black hat USA 2014

OWASP ZAP Turbo Talk

Simon Bennetts

OWASP ZAP Project Lead
Mozilla Security Team

Plan

- Introduce ZAP
- Overview of the basics
- Dive into some more advanced features
- Overview of some work in progress
- Perform more demos on the stand :
  - Breakers JK – Station 1
  - 12:45 – 15:15 (after this talk)

What is ZAP?

- Its completely free
- Its a community project
- The most active open source web appsec tool
- Its NOT a clone of <insert tool>
- A tool for beginners and pros
- The ToolsWatch.org top security tool of 2013 ;)

Some Statistics

- Released September 2010, fork of Paros
- V 2.3.1 released May 2014, > 40k downloads
- The most active OWASP Project
- Highest activity category on Open Hub
- 31 active developers
- Over 90 translators
- Being translated into over 20 languages
- Paros code ~ 20%   ZAP code ~80%

Why should you care?

- ~~Its free~~ (it is, but you're pros)
- Its very powerful (if you know how to use it)
- Its open source – you can change anything
- Its a community project – you can get involved
- Its a great environment to play in
- It promotes innovation
- Your clients could (should?) be using it
- Its 'encouraging' commercial tools to improve

The basics

- Yes, it does the basics
- Maybe in a different way to your current tool
- You'll work it out :)

Advanced stuff :)

- Contexts
- Advanced Active Scanning
- Plug-n-Hack
- Scripts
- Zest

Contexts

- Assign characteristics to groups of URLs
- An application can be:
  - One site

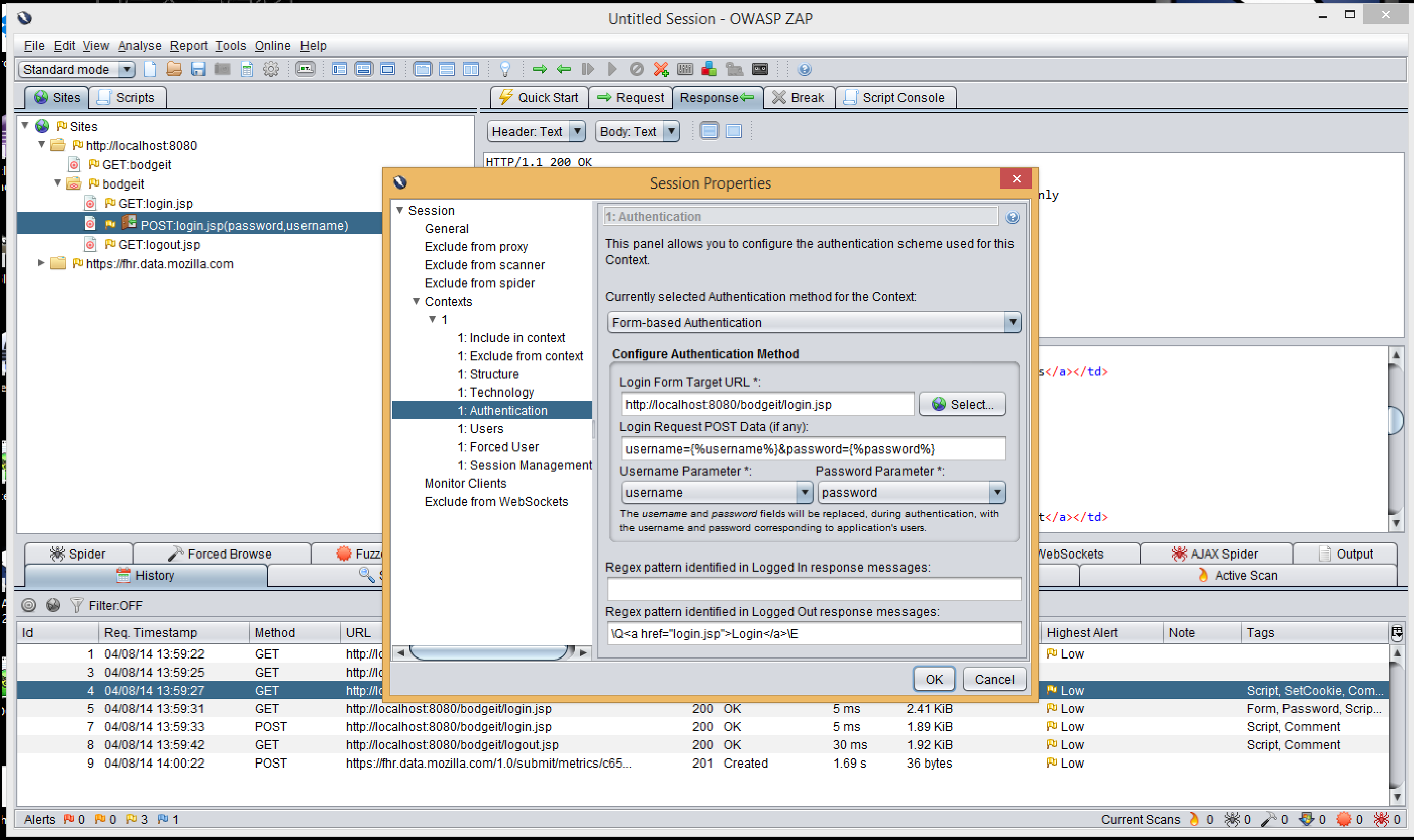
    http://www.example.com
  - A subtree

