



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

Chuck Willis
chuck.willis@mandiant.com

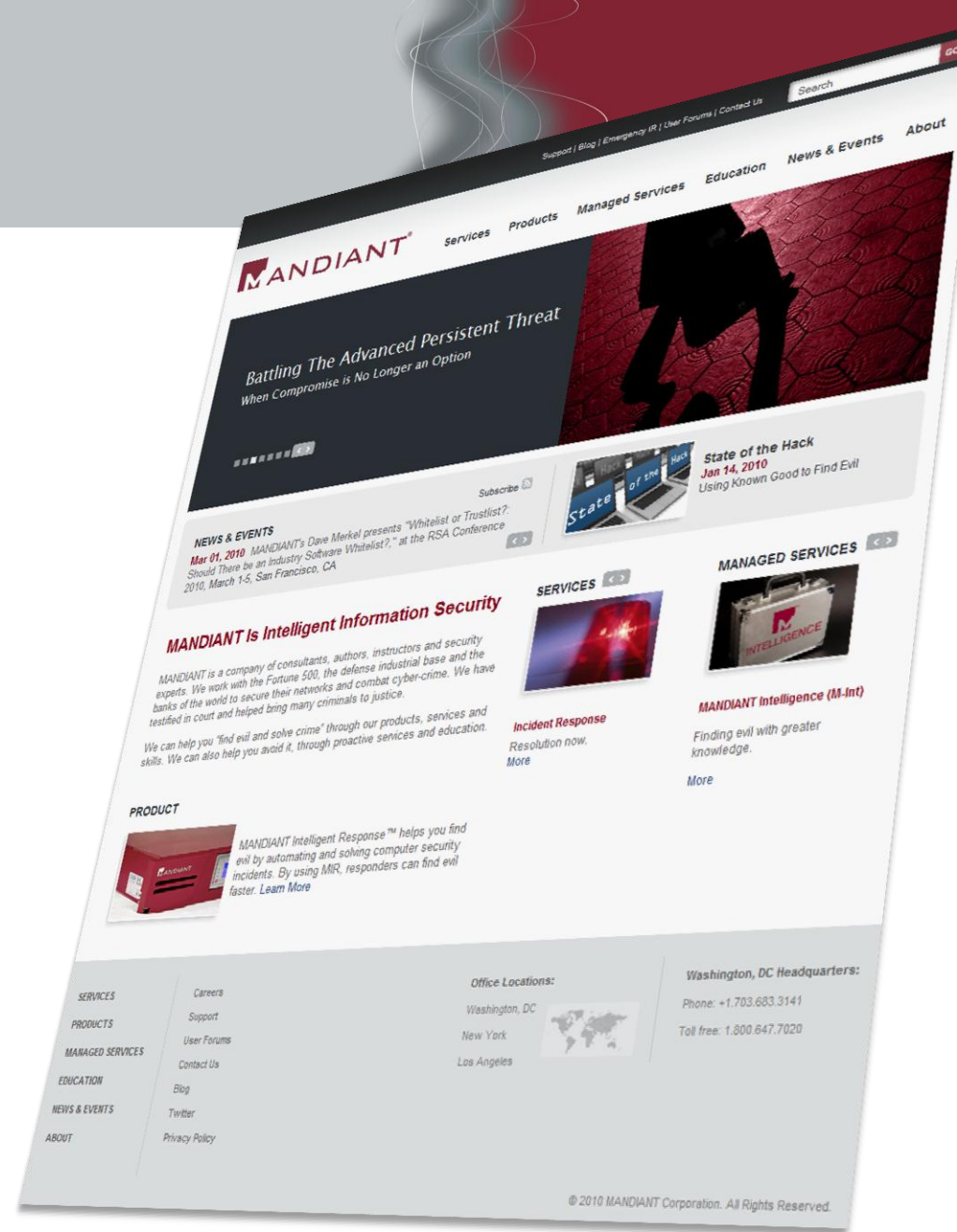
OWASP AppSec DC
April 4, 2012



- 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)

