

Sunera LLC

Web Application Security Management & Best Practices Part I

Agenda

- Trends in Data Breaches – An Overview
- Web Application Security Landscape
- Recent Web Application Security Incidents
- Innovations in Web Application Hacking
- Emerging Threats in Web Application Security
- Web Application Security and the SDLC

Trends in Data Breaches

What Constitutes a Data Breach?

- Lost or stolen hardware
- Backup tapes lost in transit
- Employees stealing information or allowing access to information
- Information bought by a fake business
- Poor business practices (e.g. mishandling of sensitive information)
- Careless disposal of information (that may be retrieved via dumpster diving)
- Malware
- A malicious attacker compromising an organization's technical infrastructure

Data Breaches Trends

- Data breaches hit record highs in 2008
 - 656 data breaches in the US ↑
 - 35 million records breached in the US (a conservative estimate due to accuracy of reporting) ↑
- Hardcopy data breaches
 - 18% of data breaches
 - 2% of total records compromised
- Electronic data breaches
 - 82% of data breaches
 - 98% of records compromised

Data Breaches by Sector

| Sector | Percentage of Data Breaches | Percentage of Records Breached |
|--------------------------|-----------------------------|--------------------------------|
| Business | 36.6% | 16.5% |
| Educational | 20% | 2.3% |
| Government/Military | 16.8% | 8.3% |
| Medical/Healthcare | 14.8% | 20.5% |
| Banking/Credit/Financial | 11.9% | 52.5% |

Data Breach Costs

- Costs are increasing
 - Average Cost of a Data Breach = \$6.65 million¹
 - Average per victim cost = \$202¹
 - Of the \$202, an average of \$139 per record is a result of lost business²
- Cost Components of Data Breaches
 - Investigation Fees Recovery Fees
 - Communications Cleanup and Recovery
 - Customer Service Lawsuits
 - Increased Audits Loss of Revenue due to customer churn
- Healthcare and Financial Services hit hardest with the highest rate of customer loss (i.e. churn)¹

¹CIO.com, February 04, 2009, Costs of a Data Breach: Can you Afford \$6.65 Million

²CIO.com, February 02, 2009, Data Theft Proving More Costly for Businesses

Web Application Security Landscape

Current Obstacles

- Web application attacks are alive and well
 - Attacks are evolving and combining
- Confusion on how to test and protect web applications
 - “Point-n-click” security, general approach, authenticated vs. unauthenticated testing, WAF’s
- Confusing risk and impact
 - Using severities advertised by tools without considering compensating controls or the relative impact of a vulnerability

Common Rebuttals

- “Reasons” for increased attack surface
 - “That site is scheduled for decommission”
 - “It’s a development server”
 - “We trust our internal users, so we don’t need to remediate that finding”
- Risk denial is nothing new, but with an already difficult threat to contain it makes the business case that much harder to justify

Recent Web Application Security Incidents

Conficker

■ Conficker

- As of January 26th, 2009, an estimated **15 million**² machines infected
- Used RPC to execute a buffer overflow on Microsoft Windows services
- Variants used small HTTP servers to download exploit code, also used as a botnet to attack specific targets¹



¹<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=215600268&subSection=Vulnerabilities+and+threats>

²http://www.upi.com/Top_News/2009/01/25/Virus_strikes_15_million_PCs/UPI-19421232924206/