    http://www.example.com/app1
  - Multiple sites

    http://www.example1.com
    http://www.example2.com

Contexts

- Allow you to define:
  - Scope
  - Session handling
  - Authentication
  - Users
  - Structure
  - with more coming soon



Sites
- http://localhost:8080
  - GET:bodgeit
  - bodgeit
    - GET:login.jsp
    - POST:login.jsp(password,username)
    - GET:logout.jsp
- https://fhr.data.mozilla.com

```
HTTP/1.1 200 OK
```

Session Properties

1: Authentication

This panel allows you to configure the authentication scheme used for this Context.

Currently selected Authentication method for the Context: Form-based Authentication

Configure Authentication Method

Login Form Target URL *: http://localhost:8080/bodgeit/login.jsp

Login Request POST Data (if any): username={%username%}&password={%password%}

Username Parameter *: username

Password Parameter *: password

The *username* and *password* fields will be replaced, during authentication, with the username and password corresponding to application's users.

Regex pattern identified in Logged In response messages:

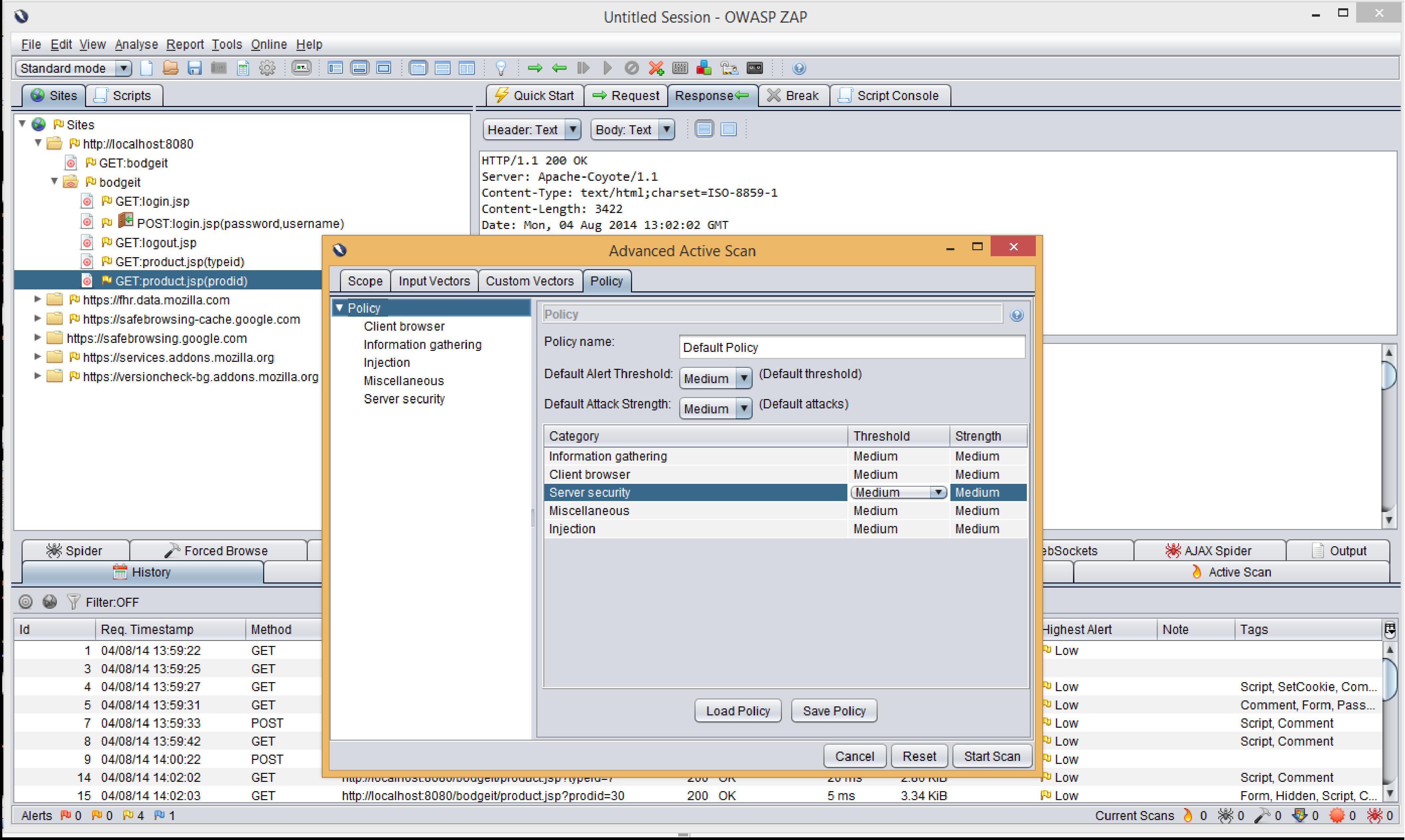
Regex pattern identified in Logged Out response messages: \Q<a href="login.jsp">Login</a>\E

