OWASP BROKEN WEB APPLICATIONS (OWASP BWA)
1.0 Release
(Candidate)

Chuck Willis
chuck.willis@mandiant.com

OWASP AppSec DC
April 4, 2012
About Me

- Technical Director at Mandiant in DC
- Leader of OWASP Broken Web Applications project
- 12+ years total experience in Information Security
- Application Security, Penetration Testing, Source Code Analysis, Forensics, Incident Response, R&D

Contact:
- chuck.willis@mandiant.com
- @chuckatsf
- Attend OWASP DC Chapter meetings and CapSec (occasionally)
We are MANDIANT

- VISA Qualified Incident Response Assessor (QIRA)
- APT and CDT experts
- Application and Network Security Evaluations
- Located in
  - Washington
  - New York
  - Los Angeles
  - San Francisco
- Professional and managed services, software and education
- We are Hiring!
Motivation
Problem

- Looking for web applications with vulnerabilities where I could:
  - Test web application scanners
  - Test manual attack techniques
  - Test source code analysis tools
  - Look at the code that implements the vulnerabilities
  - Modify code to fix vulnerabilities
  - Test web application firewalls
  - Examine evidence left by attacks
• It is a great learning tool, but…

• It is a training environment, not a real application

• Same holds for many other “artificial” applications
Proprietary “Free” Apps

- Realistic applications with vulnerabilities
- Often closed source, which prevents some uses
- Can conflict with one another
- Can be difficult to install
- Licensing restrictions
Solution

- Created 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 (or add new ones)
OWASP BWA History

- Initial 0.9 release at OWASP AppSec DC 2009

- New version released once or twice a year
  - 0.94 released in July 2011

- 1.0 release candidate 1 released today
  - Full 1.0 release after short review and bug fix period
OWASP BWA Details
Virtual Machine

- Project distributes a Virtual Machine in VMware format
- Compatible with no-cost VMware Player and VMware Server (and VMware commercial products)
- Intentionally uses older virtual machine format (compatible with Workstation 5.0+ and ESX 3.0+)
- Should work in other virtualization solutions
  - Welcome any volunteers to test this
Base Operating System

- OS is Ubuntu Linux Server 10.04 LTS
  - No X-Windows / Graphical User Interface
- Managed via
  - Console
  - OpenSSH
  - Samba
  - phpMyAdmin
Base Software

- Apache
- PHP
- Perl
- MySQL
- Tomcat
- OpenJDK
- Mono
Additional Software

- SubVersion client
- GIT client
- PostgreSQL
- ModSecurity and OWASP Core Rule Set
- Custom scripts
Training Applications
Intentionally Broken Training Apps

- OWASP WebGoat version 5.4.x (Java)
- OWASP WebGoat .NET (C#)
- OWASP ESAPI SwingSet 05b2.x (Java)
- OWASP ESAPI SwingSet Interactive 1.0.1.x (Java)
- OWASP ZAP-WAVE 0.2.x (Java JSP)
- Mutillidae version 2.1.18 (PHP)
- Damn Vulnerable Web Application version 1.8.x (PHP)
- Ghost (PHP)

Highlighted items are updates in OWASP BWA 1.0
Realistic Applications
Realistic, Intentionally Broken Apps

- OWASP Vicnum version 1.4 (PHP/Perl)
- **Jotto (PHP/Perl)**
- Peruggia version 1.2 (PHP)
- Google Gruyere version 2010-07-15 (Python)
- Hackxor (Java JSP)
- WackoPicko version **2011-07-12** (PHP)
- Bodgelt **1.3.x** (Java JSP)
Old Applications
Old Versions of Real Applications

- WordPress 2.0.0 (PHP, released December 31, 2005)
- GetBoo version 1.04 (PHP, released April 7, 2008)
- 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)
- OrangeHRM version 2.4.2 (PHP, released May 7, 2009)
- gtd-php version 0.7 (PHP, released September 30, 2006)
- Joomla version 1.5.15 (PHP, released November 4, 2009)
Other Applications
Other Applications

- **Demonstration Pages / Small Applications**
  - OWASP CSRFGuard Test Application version 2.2 (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)
Other Features
Editing Applications

- Application code can be edited via SMB shares, SSH, or the console
- Updates to PHP, JSP, etc. application files will take place immediately
- Scripts provided to rebuild and redeploy applications that require it: (new)
  - WebGoat
  - Yazd
  - CSRFGuard Test Apps
  - SwingSet Apps
Updating VM (new)

- Scripts are provided to update VM from source code repositories
  - OWASP BWA specific files from Google Code SVN repository
  - Application files from their SVN or GIT repositories
- Can break applications due to changes in database schemas or dependencies
- Can allow for using updated versions of applications without waiting for a new version of OWASP BWA
• Web server on OWASP BWA is running mod_security
• By default, no rules are enabled
• Scripts are provided to:
  – Enable logging using CRS:
    ▪ `owaspbwa-modsecurity-crs-log.sh`
  – Enable blocking using CRS:
    ▪ `owaspbwa-modsecurity-crs-block.sh`
  – Disable all rules:
    ▪ `owaspbwa-modsecurity-crs-off.sh`
• Rules can be easily edited via SMB shares
Log Files

- Logging for the web and application servers are left in their default configuration
  - What you will most likely see when responding to an incident
- Logs are available via SMB share
- Logging settings can be easily edited
- Logs are cleared when VM is packaged
User Guide (new)

- User Guide has been started on Google Code Wiki
  - Welcome any volunteers to contribute to this
Where are the vulnerabilities?

- Don’t have a master list of vulnerabilities (yet)

- Counting on the community to contribute

- Using “Trac” issue tracker at SourceForge: http://sourceforge.net/apps/trac/owaspbwa/report/1
Anyone can browse issues
Tracking Known Vulnerabilities

Anyone can search issues
Anyone can see details on issues
Anyone can submit issues
Tracking Known Vulnerabilities

Registered users can edit issues
Present and Future
Version 1.0rc1 of the VM has been released today!
- Fixes some bugs, updates some applications, and adds some applications from the 0.94 release
- Download link off http://www.owaspbwa.org/

Version 1.0 final will be released after people have had a bit of time to look at the release candidate
The Future

- Continue documenting project (User Guide)
- Continue cataloging vulnerabilities into a master list
- Incorporate additional broken apps as they are suggested
We welcome any help, feedback, or broken apps you can provide!
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
OWASP BROKEN WEB APPLICATIONS (OWASP BWA)
1.0 Release (Candidate)

Chuck Willis
chuck.willis@mandiant.com

OWASP AppSec DC
April 4, 2012