MANDIANT®

OWASP BROKEN WEB APPLICATIONS PROJECT

Chuck Willis
chuck.willis@mandiant.com

OWASP AppSec DC
November 10, 2010

About Me

- MANDIANT
  - Commercial Services
  - Federal Services
  - Training and Education
  - Product – Mandiant Intelligent Response
- My Experience
  - 10+ years total experience in Information Security
  - Penetration Testing, Application Security, Source Code Analysis, Forensics, Incident Response, R&D
- Member of OWASP DC Chapter (and CapSec)

Problem

- I was 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

Option – WebGoat

- It is a great learning tool, but
- It is a training environment, not a real application
- Same holds for other “artificial” applications

Option – 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 – OWASP Broken Web Application Project

- Free Linux-based Virtual Machine in VMware format
- 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)

Base Software

- Based on Ubuntu Linux Server 10.04 LTS
  - No X-Windows
  - Apache
  - PHP
  - Perl
  - MySQL
  - PostgreSQL
  - Tomcat
  - OpenJDK
  - Mono

Management Software

- OpenSSH
- Samba
- phpMyAdmin
- Subversion Client

Intentionally Broken Apps

- OWASP WebGoat version 5.3.x (Java)
- OWASP Vicnum version 1.4 (PHP/Perl)
- Mutillidae version 1.5 (PHP)
- Damn Vulnerable Web Application version 1.07.x (PHP)
- OWASP CSRFGuard Test Application version 2.2 (Java) – Broken and “Not broken” versions

Intentionally Broken Apps

- Ghost (PHP)
- Peruggia version 1.2 (PHP)
- Mandiant Struts Forms (Java/Struts)
- Simple ASP.NET Forms (ASP.NET/C#)
- Simple Form with DOM Cross Site Scripting (HTML/JavaScript)

- LOOKING FOR DONATIONS!

Old Versions of Real Applications

- phpBB 2.0.0 (PHP, released April 4, 2002)
- WordPress 2.0.0 (PHP, released December 31, 2005)
- 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)

- LOOKING FOR IDEAS!

OWASP Demo Applications

- Applications without known vulnerabilities

- Only one so far:
  - OWASP AppSensor Demo Application (Java)

- Looking to add:
  - ESAPI SwingSet Application (Java, maybe others)
  - Any other applications available

Who Moved My Cheese?