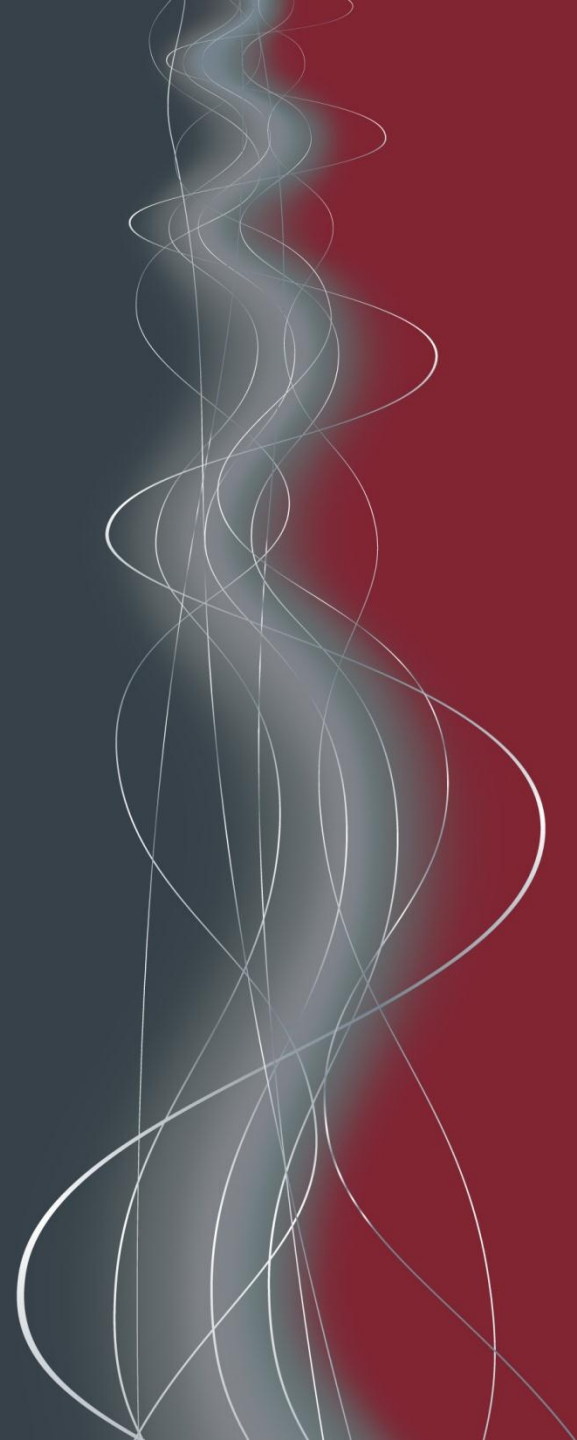
We are MANDIANT

- 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



- 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

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

- 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)

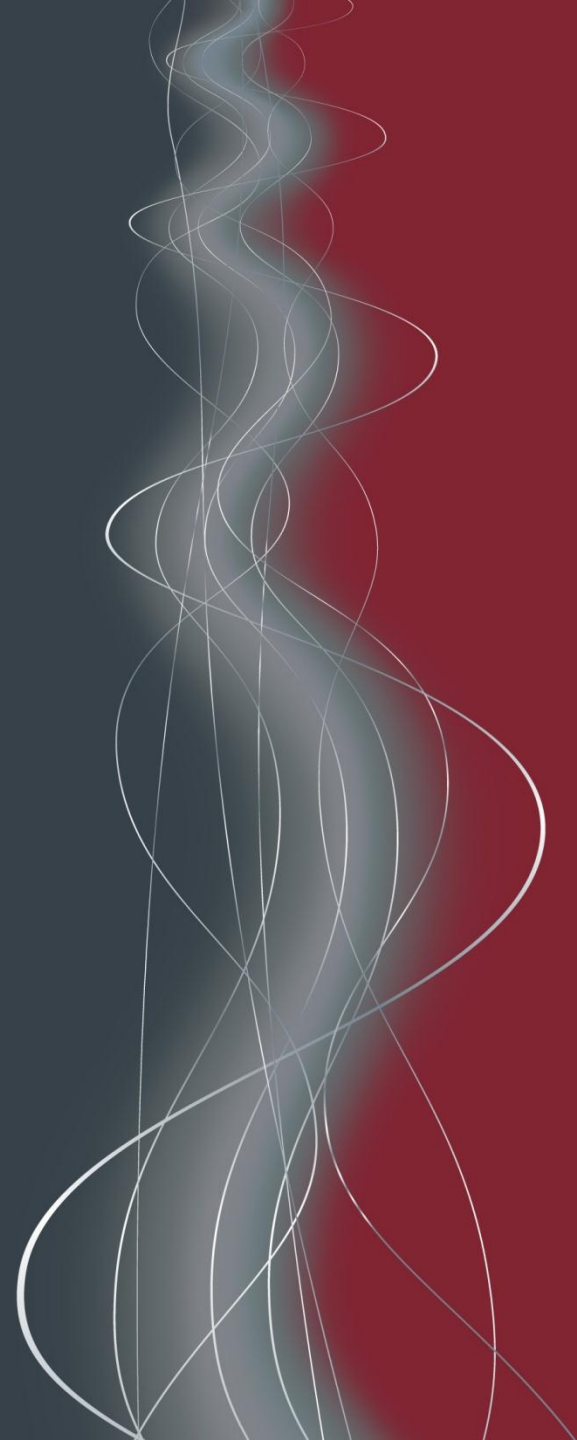
- Initial 0.9 release at OWASP AppSec DC 2009

- 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



- 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

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



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

- SubVersion client
- GIT client
- PostgreSQL
- ModSecurity and OWASP Core Rule Set
- Custom scripts