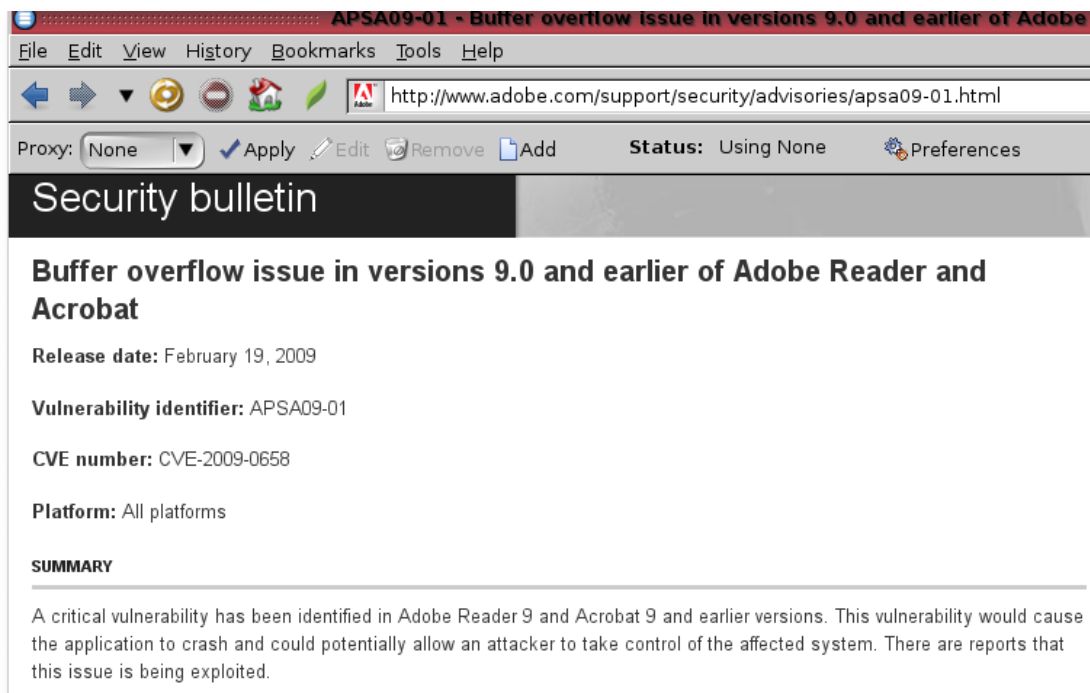
Macworld 2009 “Incident”

- ‘Steve Jobs Just Died’ Announcement
 - Hacked web “micro-blogging” feed to post inappropriate content
 - Cause: weak administration interface password



Adobe Reader 9.0 Buffer Overflow

- Adobe Acrobat Reader Plugin Buffer Overflow
 - Allows remote exploitation, system compromise
 - Community patch released in days; vendor fixes issue in weeks



Innovations in Web Application Hacking

Top Web Hacking Techniques for 2008

- Blog posting of the top web hacking techniques for 2008 judged by an all-star cast of security professionals including:
 - Jeff “RFP” Forristal – “Discoverer” of SQL Injection, RFPolicy
 - Chris Hoff – Security Industry Veteran
 - Rich Mogull – Founder, Securosis
 - HD Moore – Director of Security Research, BreakingPoint Systems, Creator of MetaSploit Framework
- 70+ of the most innovative web application attacks for 2008

GIFAR

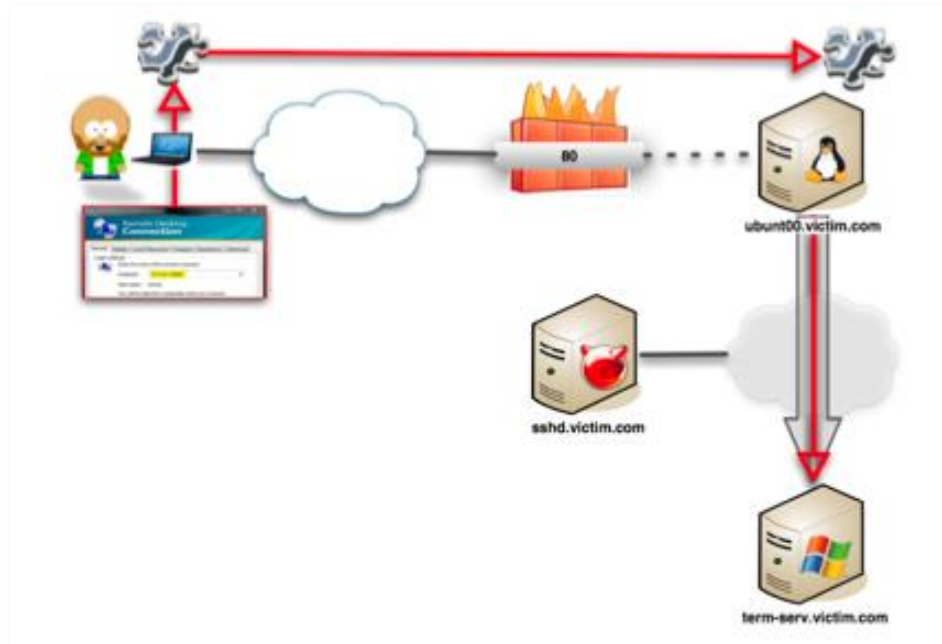
- Billy “BK” Rios, Nathan McFeters, Rob Carter, John Heasman
- Combining image files with Jar files
- Method allows attacker to host arbitrary code on a victim domain and access information contained on any subdomain
- Easiest fix is to host user-supplied files on a separate domain from the live content

