Getting Ready

In order to get the most from this session, please download / install:

- OWASP ZAP, which requires a Java runtime
- A virtualization package, such as the free VirtualBox, free VMware Player, or commercial VMware Workstation
- The OWASP BWA VM
  - I have copies on flash drives
  - Uncompress the VM

OWASP Broken Web Applications (BWA) VM and Zed Attack Proxy (ZAP)

PRESENTED BY: **Chuck Willis**

chuck.willis@mandiant.com

@chuckatsf

Agenda

- Introductions
- Zed Attack Proxy
- Bonus Content!
- Broken Web Applications VM

Introduction – Chuck Willis

- Technical Director @ Mandiant
- Application Security, Source Code Analysis, Penetration Testing, Forensics, Incident Response, R&D
- Leader of OWASP Broken Web Apps Project
- (Very) occasional visitor to Unallocated Space
- Twitter: @chuckatsf
- chuck.willis@mandiant.com

OWASP BWA
Sponsored By
MANDIANT®

We are Mandiant

- **What are we?**
  - Threat detection, response and containment experts
  - Software, professional & managed services, and education
  - Application and network security evaluations
- **Where are we?**
  - Washington
  - New York
  - Los Angeles
  - Redwood City
  - San Francisco
  - Albuquerque
  - Ann Arbor
  - Dublin, Ireland

SECURITY BREACHES ARE INEVITABLE | BEING A HEADLINE IS NOT

Detecting, responding and containing advanced targeted attacks for the Fortune 500

EMERGENCY RESPONSE
HAVE YOU BEEN COMPROMISED?
No attack is too advanced or persistent for us. We've got the talent, tools and tenacity to diagnose, manage and resolve your incident.

THREAT LANDSCAPE
FINDING ADVANCED ATTACKERS
No security program is perfect. Understand how you can find the threats that slip through your preventive defenses.

RT @ryankaz42: Visualization of unfiltered results for non-memory artifacts in Redline is coming in future releases #m_fp

THE SMARTEST COMBO OF PRODUCTS AND HUMAN INTELLIGENCE

UPCOMING EVENTS

April 17, 2012
SOURCE Conference Boston
Boston, MA

May 24, 2012
Fresh Prints of Mal-Ware: The Nutts and Boltz of M-Trends
Webinar: Register Today

M-UNITION: FROM THE BLOG

Investigating Indicators of Compromise In Your Environment With Latest Version of Redline
April 19, 2012

Leveraging the Application Compatibility Cache in Forensic Investigations
April 17, 2012

Defining the Hack: Insight into the Advanced Persistent Threat
April 16, 2012

Malware and Incident Response Training at Black Hat USA 2012
April 12, 2012

TEL +1 (703) 683-3141 TOLL FREE (800) 647-7020
DC HEADQUARTERS: 2318 MILL ROAD #500, ALEXANDRIA, VA 22314

© 2012 Mandiant Corporation.

MANDIANT®

What is OWASP?

- The Open Web Application Security Project
- 501c3 not-for-profit worldwide charitable organization with chapters around the globe.
- Focused on improving the security of application software
  - Visibility into security
  - Informed decisions about real risk
- Free to participate, free to use
- Personal and corporate supporters

What is OWASP?

- OWASP Top Ten
  - Web Application Security Risks
- OWASP Guides
  - Development Guide
  - Testing Guide
  - Code Review Guide
- Application Security Verification Standard
- Open Software Assurance Maturity Model
- Enterprise Security API

More info and lots of free materials at www.owasp.org

OWASP Zed Attack Proxy (ZAP)

OWASP Zed Attack Proxy Project

“The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing.

ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.”

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

The Zed Attack Proxy

- Released September 2010
- Ease of use a priority
- Comprehensive help pages
- Free, Open source
- Cross platform
- A fork of the well regarded Paros Proxy
- Involvement actively encouraged
- Adopted by OWASP October 2010

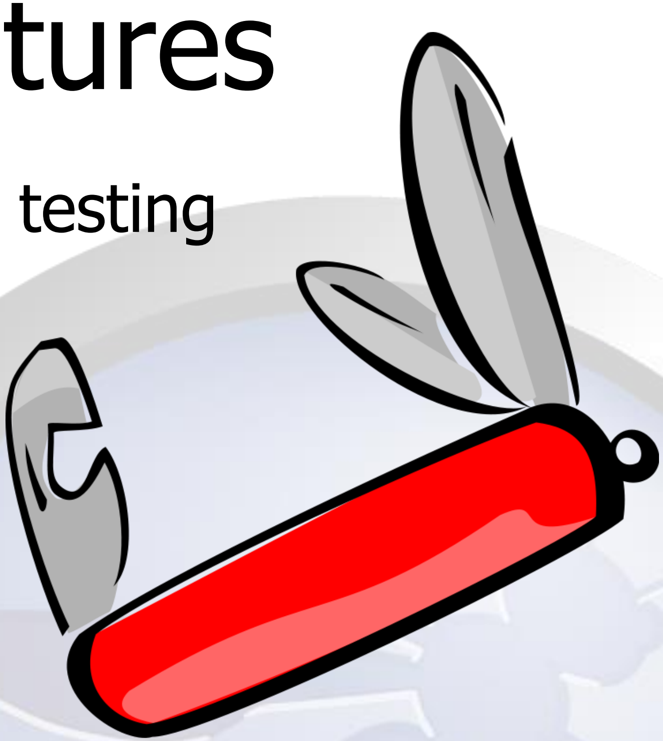
ZAP Principles

- Free, Open source
- Cross platform
- Easy to use
- Easy to install
- Internationalized
- Fully documented
- Involvement actively encouraged
- Reuse well regarded components