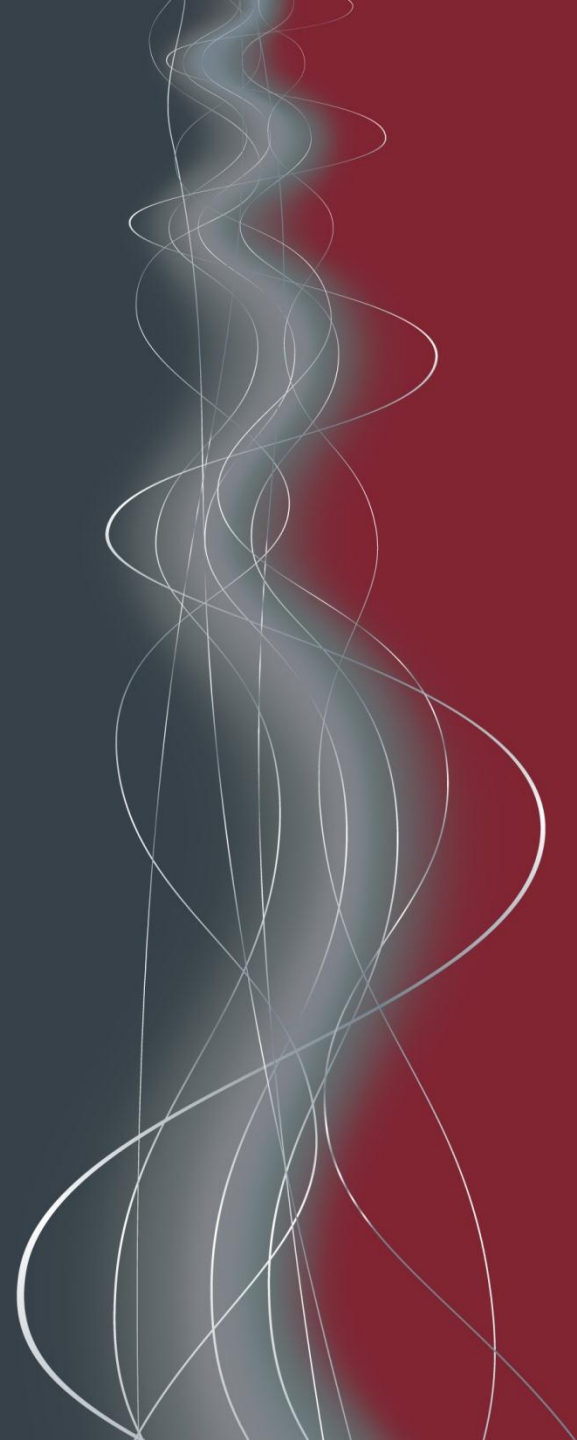
Training Applications



- 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



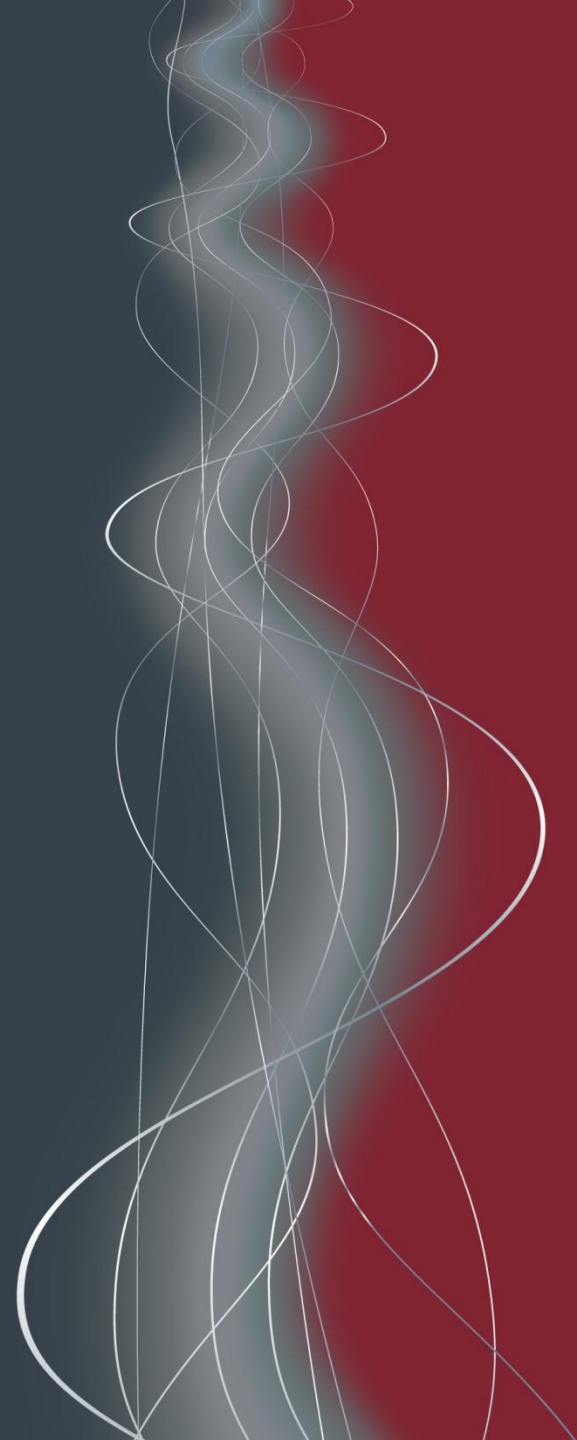
Realistic Applications



- 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)