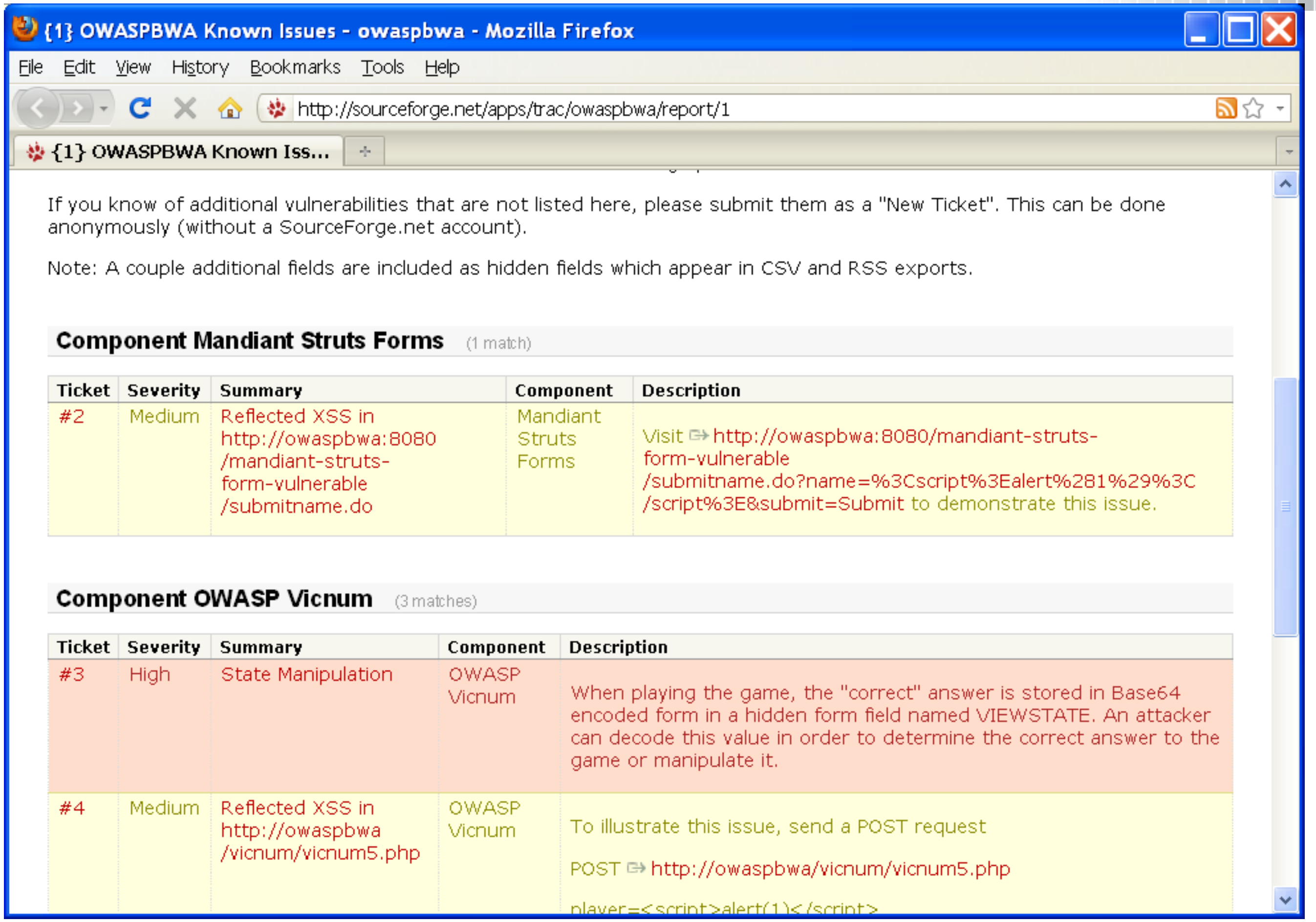
- We would like to include Google’s Gruyere in the VM, but we cannot:
  - Its license does not allow for distribution of modified versions
  - It contains security controls that restrict remote access to the application

- If anyone from Google is here, I’d love to talk

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


{1} OWASPBWA Known Issues - owaspbwa - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://sourceforge.net/apps/trac/owaspbwa/report/1
{1} OWASPBWA Known Iss...

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)

