Assessing & Defending Web Applications: Tools & Methodologies

OWASP Presentation

James Tarala

Enclave Security / The SANS Institute

Presenter Bio

- James Tarala
  - Principal Consultant & Founder of Enclave Security
  - James.tarala@enclavesecurity.com
  - Twitter: @jamestarala; @isaudit
  - http://www.enclavesecurity.com/blogs/

Background of the 20 Critical Controls

What's the Point?

- Government & private sector organizations are being attacked and compromised daily
- What we're doing today to defend systems is mostly not working!
- We need priorities and a meta-view of the problem
- We need someone to take a stand and provide the industry with a set of real priorities for defense

Examples from the News

- PrivacyRights.org (updated weekly)
- Here are some that are reported (most are not)
- Just a small sample (organization/records breached):
  - Heartland Payment Systems (130+ million – 1/2009)
  - Oklahoma Dept of Human Services (1 million – 4/2009)
  - Oklahoma Housing Finance Agency (225,000 – 4/2009)
  - University of California (160,000 – 5/2009)
  - Network Solutions (573,000 – 7/2009)
  - U.S. Military Veterans Administration (76 million – 10/2009)
  - BlueCross BlueShield Assn. (187,000 – 10/2009)

Project Guiding Principles

- Defenses should focus on addressing the most common and damaging attack activities occurring today, and those anticipated in the near future.
- Enterprise environments must ensure consistent controls across an enterprise to effectively negate attacks.

Project Guiding Principles (2)

- Defenses should be automated where possible, and periodically or continuously measured using automated measurement techniques where feasible.
- To address current attacks occurring on a frequent basis against numerous organizations, a variety of specific technical activities should be undertaken to produce a more consistent defense.

Why are the Controls Important?

- Cyber security is complex and becoming even more complicated every day
- Organizations are being compromised, even after spending large portions of their budget on infosec
- CIOs & CISOs need prioritized controls to get the most return from their investment
- More controls rarely hurt, but how do we decide which controls to start with?
- **It's critical that we have priorities**!

Why are the Controls Important? (2)

- We need agreement between:
  - Inspector Generals (IGs – auditors)
  - Operations (sys-admins)
  - Security Engineers
- We need metrics and measurements that everyone can agree to use
- We need to stop people from violating systems & compromising the C-I-A of our data

Document Contributors

- Blue team members inside the Department of Defense
- Blue team members who provide services for non-DoD government agencies
- Red & blue teams at the US National Security Agency
- US-CERT and other non-military incident response teams
- DoD Cyber Crime Center (DC3)
- Military investigators who fight cyber crime
- The FBI and other police organizations
- US Department of Energy laboratories
- US Department of State

