Watcher

Surfing for Bugs

OWASP AppSecDC

November 2009

Chris Weber

chris@casabasecurity.com

Casaba Security

Watcher

Get it

http://websecuritytool.codeplex.com

Watcher

Main Features

- Passive detection
- Simple use, low overhead
- 35 checks and growing
- Integrated Bug Reporting
- Extensible

Watcher

Why should you use it?

- It’s free
- It works
- Microsoft SDL recommended tool

Watcher

How do you use it?

- Install Fiddler
- Install Watcher plugin
- Open your Web browser
- Cruise your site (*exploratory-testing*)

Watcher

Intended purpose

- Quick sanity checks between dev builds
- **Hot-spot** detection for pen-testing
- Automated auditing of low-hanging fruit

Watcher

Design

- C#
- A plugin for Fiddler HTTP proxy
  - www.fiddlertool.com
- Analyze HTTP requests/responses

Watcher

35+ checks and counting…

- Unicode hot-spots
- XSS hot-spots
- User-controlled HTML
- Cross-domain issues
- Insecure cookies
- Insecure HTTP/HTTPS transitions
- SSL protocol and certificate issues
- Flash issues
- Silverlight issues
- Information disclosure
- …

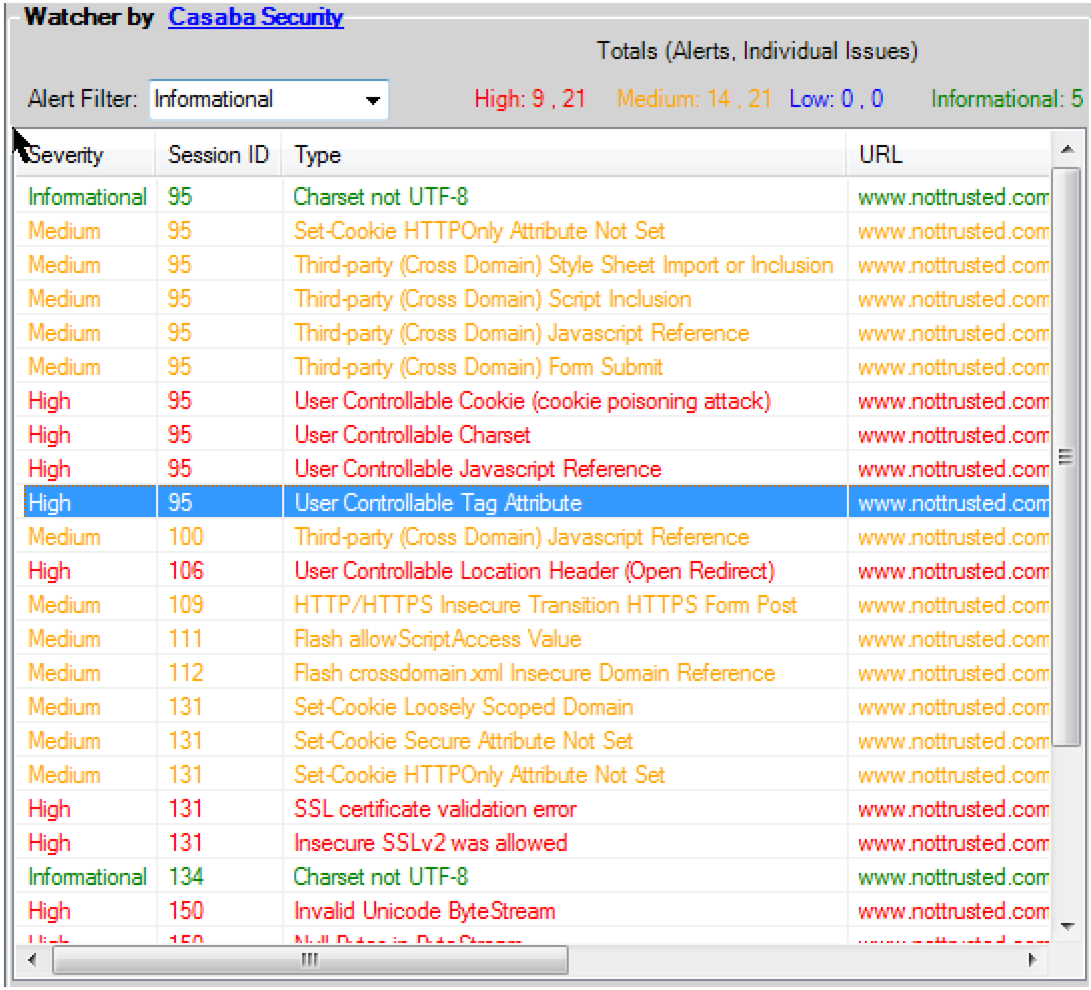
Watcher

Roadmap

- Looking for contributors
- Checks
  - Flash analysis
  - Silverlight analysis
  - Better XSS detection

Watcher

Demo



Watcher by Casaba Security

Totals (Alerts, Individual Issues)

Alert Filter: Informational

High: 9 , 21 Medium: 14 , 21 Low: 0 , 0 Informational: 5

Severity	Session ID	Type	URL
Informational	95	Charset not UTF-8	www.nottrusted.com
Medium	95	Set-Cookie HTTPOnly Attribute Not Set	www.nottrusted.com
Medium	95	Third-party (Cross Domain) Style Sheet Import or Inclusion	www.nottrusted.com
Medium	95	Third-party (Cross Domain) Script Inclusion	www.nottrusted.com
Medium	95	Third-party (Cross Domain) Javascript Reference	www.nottrusted.com
Medium	95	Third-party (Cross Domain) Form Submit	www.nottrusted.com
High	95	User Controllable Cookie (cookie poisoning attack)	www.nottrusted.com
High	95	User Controllable Charset	www.nottrusted.com
High	95	User Controllable Javascript Reference	www.nottrusted.com
High	95	User Controllable Tag Attribute	www.nottrusted.com
Medium	100	Third-party (Cross Domain) Javascript Reference	www.nottrusted.com
High	106	User Controllable Location Header (Open Redirect)	www.nottrusted.com
Medium	109	HTTP/HTTPS Insecure Transition HTTPS Form Post	www.nottrusted.com
Medium	111	Flash allowScriptAccess Value	www.nottrusted.com
Medium	112	Flash crossdomain.xml Insecure Domain Reference	www.nottrusted.com
Medium	131	Set-Cookie Loosely Scoped Domain	www.nottrusted.com
Medium	131	Set-Cookie Secure Attribute Not Set	www.nottrusted.com
Medium	131	Set-Cookie HTTPOnly Attribute Not Set	www.nottrusted.com
High	131	SSL certificate validation error	www.nottrusted.com
High	131	Insecure SSLv2 was allowed	www.nottrusted.com
Informational	134	Charset not UTF-8	www.nottrusted.com
High	150	Invalid Unicode ByteStream	www.nottrusted.com
High	150	Null Bytes in ByteStream	www.nottrusted.com

Thank you!

Casaba Security

www.casabasecurity.com

Chris Weber

Blog: www.lookout.net

Email: chris@casabasecurity.com

LinkedIn: http://www.linkedin.com/in/chrisweber