



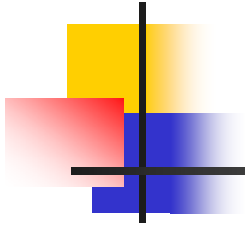
Web Application Security

K.K. Moohkey Network Intelligence

Steve Orrin, Independent Security Professional

John Weinschenk Cenzic

David Piscitello, Core Competence, Moderator



What is Web Application Security?

- Measures to detect and block attacks against web server and web-enabled applications
 - Exploit poor code and configuration, e.g.,
 - Malicious composition of URLs
 - Data manipulation and injection
- HTTP/80 is fair game
- HTTPS/443 is vulnerable as well



Is web application security all about badly written application software?

- What must we do to ensure security in outsourced and COTS software development?
- Input validation attracts most of the attention. What other vectors can be exploited, even if I'm doing correct input validation?
- What new attacks and techniques do you see coming down the road?
- What responsibilities should be borne by the commercial software vendors for application security?



What about web, OS, and application configuration?

- Isn't configuration and management a factor in web application security?
 - How much so?
 - Why?
 - What measures are available to test and correct "web presence" configurations?
- Will web applications be more secure in the future, or less?
 - What will make them so?



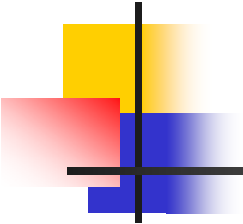
Testing and Assessment

- When and how often should we test web application code?
 - When do we test code?
 - How, and how frequently?
 - What does a good test methodology encompass?
 - What are the best tools for web application security testing?
- Is application vulnerability assessment an in-house or outsourced activity?



Is Web App Security strictly a large enterprise problem?

- What web application security challenges do customers (organizations) cite as most critical?
 - Do these differ from SMB to large enterprise?
- Should a Small-to-Medium enterprise be concerned about web application security?
 - What steps can SMBs take?
 - How labor intensive is this?
 - How resource intensive?
 - How expertise-intensive?



Web App Protection: Reactive or Proactive?

- What's the best strategy and ROI for protecting web applications?
 - Are proactive measures – secure code, review, and secure configuration – enough?
 - How do you calculate the ROI of application security solutions?
- What solutions can I apply to secure applications? What's most effective?
 - Are web application firewalls and web IDS/IPS useful and necessary?
 - How much do I invest in either, or both?



Regulatory Impact, Public perception

- Why do we continue to ignore application security despite the frequency of attacks?
- Has regulatory legislation affected web application security priorities?
 - What web application security measures help satisfy compliance criteria?
 - How critical are application security issues for compliance of Sarbox, GLBA, SB 1386 and others?
- Have identity theft and phishing affected the web application security market?