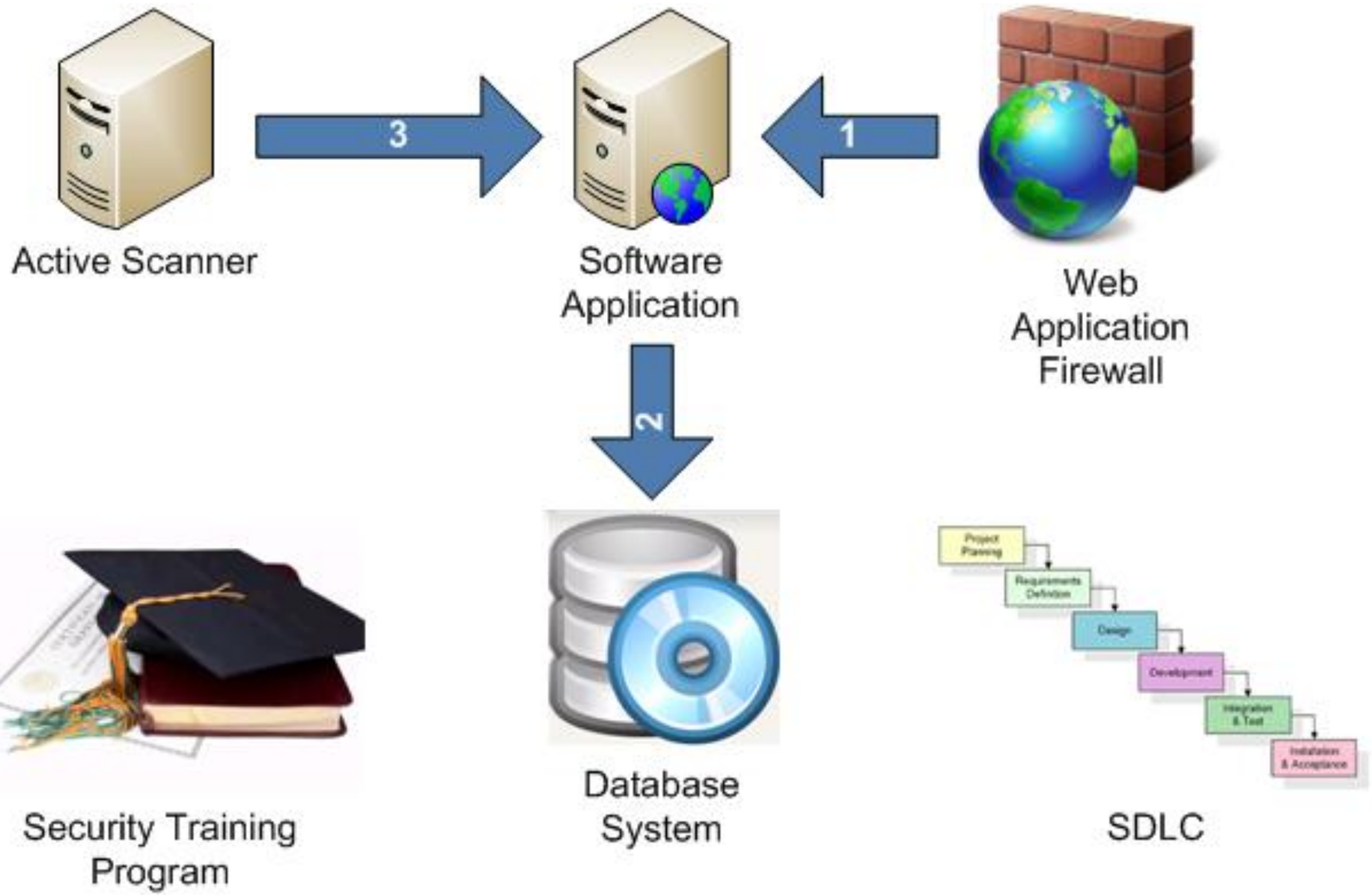
Document Contributors (2)

- Army Research Laboratory
- US Department of Homeland Security
- DoD and private forensics experts
- Red team members in DoD
- The SANS Institute
- Civilian penetration testers
- Federal CIOs and CISOs
- The Government Accountability Office (GAO)
- Plus over 100 other collaborators

Evaluating Critical Control #7

- Business goal of this control:
  - Security flaws in applications must be remediated in order to protect sensitive data sets & systems
- Systems to be tested:
  - Application code
  - Database systems
  - Code analysis scanners
  - Application firewalls
- Test to Perform:
  - Run vulnerability scanners & code analysis tools against business applications & systems in order to identify flaws

Control System Entity Relationship Diagram (ERD)



Core Evaluation Steps

- Run a web application vulnerability scanner against Internet facing web applications
  - Based on 25 Most Critical Programming Errors
  - Alerts should be sent within 2 minutes of completing a scan
- Run a static code analysis tool against Internet facing web applications
- Run a database configuration scanning tool against all databases in Internet facing web applications

Core Evaluation Steps (2)

- Ensure that all identified vulnerabilities have been fixed or remediated with a compensating control within 15 days
- Ensure the scans completed for each of the last 30 cycles
  - If the scan failed, an automated notification to administrators must be generated