Id	Req. Timestamp	Method	URL					Highest Alert	Note	Tags
1	04/08/14 13:59:22	GET	http://lc					Low		
3	04/08/14 13:59:25	GET	http://lc							
4	04/08/14 13:59:27	GET	http://lc					Low		Script, SetCookie, Com...
5	04/08/14 13:59:31	GET	http://localhost:8080/bodgeit/login.jsp	200	OK	5 ms	2.41 KiB	Low		Form, Password, Scrip...
7	04/08/14 13:59:33	POST	http://localhost:8080/bodgeit/login.jsp	200	OK	5 ms	1.89 KiB	Low		Script, Comment
8	04/08/14 13:59:42	GET	http://localhost:8080/bodgeit/logout.jsp	200	OK	30 ms	1.92 KiB	Low		Script, Comment
9	04/08/14 14:00:22	POST	https://fhr.data.mozilla.com/1.0/submit/metrics/c65...	201	Created	1.69 s	36 bytes	Low		

Alerts 0 0 3 1 Current Scans 0 0 0 0 0 0

Advanced Scanning

- Gives you fine grained control over:
  - Scope
  - Input Vectors
  - Custom Vectors
  - Policy
- Accessed from:
  - Right click Attack menu
  - Tools menu
  - Key board shortcut (default Ctrl-Alt-A)



```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 3422
Date: Mon, 04 Aug 2014 13:02:02 GMT
```

Policy

Policy name: Default Policy

Default Alert Threshold: Medium (Default threshold)

Default Attack Strength: Medium (Default attacks)

Category	Threshold	Strength
Information gathering	Medium	Medium
Client browser	Medium	Medium
Server security	Medium	Medium
Miscellaneous	Medium	Medium
Injection	Medium	Medium

Id	Req. Timestamp	Method						Highest Alert	Note	Tags
1	04/08/14 13:59:22	GET						Low		
3	04/08/14 13:59:25	GET								
4	04/08/14 13:59:27	GET						Low		Script, SetCookie, Com...
5	04/08/14 13:59:31	GET						Low		Comment, Form, Pass...
7	04/08/14 13:59:33	POST						Low		Script, Comment
8	04/08/14 13:59:42	GET						Low		Script, Comment
9	04/08/14 14:00:22	POST						Low		
14	04/08/14 14:02:02	GET	http://localhost:8080/bodgeit/product.jsp?typeid=7	200	OK	20 ms	2.80 KiB	Low		Script, Comment
15	04/08/14 14:02:03	GET	http://localhost:8080/bodgeit/product.jsp?prodid=30	200	OK	5 ms	3.34 KiB	Low		Form, Hidden, Script, C...