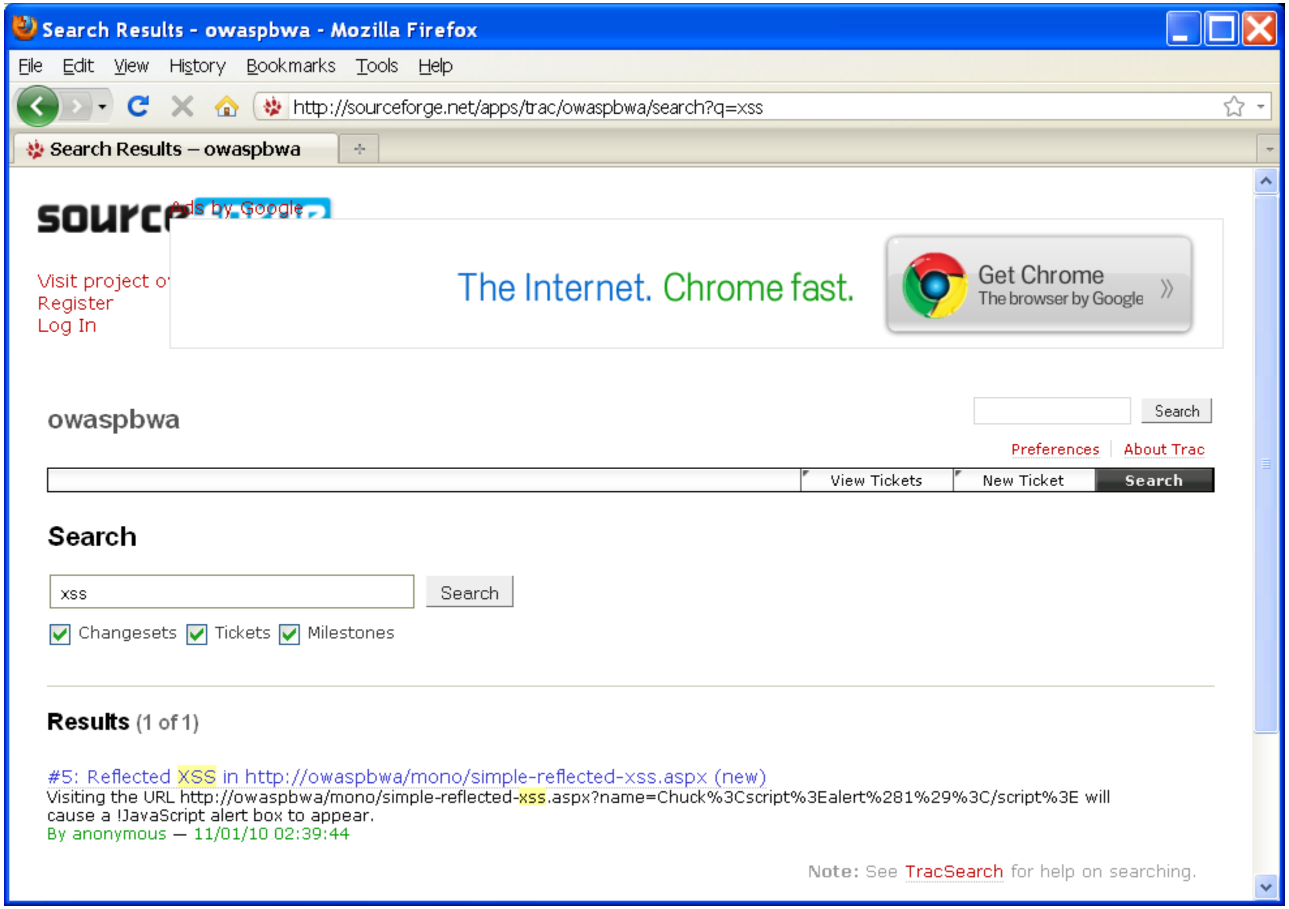
Ticket	Severity	Summary	Component	Description
#2	Medium	Reflected XSS in http://owaspbwa:8080/mandiant-struts-form-vulnerable/submitname.do	Mandiant Struts Forms	Visit http://owaspbwa:8080/mandiant-struts-form-vulnerable/submitname.do?name=%3Cscript%3Ealert%281%29%3C/script%3E&submit=Submit to demonstrate 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 player=<script>alert(1)</script>

Anyone can browse issues

Tracking Known Vulnerabilities



Search Results - owaspbwa - Mozilla Firefox

http://sourceforge.net/apps/trac/owaspbwa/search?q=xss

Ads by Google

The Internet. Chrome fast. Get Chrome The browser by Google

Visit project o
Register
Log In

owaspbwa

Preferences | About Trac

View Tickets | New Ticket | Search

Search

xss [Search]