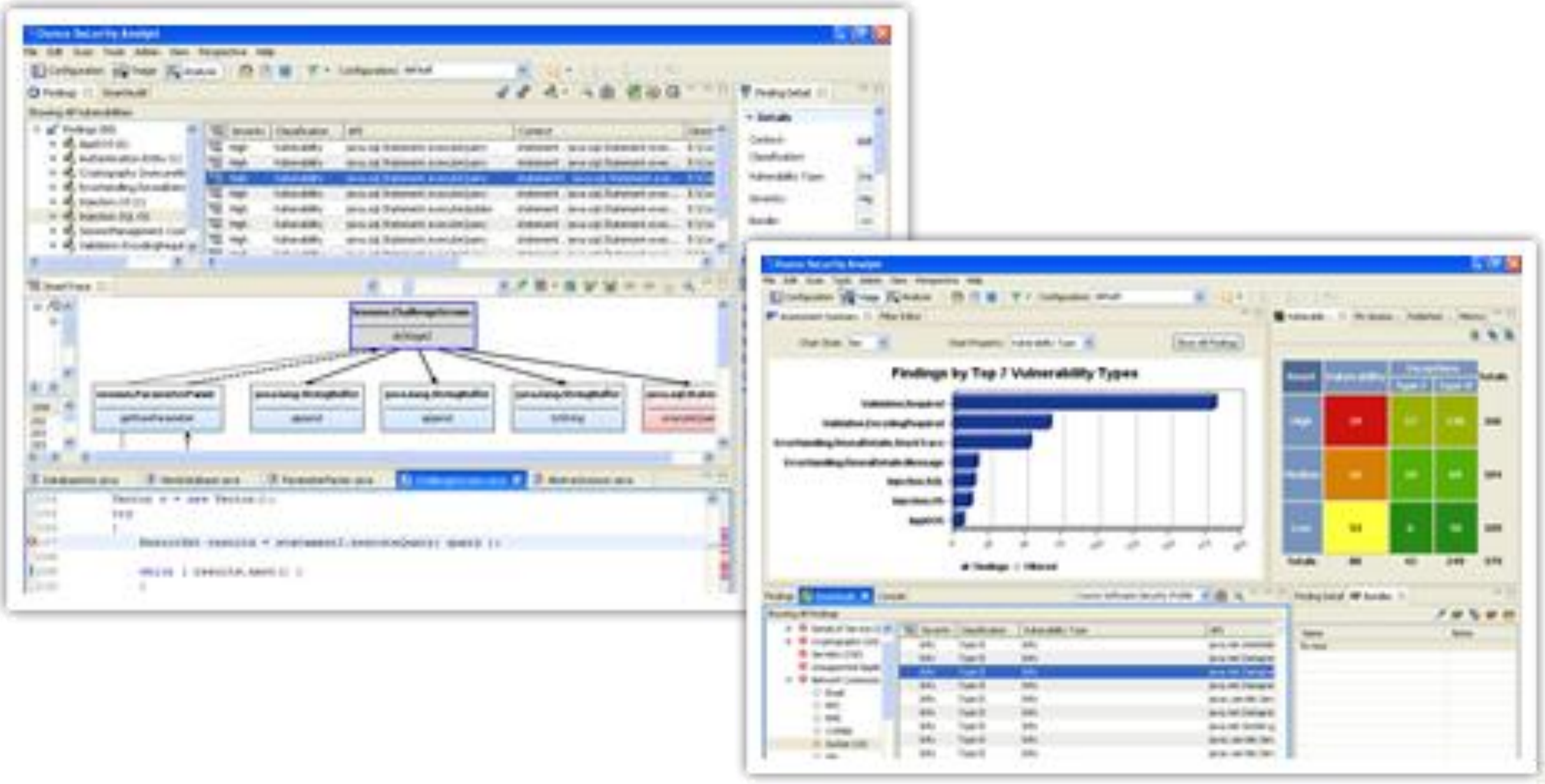
Testing / Reporting Metrics

ID	Testing / Reporting Metric	Response
7a	Can the application system detect attacks & block them within 2 minutes of being detected?	Yes/No
7b	Are all Internet facing applications scanned by web application vulnerability scanners at least weekly?	Yes/No
7c	How long does it take for alerts to be generated & sent to system administrators that a vulnerability scan has or has not completed?	Time in Minutes
7d	Are all vulnerabilities detected by the scanning tools fixed or remediated within 15 days of detection?	Yes/No