Clickjacking

- Jeremiah Grossman, Robert Hansen
- Dynamically assigning the click target of the mouse when visiting a fabricated page, regardless of where the cursor may be located
- When combined with other technologies, like Flash LSO's, may offer slim windows of opportunity for unintentional executable download by victims
- Frame busting logic successfully addresses this issue.

reDuh

- “reDuh is actually a tool that can be used to create a TCP circuit through validly formed HTTP requests.”¹
 - “Essentially this means that if we can upload a JSP/PHP/ASP page on a server, we can connect to hosts behind that server trivially”¹



¹ <http://www.sensepost.com/research/reDuh/>

Emerging Threats

Overview

- EV-SSL and Man-in-the-Middle / Phishing Attacks
 - Limited adoption of EV-SSL certificates
- LSO (Local Shared Objects) Abuse
 - Large storage capacity, unfamiliarity with technology by users
- Social Network Abuse
 - A goldmine for the experienced Social Engineer

EV-SSL

- What is EV-SSL?
 - *“Extended Validation SSL Certificates give high-security Web browsers information to clearly identify a Web site’s organizational identity”*¹
- Since EV-SSL’s inception two years ago, it is reported that only 10,000 sites out of 1 million SSL-capable sites use EV-SSL ²
- Concern over who is NOT taking advantage of this technology to best protect customers
 - *“For businesses with a high profile brand, using Extended Validation SSL is the most effective defense against phishing scams.”*¹
- Advances in attacking SSL-capable sites with man-in-the-middle attack automation tools like SSLStrip ³ make the adoption of EV-SSL certificates that much more appealing (one would think anyway)

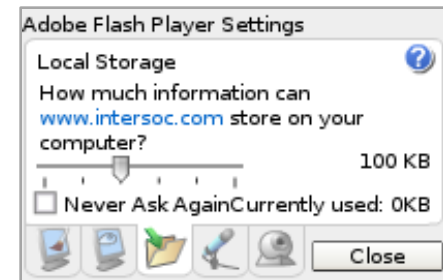
¹<http://www.verisign.com/ssl/ssl-information-center/extended-validation-ssl-certificates/>

²<http://research.zscaler.com/2009/02/ev-ssl-ssl-and-whos-not-using-it.html>

³<https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf>

Local Shared Object (LSO) Abuse

- LSO's, aka Flash Cookies, are a new spin on an old problem
 - *“The greatest advantage of Flash cookies appears to be the fact that users aren't overly familiar with them and wouldn't know how to delete them even if they were.”¹*
- LSO's are particularly attractive for the following reasons: ¹
 1. Storage can exceed 100k (vs. 4k for Cookies)
 2. Default Settings allow for unprompted use of client side storage (up to 100k)
 3. Users aren't as familiar with LSO's
 4. No default expiration
- In the wild, LSO's are being used as storage for downloading Malware to unsuspecting users
- Attack chaining by using 'ClickJacking' to influence the LSO settings panel can result in a devastating privacy violation



¹<http://research.zscaler.com/2009/03/demystifyingabusing-flash-cookies.html>

Social Network Abuse

- Publicly Available Information is “double-edged”
 - *“Many employers believe it is essential to do so in light of potential liability for negligent hiring and retention. However, employers that use social networking sites in such a manner need to be aware of the legal risks.”¹*
- Correlating this information is trivial with minimal client and server side web application programming or with tools such as Maltego²

