Requests
- Vulnerable Dependencies
- Weak Authentication

- Weak Browser Cache Management
- Weak Cryptography & Ciphers
- XML External Entity Injection (XXE)
- XML Injection
How is this different from WAF?

• Where it sits in the stack, generally
• Complementary since they sit in different locations
• Should feed each other and tighten the net
Why RASP?

Defense in Depth, but...

Zero Days Increasing

Too Many OLD Vulnerabilities

Deserialization Attacks on Rise

WAF Learning is SLOW

VENDOR PRESSURE
Really...Why RASP?

OR, why does management care?

What makes it so different that we need to add it into an already confusing jumble of security acronyms?

1. Gives developers time!!!
2. Moves beyond speculative security issues
3. Visibility that can be distributed to various security functions
   • Developers
   • GSOC
   • Management
Selection Process
How to Upset Vendors in 101 Ways
Deployment Methodology – First Try

- Communicate with applications
- Put the tools in their hands
- Give deployment timeline requirements
  - FAIL
- Escalate to application management chains
  - FAIL
- Escalate to Senior IT Management
  - FAIL
10 Months Later – Reboot Process

- Hire Dedicated Project Manager
- Hire Dedicated Manager
- Hire Dedicated Staff
- Attack the Problem
- FORCE Teams to Implement
- Deployment Success
Now What?

• HOW do we see the information?
• WHO should see WHAT information?
• What happens if something changes?
• How far do we expand? Does every app need this?
• Should Sr. Management feel more secure?
Survey Results

• Have you implemented RASP?
• How many applications have been implemented?
• What vendor are you using?
• What is your biggest barrier to deployment?
• How would you rate the value of RASP?