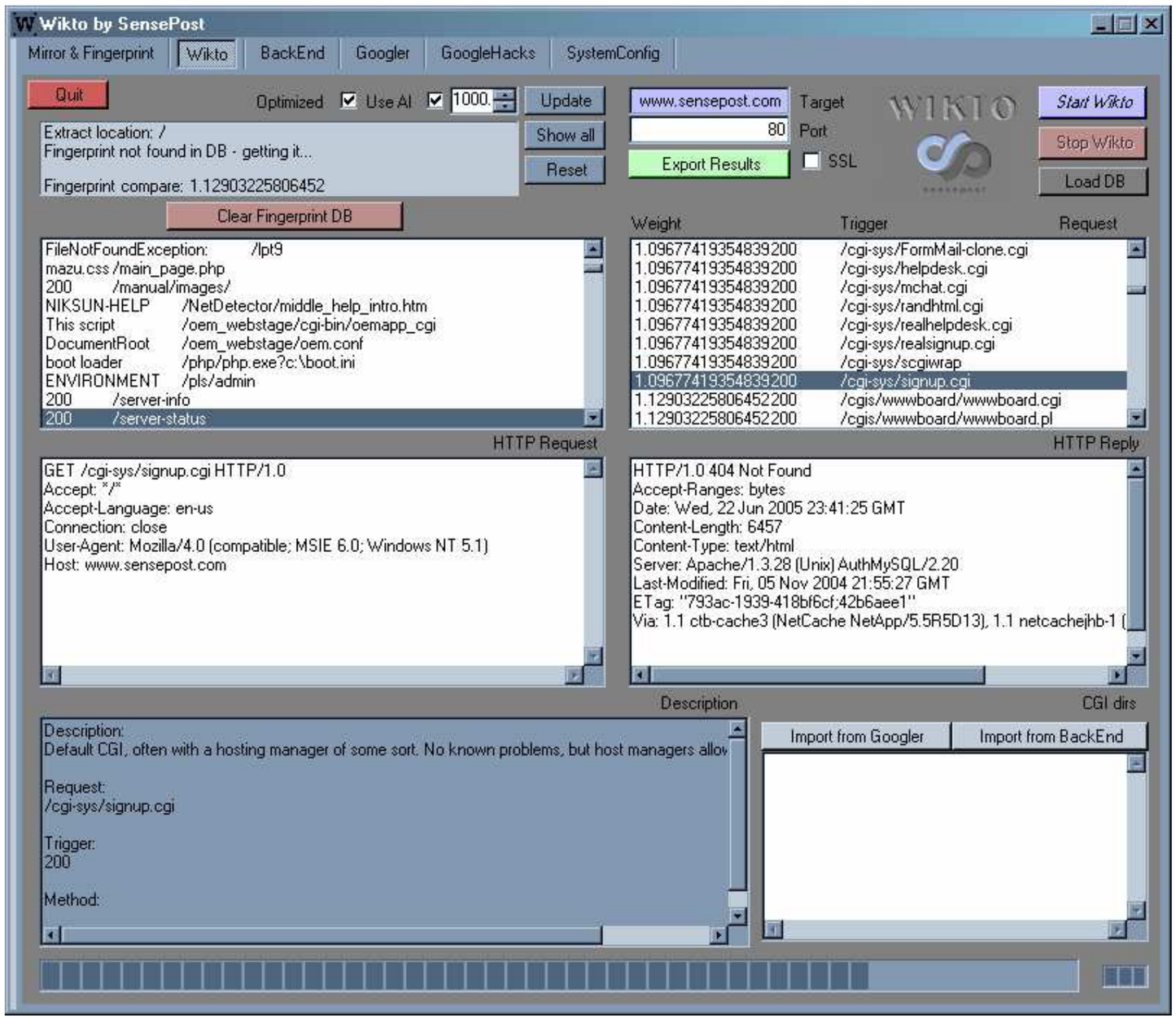
Evaluation Tools

- Questionnaire & Interviews
- Free or Open Source Tools
  - W3af
  - FxCop / FindBugs / BLAST
  - Wikto / Paros / WebScarab
  - Scuba
- Commercial Tools
  - Fortify 360
  - Ounce Labs Core