☑ Changesets ☑ Tickets ☑ Milestones

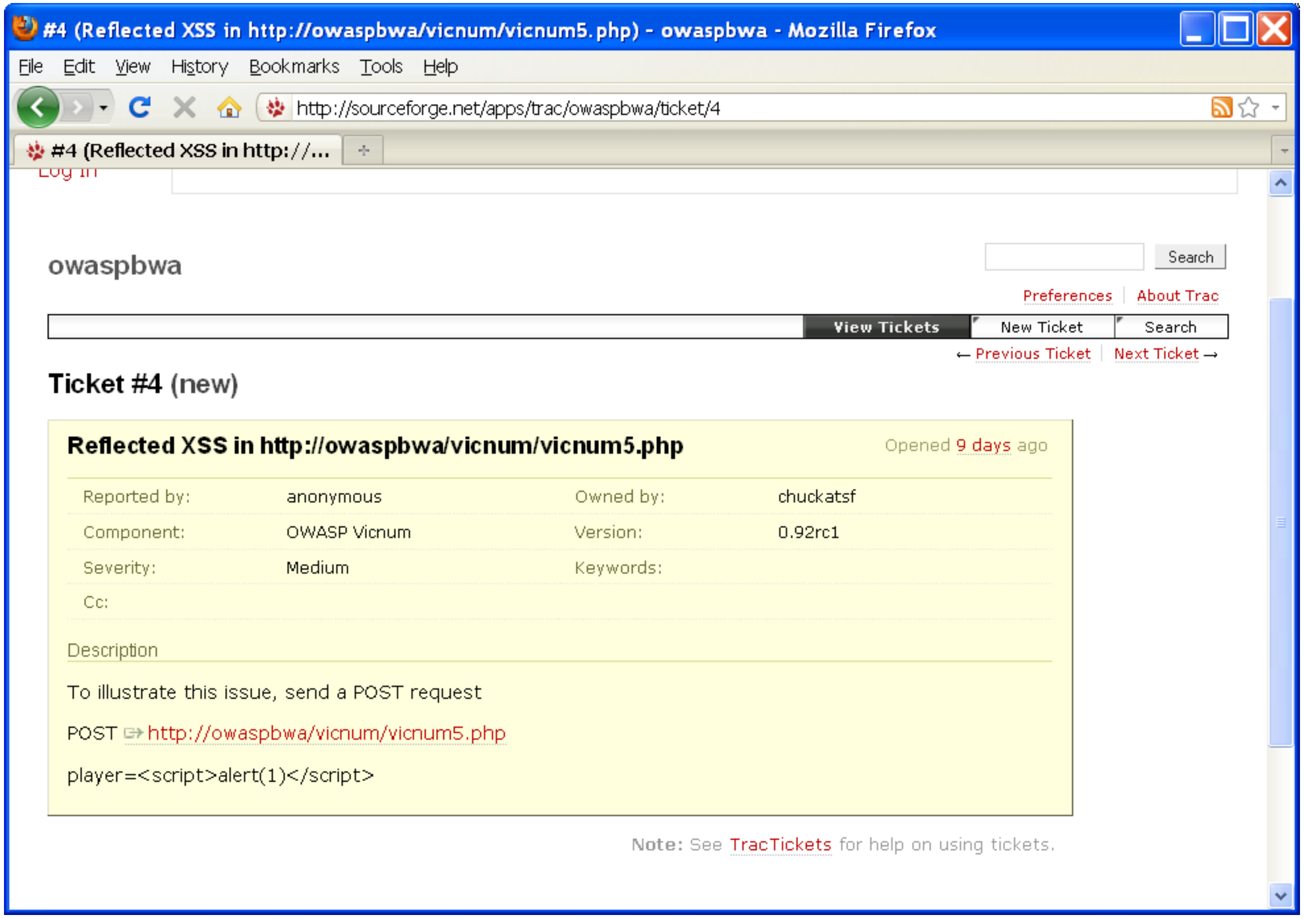
Results (1 of 1)

#5: Reflected XSS in http://owaspbwa/mono/simple-reflected-xss.aspx (new)
Visiting the URL http://owaspbwa/mono/simple-reflected-xss.aspx?name=Chuck%3Cscript%3Ealert%281%29%3C/script%3E will cause a !JavaScript alert box to appear.
By anonymous — 11/01/10 02:39:44

Note: See TracSearch for help on searching.

Anyone can search issues

Tracking Known Vulnerabilities


#4 (Reflected XSS in http://owaspbwa/vicnum/vicnum5.php) - owaspbwa - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://sourceforge.net/apps/trac/owaspbwa/ticket/4
#4 (Reflected XSS in http://...
Log in
owaspbwa
Search
Preferences
About Trac
View Tickets
New Ticket
Search
← Previous Ticket
Next Ticket →