The Main Features

All the essentials for web application testing

- Intercepting Proxy
- Active and Passive Scanners
- Spider
- Report Generation
- Brute Force (using OWASP DirBuster code)
- Fuzzing (using OWASP JBroFuzz code)



The Additional Features

- Auto tagging
- Port scanner
- Smart card support
- Session comparison
- Invoke external apps
- BeanShell integration
- API + Headless mode
- Dynamic SSL Certificates
- Anti CSRF token handling

Let’s try out ZAP!

OWASP Vicnum Project

- OWASP Vicnum Project

http://vicnum.ciphertechs.com/

HTTPS

- ZAP has it’s own CA cert that can be installed in your browser to avoid warning messages

- Try going to an HTTPS site, like https://www.google.com/

Bonus: OWASP Vulnerable Web Applications Directory Project

OWASP Vulnerable Web Applications Directory

- “comprehensive and well maintained registry of all known vulnerable web applications currently available”
- Available at:

https://www.owasp.org/index.php?title=OWASP_Vulnerable_Web_Applications_Directory_Project

OWASP Broken Web Application (BWA) Project

OWASP Broken Web Apps VM

- Free, Linux-based Virtual Machine
- Contains a variety of web applications
  - Some intentionally broken
  - Some old versions of open source applications
- Pre-configured and ready to use / test
- All applications are open source
  - Allows for source code analysis
  - Allows users to modify the source to fix vulnerabilities

Sponsored By

MANDIANT®

More info and free download at www.owaspbwa.org

OWASP Broken Web Apps VM

- Training Applications
  - OWASP WebGoat (Java)
  - OWASP WebGoat.NET (ASP.NET/C#)
  - OWASP ESAPI Java SwingSet Interactive (Java)
  - OWASP Mutillidae II (PHP)
  - OWASP RailsGoat (Ruby on Rails)
  - OWASP Bricks (PHP)
  - Damn Vulnerable Web Application (PHP)
  - Ghost (PHP)
  - Magical Code Injection Rainbow (PHP)

Sponsored By

MANDIANT®

More info and free download at www.owaspbwa.org

OWASP Broken Web Apps VM

- Realistic, Intentionally Vulnerable Applications:
  - OWASP Vicnum (PHP/Perl)
  - OWASP 1-Liner (Java/JavaScript)
  - Google Gruyere (Python)
  - Hackxor (Java JSP)
  - WackoPicko (PHP)
  - BodgeIt (Java JSP)
  - Cyclone Transfers (Ruby on Rails)
  - Peruggia (PHP)

Sponsored By

MANDIANT®

More info and free download at www.owaspbwa.org

OWASP Broken Web Apps VM

- Old Versions of Real Applications
  - WordPress 2.0.0 (PHP, released December 31, 2005)
    - myGallery plugin version 1.2
    - Spreadsheet for WordPress plugin version 0.6
  - OrangeHRM version 2.4.2 (PHP, released May 7, 2009)
  - GetBoo version 1.04 (PHP, released April 7, 2008)
  - gtd-php version 0.7 (PHP, released September 30, 2006)
  - Yazd version 1.0 (Java, released February 20, 2002)
  - WebCalendar version 1.03 (PHP, released April 11, 2006)
  - TikiWiki version 1.9.5 (PHP, released September 5, 2006)
  - Gallery2 version 2.1 (PHP, released March 23, 2006)
  - Joomla version 1.5.15 (PHP, released November 4, 2009)
  - AWStats version 6.4 (Perl, released February 25, 2005)

Sponsored By

MANDIANT

More info and free download at www.owaspbwa.org

OWASP Broken Web Apps VM

- Applications for Testing Tools
  - OWASP ZAP-WAVE (Java JSP)
  - WAVSEP (Java JSP)
  - WIVET (Java JSP)

OWASP Broken Web Apps VM

- Demonstration Pages / Small Applications
  - OWASP CSRFGuard Test Application (Java)
  - Mandiant Struts Forms (Java/Struts)
  - Simple ASP.NET Forms (ASP.NET/C#)
  - Simple Form with DOM Cross Site Scripting (HTML/JavaScript)
- OWASP Demonstration Applications
  - OWASP AppSensor Demo Application (Java)

VM Features

- Samba shares for editing and viewing
  - Source code
  - Configuration files
  - Log files
- Scripts for recompiling applications
- ModSecurity installed
  - OWASP Core Rule Set can be enabled

More Information and Getting Involved

- More information on the project can be found at http://www.owaspbwa.org/
- Join our Google Group: owaspbwa
- Follow us on Twitter @owaspbwa
- Submit bugs and security issues to the trackers

MANDIANT®

OWASP Broken Web Applications (BWA) VM and Zed Attack Proxy (ZAP)

PRESENTED BY: **Chuck Willis**

chuck.willis@mandiant.com

@chuckatsf