  - HP WebInspect
  - IBM AppScan

Sample Analysis:
Auditing Output from Ounce Labs



Sample Analysis: Auditing Output from Wikto

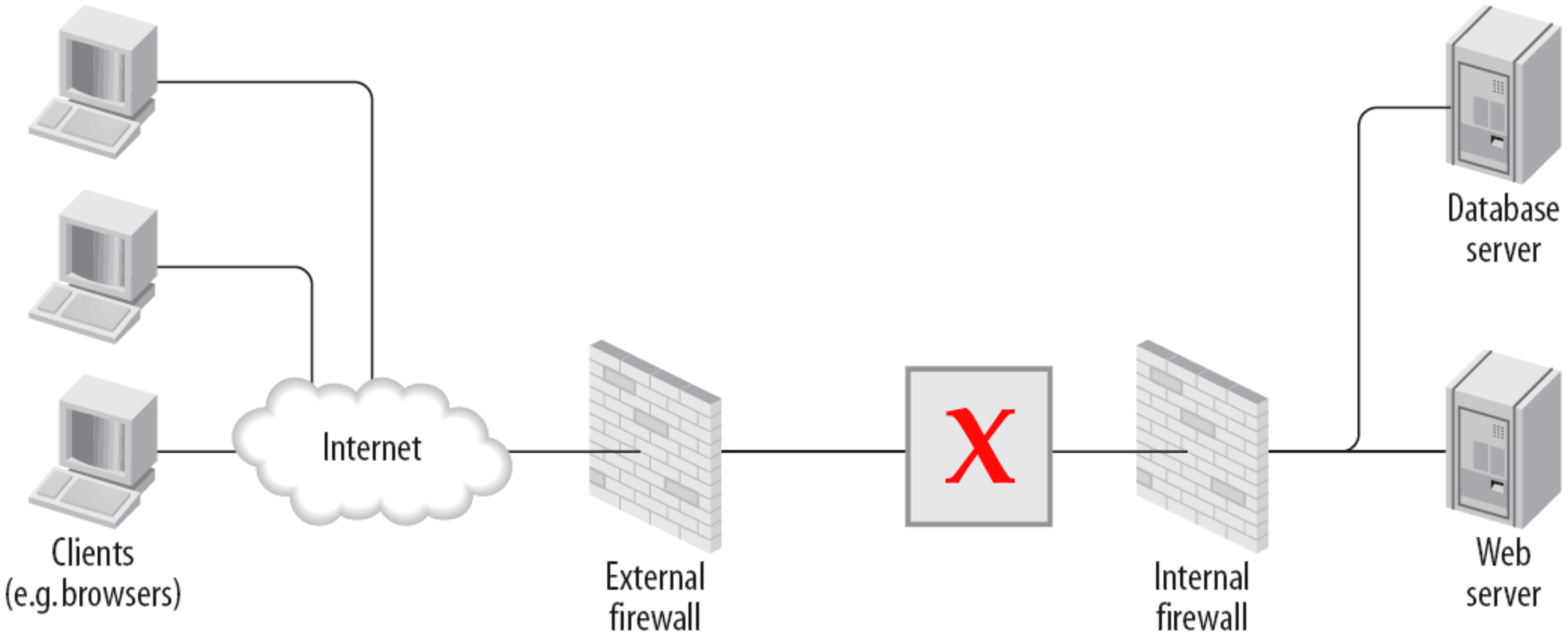


Web Application Firewalls

What are Web Application Firewalls?