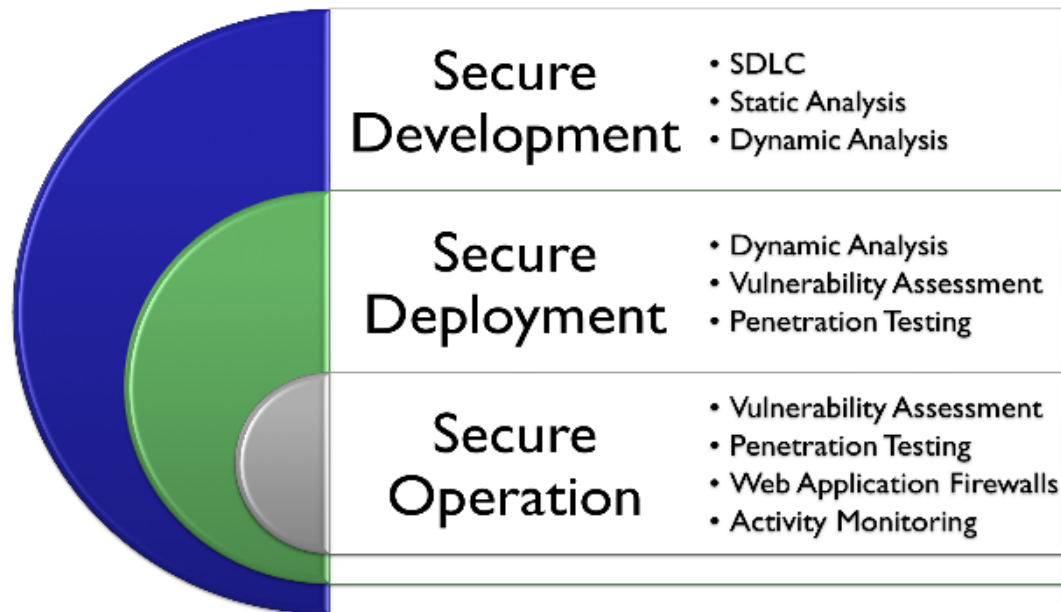
¹ http://www.talentmgt.com/newsletters/talent_management_perspectives/2009/March/889/index.php

² <http://www.paterva.com/maltego/>

Web Application Security and the SDLC

Building a Web Application Security Program

- “Building a Web Application Security Program,” paper released March 9th, 2009
- Addresses many of the hurdles encountered by all parties involved in creating an SDLC that’s tailored for web application security.



Automated Scanning and the SDLC

- “You need the right tool in the right hands as part of the right process”
 - Experienced assessors must be used to run automated tools in order to ensure maximum coverage with accurate results
- “No single web application security tool provides effective security on its own”
 - Over reliance on automated tools produces a false sense of security. The best approach is a blend of automated tools and manual analysis with human interpretation.

Prerequisites for a Successful Program

- “Custom code equals custom vulnerabilities”
 - A certain level of understanding of web development alongside current and emerging trends for web application security is required in order to fully assess the strength of the security controls applied to web applications.

- “The importance of performing both authenticated and non-authenticated automated vulnerability scanning...”
 - Performing a role analysis from both authenticated and unauthenticated perspectives will ensure that important portions of the application are also covered in automated analysis. To date, session strength and tendencies for horizontal and vertical privilege escalation have been noticeably absent from automated scanners.


- “...highlight the need for development organizations to consider security as a requirement during each phase of development” or “Secure SDLC”
 - Like functional tests, use cases for security must also be integrated in to each step within the SDLC as functional SECURITY requirements

Contact Information

- For additional information on Sunera's security services, visit our website at www.sunera.com
- Or contact the following Sunera representatives:

Andrew Cannata, CISSP, CISM
Managing Director
Information Security & Network Services
acannata@sunera.com

Joe Sechman, CISSP, CISA
Manager
Information Security & Network Services
jsechman@sunera.com



Sunera South Florida Office Address:
3350 SW 148th Avenue, Suite 210
Miramar, FL 33027