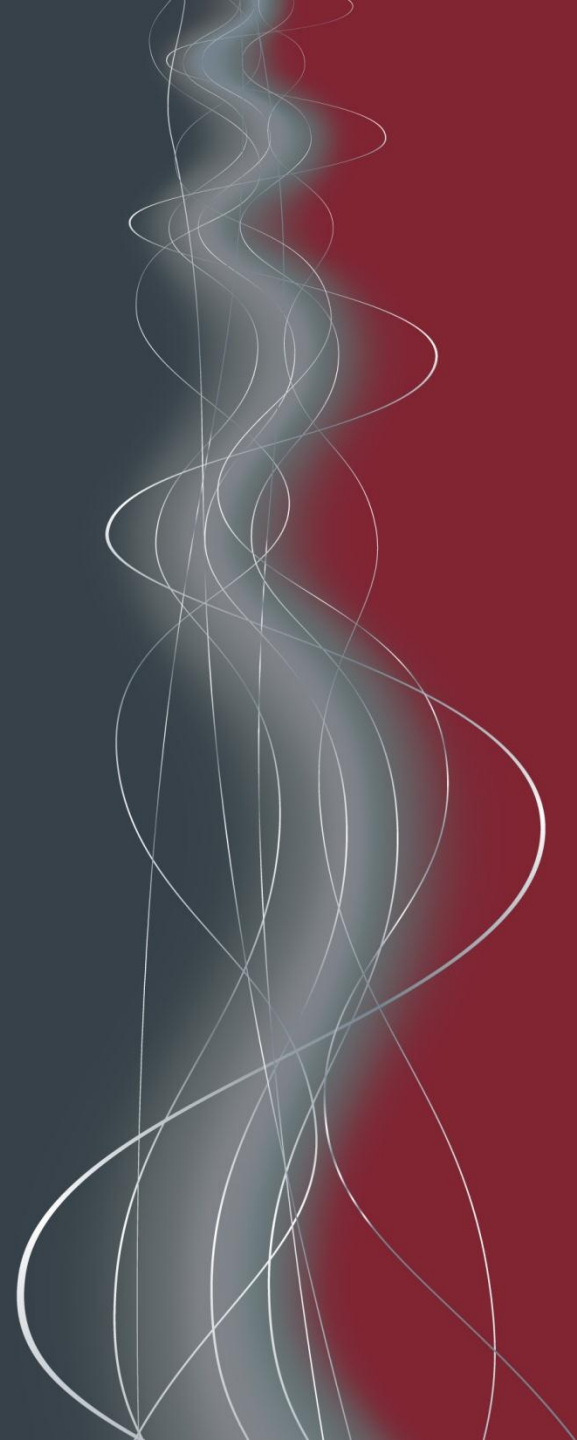
Old Applications



- 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)
- AWStats version 6.4 (Perl, released February 25, 2005)
- OrangeHRM version 2.4.2 (PHP, released May 7, 2009)
- gtd-php version 0.7 (PHP, released September 30, 2006)
- Gallery2 version 2.1 (PHP, released March 23, 2006)
- Joomla version 1.5.15 (PHP, released November 4, 2009)



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



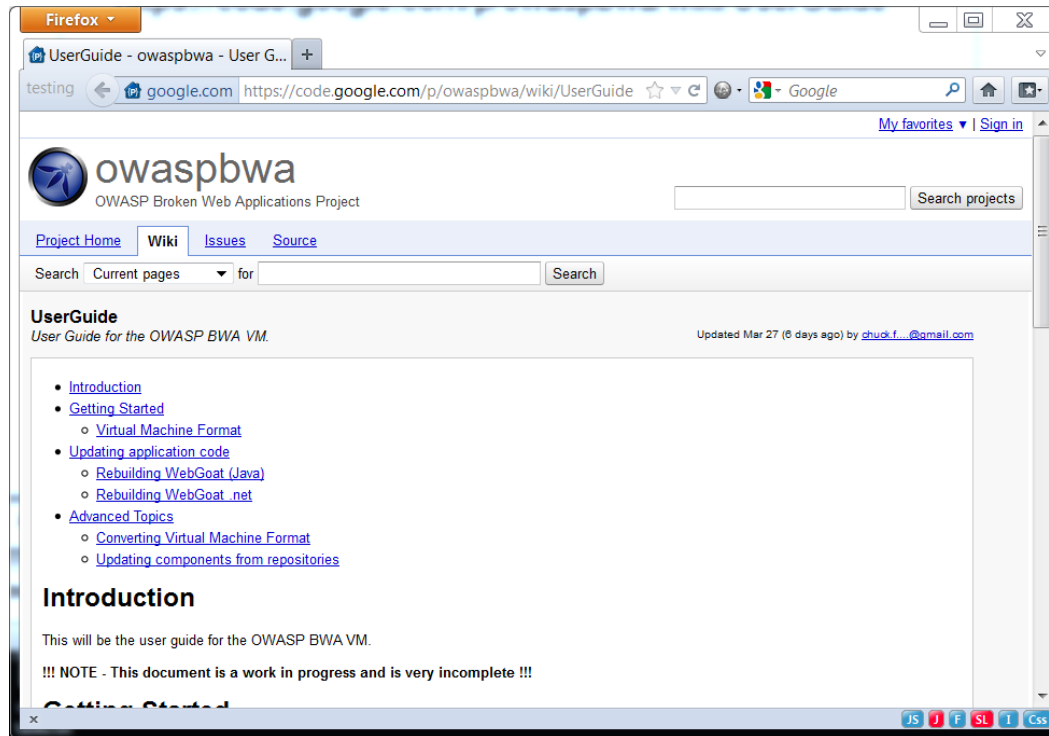
- Application code can be edited via SMB shares, SSH, or the console
- Updates to PHP, JSP, etc. application files will take place immediately
- Scripts provided to rebuild and redeploy applications that require it: **(new)**
 - WebGoat
 - Yazd
 - CSRFGuard Test Apps
 - SwingSet Apps