- Software or appliances used to filter unwanted TCP port 80/443 traffic from connecting to a web server
- Web Application Firewalls:
  - Examine within the data payload, beyond simply the IP or TCP headers
  - Perform "Deep packet inspection"
  - Detect and respond to signatures for known application vulnerabilities
  - Do not require modifications to existing application code

A Typical WAF Architecture



http://www.modsecurity.org/documentation/Web_Application_Firewalls_-_When_Are_They_Useful.pdf

Common WAF Features

- Network Protocol Filtering
- HTTP Protocol Filtering
- Stateful Connection Monitoring
- High Availability Support
- Session Management Controls
  - Traffic flow assessments
  - Timeout enforcements
  - Session hijacking monitoring
- Cookie Monitoring/Protection
- Hidden Field Enforcement
- Brute-force Monitoring
- Honeypot/Honeynet Integration

Relevant Research

- Web Application Firewall Evaluation Criteria (Web Application Security Consortium)
  (http://www.webappsec.org/projects/wafec/)
- The Web Application Firewall Forecast: 2007 to 2010 (Jennifer Albornoz Mulligan, Chenxi Wang, Forrester)
  (http://www.forrester.com/Research/Document/Excerpt/0,7211,41780,00.html)
- Application Firewalls – Are they Worth the Investment? (Michael Gavin, Forrester)
  (http://www.imperva.com/lg/lgw.asp?pid=83)
- Application Assurance Platforms Arise from Web App Firewall Market's Ashes (Andrew Jaquith, Yankee Group)
  (http://www.imperva.com/lg/lgw.asp?pid=83)
- The Open Web Application Security Project (OWASP)
  (http://www.owasp.org/index.php/Main_Page)

Difficulty of Code Review

- Enterprise resources are limited – both financial & time
- "Don't fix what isn't broken"
- Vendor contracts often limit our right to audit their applications
- Even well coded applications may be vulnerable to OS or web server flaws

- There is an industry wide shortage of software security professionals
- SANS Software Security Institute (http://www.sans-ssi.org)

Generic Benefits of a WAF

- Application attacks can be stopped before reaching a web server by filtering traffic:
  - At the IP/TCP level (layers 3-4)
  - At the application level (layers 5-7)
- Faulty code will be protected from threats to:
  - Operating system vulnerabilities
  - Web server vulnerabilities
  - Web application vulnerabilities
- A network infrastructure solution can be provided for a software security problem
- Resources normally dedicated to securing the code can be devoted to other security threats

Industry Specific Benefits to a WAF

- WAFs are useful in situations where reviewing the application code is not an option:
  - Custom code, when there are no developers to support it
  - Vendor code, when contract language limits code review
  - Off the shelf applications
  - Legacy information systems
- Vertical industries most likely to benefit:
  - Government
  - Healthcare
  - Retail / E-commerce
  - Manufacturing / Industrial

In short…

Simply put, in a perfect world proper, secure application code would be written by developers to keep their data safe. But we don't live in a perfect world. Therefore compensating controls, like Web Application Firewalls, will continue to be necessary to protect organizations' private data from being exposed.

Conclusions

1. Organizations cannot ignore the importance of application code review
2. Whenever possible, the root cause of any security problem should be addressed before compensating controls
3. Not all organizations have the capability to address security flaws at the code level
4. Even well-coded applications may eventually be vulnerable to OS level attacks
5. WAFs provide the compensating controls that many organizations need to protect their web applications
6. "No one was ever fired for recommending defense-in-depth."

Questions?

- If you do have questions later, don't hesitate to ask
- You can reach me at:
  - James.tarala@enclavesecurity.com
  - Twitter: @jamestarala; @isaudit
  - http://www.enclavesecurity.com/blogs/