Plug-n-Hack

- Allows browsers and security tools to work better together
- Developed by the Mozilla Security Team
- Adopted by Burp and OWTF
- V1 allows you to:
  - Quickly configure your browser and security tool
  - Control your security tool from the browser
- V2 allows you to intercept, change and fuzz client side messages

Scripting

- Full access to ZAP internals
- Invoked from all key parts of the ZAP core
- Plugable – you can add your own types
- Support for all JSR 223 languages, inc
  - JavaScript
  - Jython
  - Jruby
  - Zest :)

Scripting

- Different types of scripts

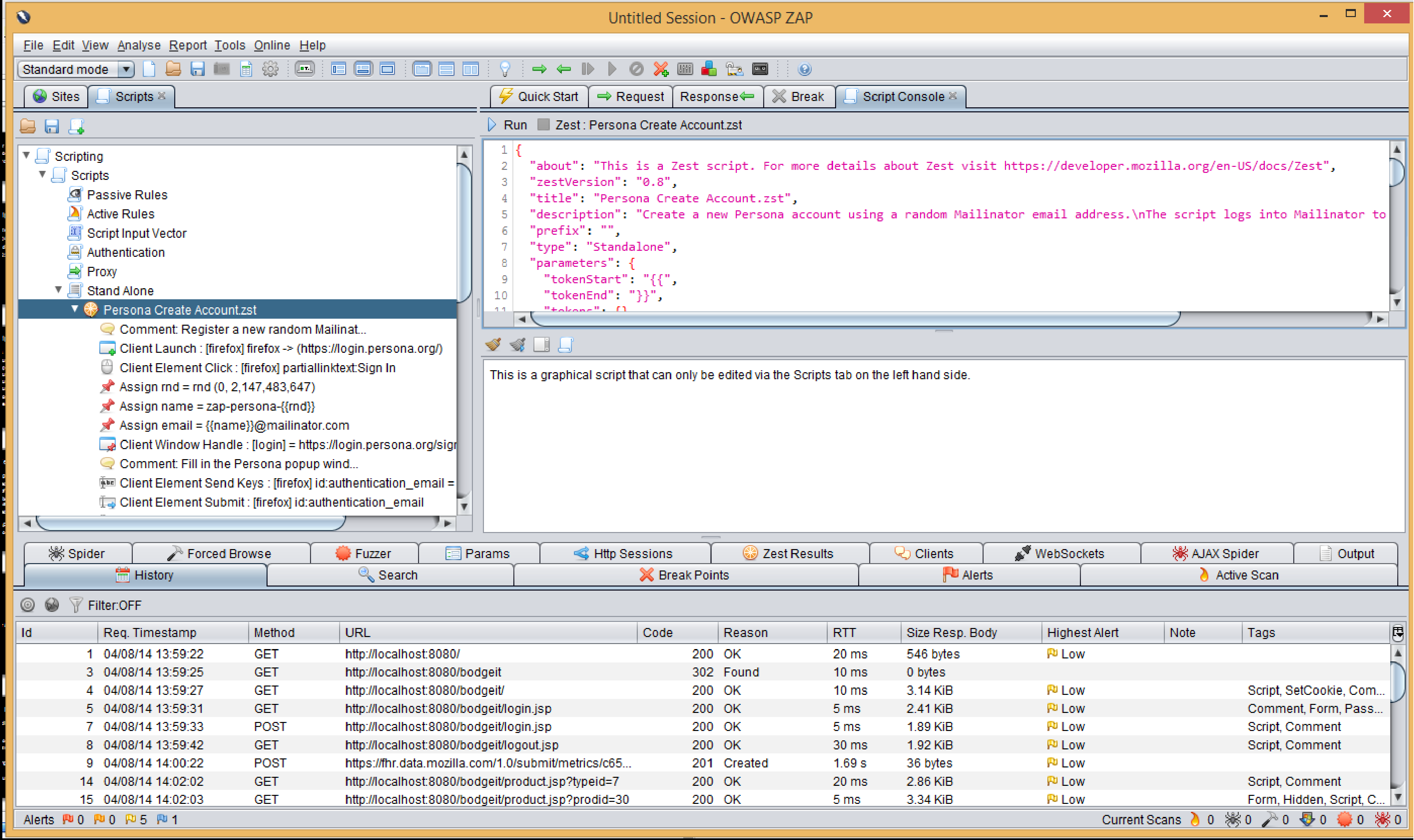
– Stand alone	Run when you say
– Targeted	Specify URLs to run against
– Active	Run in Active scanner
– Passive	Run in Passive scanner
– Proxy	Run 'inline'
– Authentication	Complex logins
– Input Vector	Define what to attack