- 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

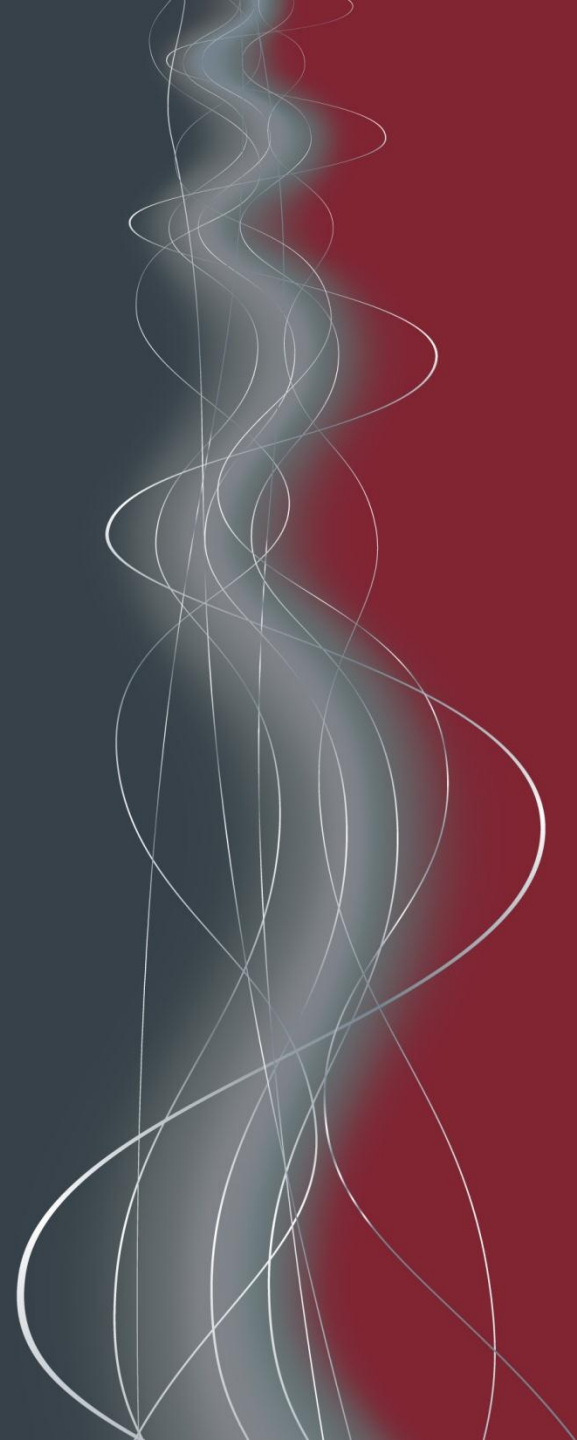
- Logging for the web and application servers are left in their default configuration
 - What you will most likely see when responding to an incident
- Logs are available via SMB share
- Logging settings can be easily edited
- Logs are cleared when VM is packaged

- User Guide has been started on Google Code Wiki
 - <https://code.google.com/p/owaspbwa/wiki/UserGuide>
 - Welcome any volunteers to contribute to this