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

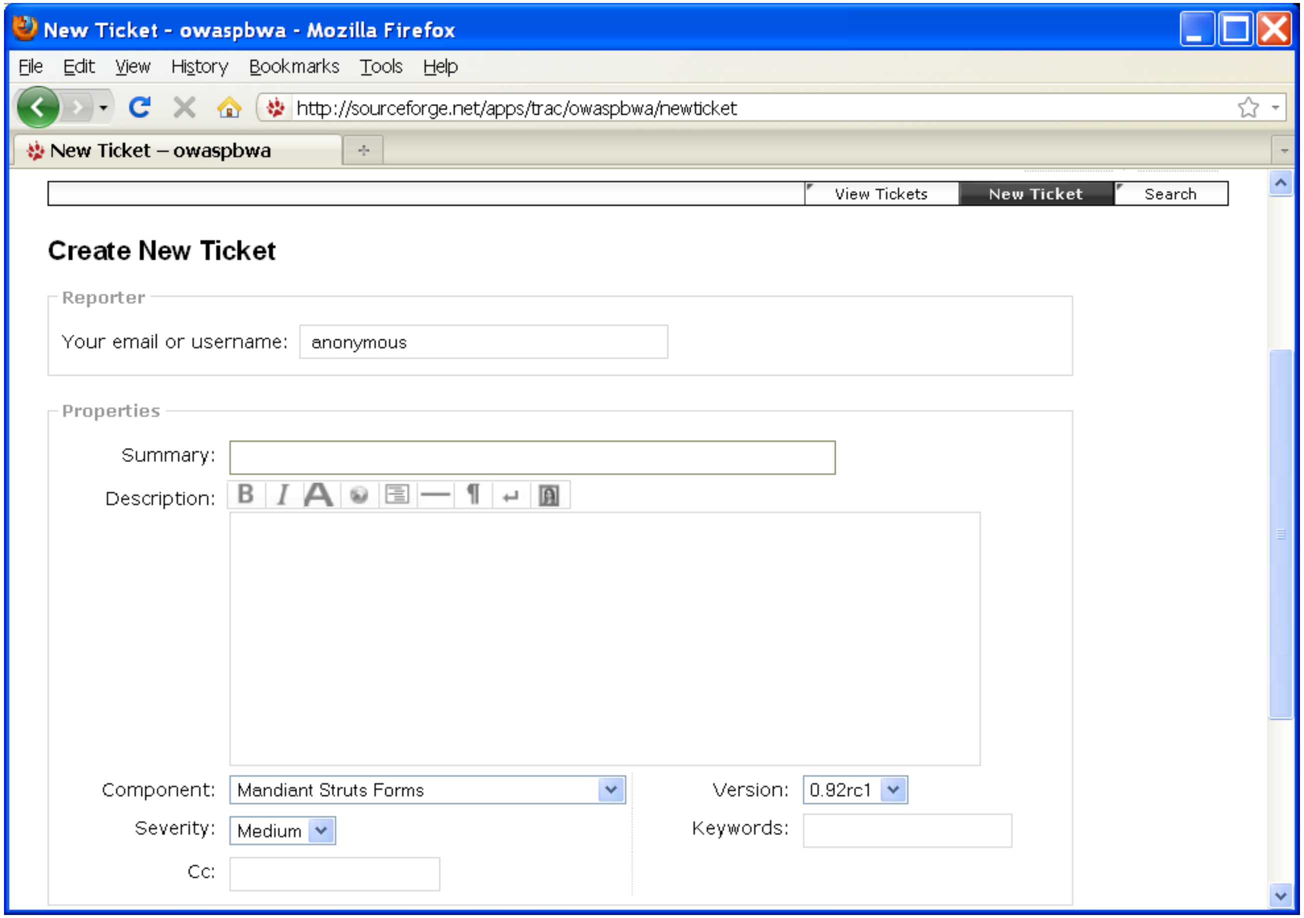
POST http://owaspbwa/vicnum/vicnum5.php

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

Note: See TracTickets for help on using tickets.

Anyone can see details on issues

Tracking Known Vulnerabilities


New Ticket - owaspbwa - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://sourceforge.net/apps/trac/owaspbwa/newticket
New Ticket – owaspbwa
View Tickets
New Ticket
Search

Create New Ticket

Reporter

Your email or username: anonymous

Properties

Summary:

Description:

Component: Mandiant Struts Forms

Version: 0.92rc1

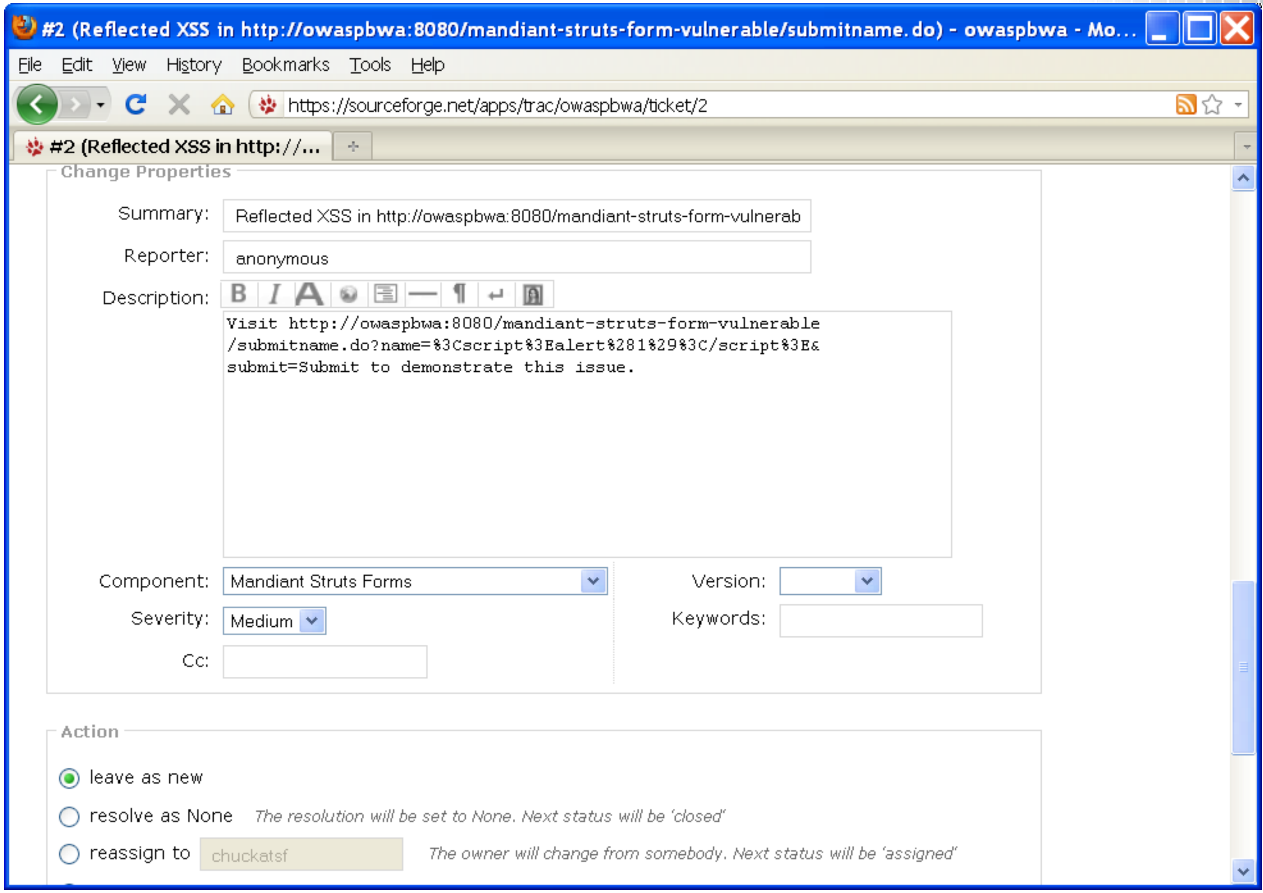
Severity: Medium

Keywords:

Cc:

Anyone can submit issues

Tracking Known Vulnerabilities


#2 (Reflected XSS in http://owaspbwa:8080/mandiant-struts-form-vulnerable/submitname.do) - owaspbwa - Mo...
File Edit View History Bookmarks Tools Help
https://sourceforge.net/apps/trac/owaspbwa/ticket/2
#2 (Reflected XSS in http://...

Change Properties

Summary: Reflected XSS in http://owaspbwa:8080/mandiant-struts-form-vulnerab

Reporter: anonymous

Description:

```
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: Mandiant Struts Forms

Version:

Severity: Medium

Keywords:

Cc:

Action

● leave as new

○ resolve as None *The resolution will be set to None. Next status will be 'closed'*

○ reassign to chuckatsf *The owner will change from somebody. Next status will be 'assigned'*

Registered users can edit issues (may open this to all)

New Release and Downloads

- Version 0.92rc1 of the VM has been released today!
  - Fixes some bugs and adds some applications from the 0.91rc1 release
  - Fully functional, just fewer applications than we would like
  - Download link off http://www.owaspbwa.org/

- Version 1.0 release is on the horizon

The Future

- Incorporate additional broken apps
  - The larger, the better
  - More Java applications, especially ones based on Struts or Spring
  - Non-trivial .NET applications
  - Adobe Flash (could use some help here)
  - Other languages? Ruby, Perl, Python, others?
- Catalog vulnerabilities into a master list
- Add ability to easily enable / configure ModSecurity
- Include additional OWASP “Demo” applications

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 PROJECT

Chuck Willis
chuck.willis@mandiant.com

OWASP AppSec DC
November 10, 2010