Zest

- An experimental scripting language
- Developed by Mozilla Security Team
- Free and open source (of course)
- Tool independent – can be used in open and closed, free or commercial software
- Format: JSON – designed to be represented visually in security tools
- Included by default in ZAP from 2.2.0
- ZAP's macro language (on steroids)

Zest use cases

- Reporting vulnerabilities to companies
- Reporting vulnerabilities to developers
- Defining tool independent active and passive scan rules
- Deep integration with security tools



Untitled Session - OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Scripts
Quick Start
Request
Response
Break
Script Console
Run
Zest : Persona Create Account.zst

Scripting
- Scripts
  - Passive Rules
  - Active Rules
  - Script Input Vector
  - Authentication
  - Proxy
  - Stand Alone
    - Persona Create Account.zst
      - Comment: Register a new random Mailinat...
      - Client Launch : [firefox] firefox -> (https://login.persona.org/)
      - Client Element Click : [firefox] partiallinktext:Sign In
      - Assign rnd = rnd (0, 2,147,483,647)
      - Assign name = zap-persona-{{rnd}}
      - Assign email = {{name}}@mailinator.com
      - Client Window Handle : [login] = https://login.persona.org/sign
      - Comment: Fill in the Persona popup wind...
      - Client Element Send Keys : [firefox] id:authentication_email =
      - Client Element Submit : [firefox] id:authentication_email

```
{
  "about": "This is a Zest script. For more details about Zest visit https://developer.mozilla.org/en-US/docs/Zest",
  "zestVersion": "0.8",
  "title": "Persona Create Account.zst",
  "description": "Create a new Persona account using a random Mailinator email address.\nThe script logs into Mailinator to
  "prefix": "",
  "type": "Standalone",
  "parameters": {
    "tokenStart": "{{",
    "tokenEnd": "}}",
```

This is a graphical script that can only be edited via the Scripts tab on the left hand side.

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	04/08/14 13:59:22	GET	http://localhost:8080/	200	OK	20 ms	546 bytes	Low		
3	04/08/14 13:59:25	GET	http://localhost:8080/bodgeit	302	Found	10 ms	0 bytes			
4	04/08/14 13:59:27	GET	http://localhost:8080/bodgeit/	200	OK	10 ms	3.14 KiB	Low		Script, SetCookie, Com...
5	04/08/14 13:59:31	GET	http://localhost:8080/bodgeit/login.jsp	200	OK	5 ms	2.41 KiB	Low		Comment, Form, Pass...
7	04/08/14 13:59:33	POST	http://localhost:8080/bodgeit/login.jsp	200	OK	5 ms	1.89 KiB	Low		Script, Comment
8	04/08/14 13:59:42	GET	http://localhost:8080/bodgeit/logout.jsp	200	OK	30 ms	1.92 KiB	Low		Script, Comment
9	04/08/14 14:00:22	POST	https://fhr.data.mozilla.com/1.0/submit/metrics/c65...	201	Created	1.69 s	36 bytes	Low		
14	04/08/14 14:02:02	GET	http://localhost:8080/bodgeit/product.jsp?typeid=7	200	OK	20 ms	2.86 KiB	Low		Script, Comment
15	04/08/14 14:02:03	GET	http://localhost:8080/bodgeit/product.jsp?prodid=30	200	OK	5 ms	3.34 KiB	Low		Form, Hidden, Script, C...

Work in progress

- Zest client side recording
- Sequence scanning
- Google Summer of Code projects:
  - Advanced access control testing
  - Advanced fuzzing
  - SOAP service scanning
  - Firefox Zest add-on
- Mozilla Winter of Security projects:
  - Scripted extensions
  - AMF support

Conclusion

- ZAP is changing rapidly
- Its the most active O/S web appsec security tool
- Its great for people new to appsec ...
- … and also for security pros
- If you dont know its capabilities, how can you know you're using the most appropriate tool?
- Its a community based tool – get involved
- Come over to the stand to learn more :)

Thank you!

OWASP ZAP

ToolsWatch.org top security tool of 2013

For more info and demos:

Breakers JK – Station 1

12:45 – 15:15