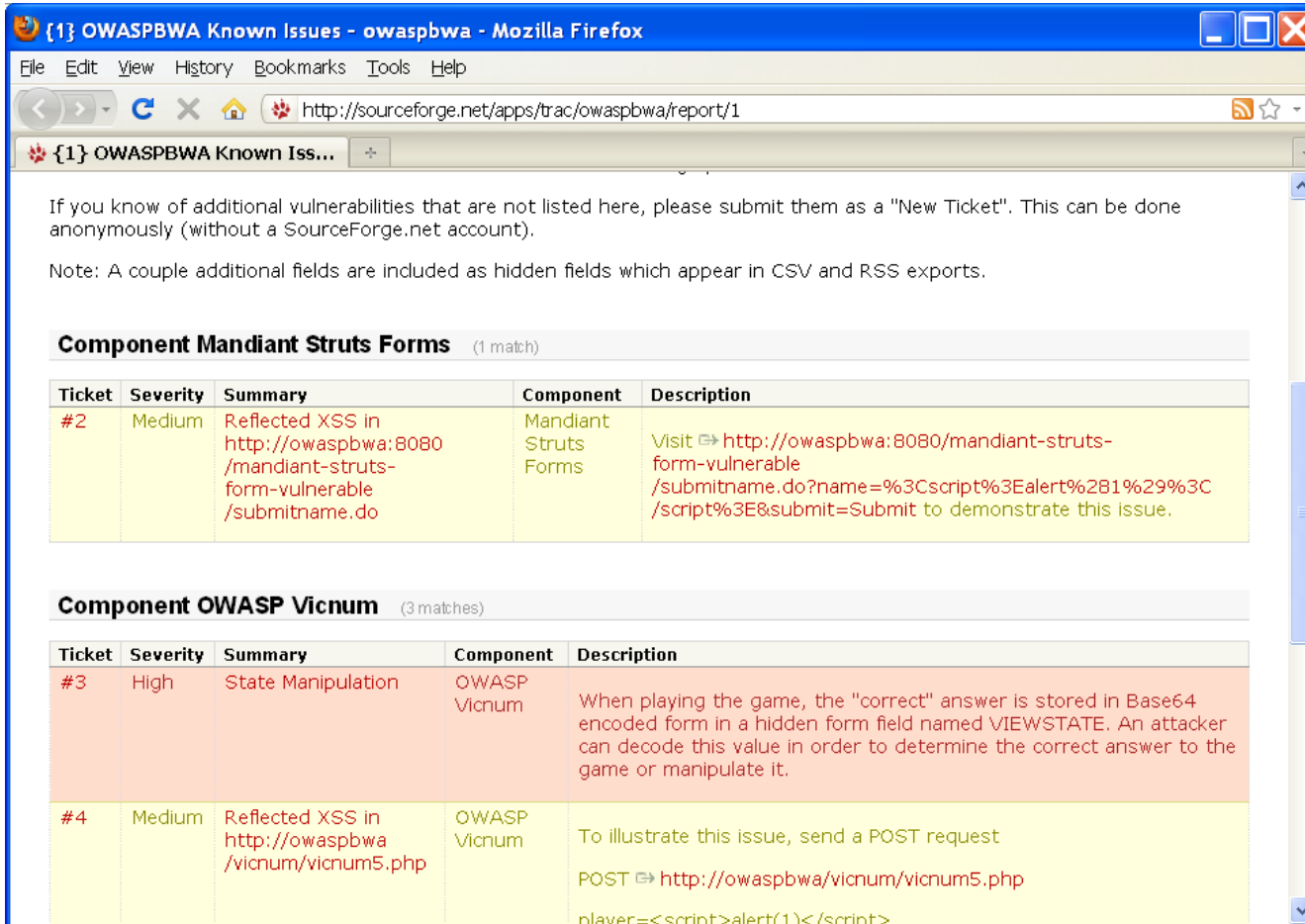
Vulnerabilities



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>

Tracking Known Vulnerabilities



If you know of additional vulnerabilities that are not listed here, please submit them as a "New Ticket". This can be done anonymously (without a SourceForge.net account).

Note: A couple additional fields are included as hidden fields which appear in CSV and RSS exports.

Component Mandiant Struts Forms (1 match)

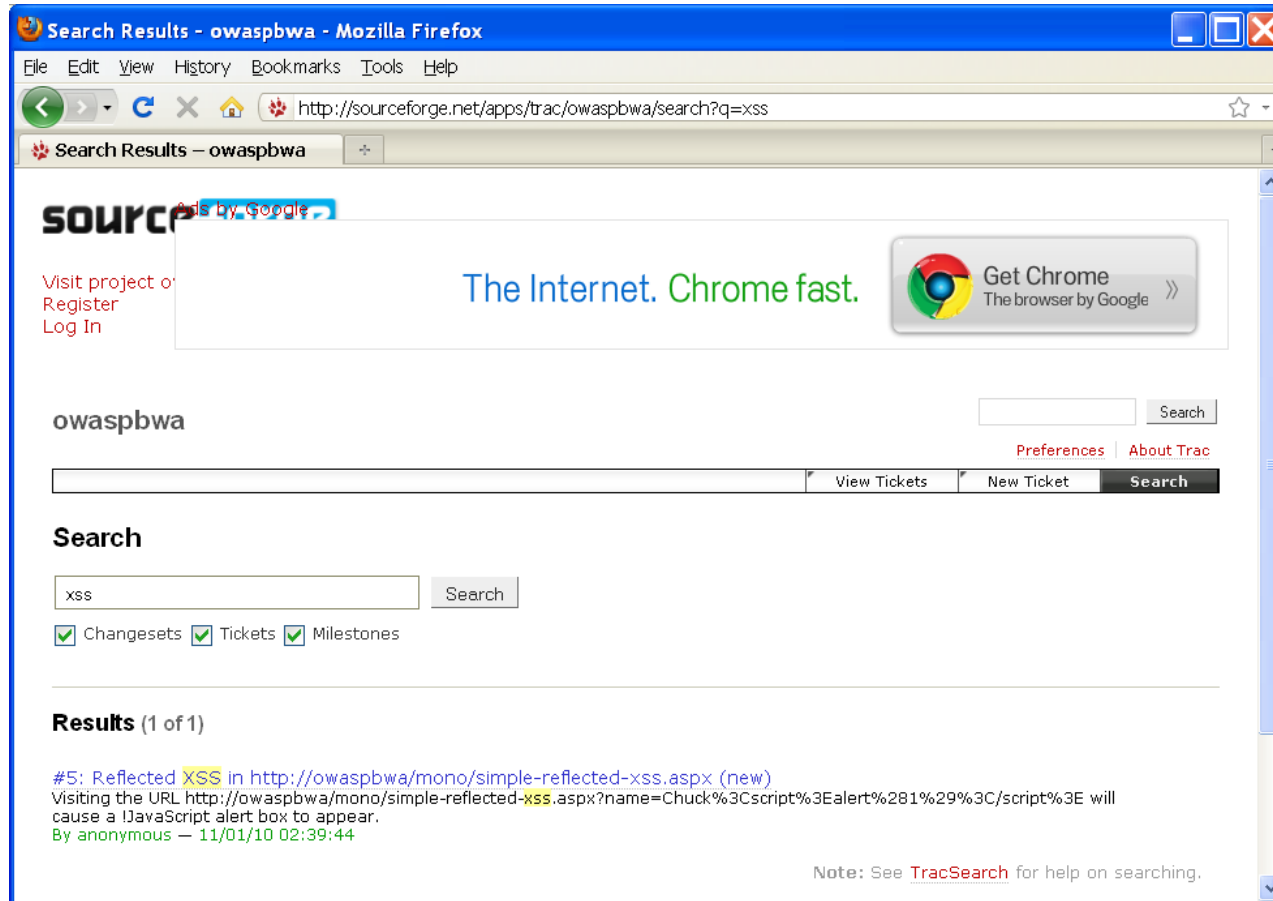
Ticket	Severity	Summary	Component	Description
#2	Medium	Reflected XSS in http://owaspbwa:8080/mandiant-struts-form-vulnerable/submitname.do	Mandiant Struts Forms	Visit http://owaspbwa:8080/mandiant-struts-form-vulnerable/submitname.do?name=%3Cscript%3Ealert%281%29%3C/script%3E&submit=Submit to demonstrate this issue.

Component OWASP Vicnum (3 matches)

Ticket	Severity	Summary	Component	Description
#3	High	State Manipulation	OWASP Vicnum	When playing the game, the "correct" answer is stored in Base64 encoded form in a hidden form field named VIEWSTATE. An attacker can decode this value in order to determine the correct answer to the game or manipulate it.
#4	Medium	Reflected XSS in http://owaspbwa/vicnum/vicnum5.php	OWASP Vicnum	To illustrate this issue, send a POST request POST http://owaspbwa/vicnum/vicnum5.php <code>player=<script>alert(1)</script></code>

Anyone can browse issues

Tracking Known Vulnerabilities



Anyone can search issues

Tracking Known Vulnerabilities

The screenshot shows a Mozilla Firefox browser window with the title "#4 (Reflected XSS in http://owaspbwa/vicnum/vicnum5.php) - owaspbwa - Mozilla Firefox". The address bar shows the URL "http://sourceforge.net/apps/trac/owaspbwa/ticket/4". The page content includes a search bar, navigation links like "View Tickets", "New Ticket", and "Search", and a detailed view of "Ticket #4 (new)".

Ticket #4 (new)

Reflected XSS in http://owaspbwa/vicnum/vicnum5.php Opened 9 days ago

Reported by:	anonymous	Owned by:	chuckatsf
Component:	OWASP Vicnum	Version:	0.92rc1
Severity:	Medium	Keywords:	
Cc:			

Description

To illustrate this issue, send a POST request

POST ⇒ <http://owaspbwa/vicnum/vicnum5.php>

```
player=<script>alert(1)</script>
```

Note: See [TracTickets](#) for help on using tickets.

Anyone can see details on issues

Tracking Known Vulnerabilities

The screenshot shows a Mozilla Firefox browser window titled "New Ticket - owaspbwa - Mozilla Firefox". The address bar displays the URL "http://sourceforge.net/apps/trac/owaspbwa/newticket". The page content includes a navigation bar with "View Tickets", "New Ticket", and "Search" buttons. The main heading is "Create New Ticket".

Reporter
Your email or username:

Properties

Summary:

Description:
B I A [Rich Text Editor Icons]

Component:

Version:

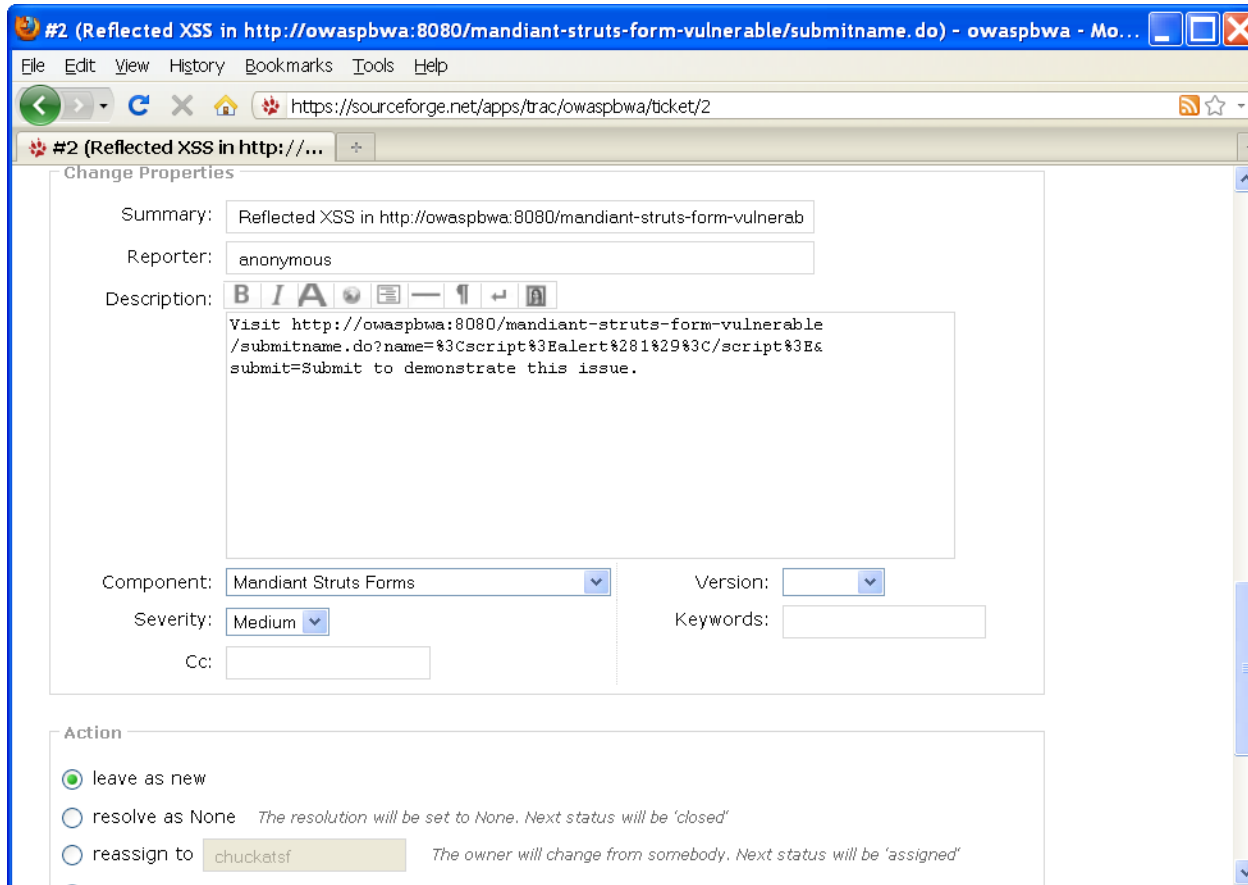
Severity:

Keywords:

Cc:

Anyone can submit issues

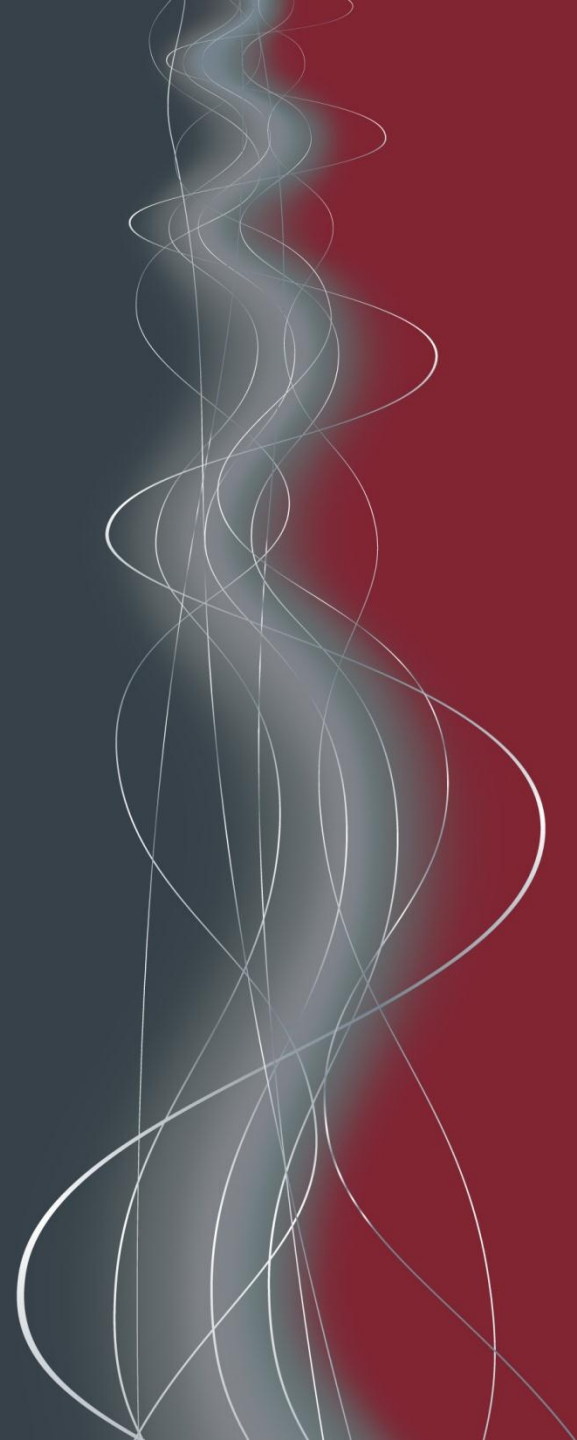
Tracking Known Vulnerabilities



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

- 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 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

