An Introduction to ZAP

OWASP

Zed Attack Proxy

Simon Bennetts

OWASP ZAP Project Lead

Mozilla Security Team

psiinon@gmail.com

What is ZAP?

- An easy to use webapp pentest tool
- Completely free and open source
- An OWASP flagship project
- Ideal for beginners
- But also used by professionals
- Ideal for devs, esp. for automated security tests
- Becoming a framework for advanced testing

ZAP Principles

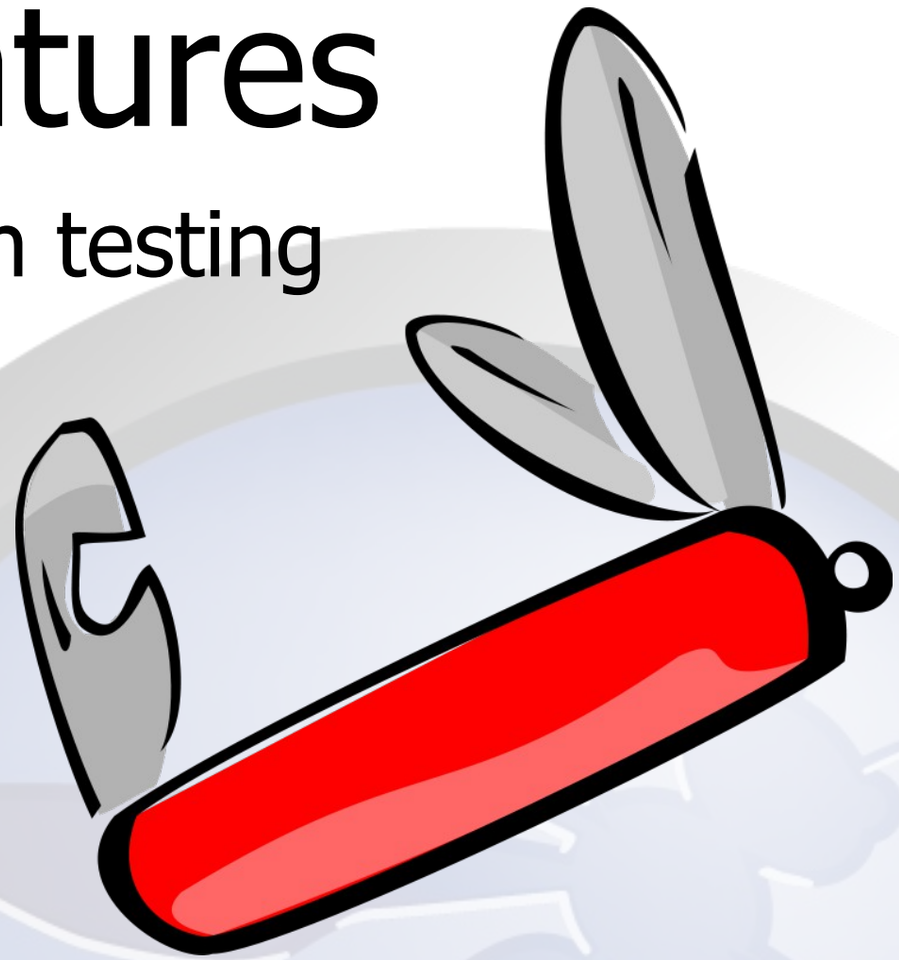
- Free, Open source
- Involvement actively encouraged
- Cross platform
- Easy to use
- Easy to install
- Internationalized
- Fully documented
- Work well with other tools
- Reuse well regarded components

Statistics

- Released September 2010, fork of Paros
- V 1.4.0 downloaded 19,000 times
- V 1.4.1 released in August
- Fully internationalized
- Translated into 11 languages
- Mostly used by Professional Pentesters?
- Paros code: ~30% ZAP Code: ~70%

The Main Features

All the essentials for web application testing



- Intercepting Proxy
- Active and Passive Scanners
- Spider
- Report Generation
- Brute Force (using OWASP DirBuster code)
- Fuzzing (using fuzzdb & OWASP JBroFuzz)
- Extensibility

The Additional Features

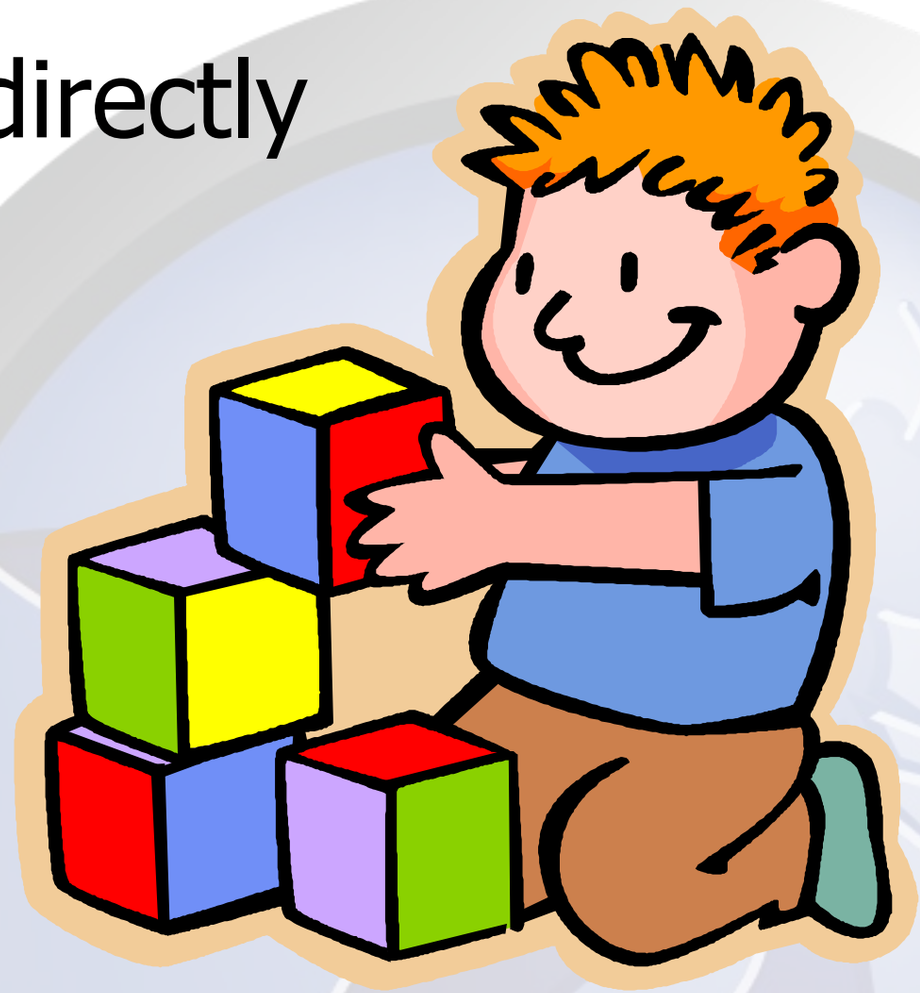
- Auto tagging
- Port scanner
- Smart card support
- Session comparison
- Invoke external apps
- BeanShell integration
- API + Headless mode
- Dynamic SSL Certificates
- Anti CSRF token handling

New in Version 1.4

- Syntax highlighting
- Fuzzdb integration
- Parameter analysis
- Enhanced XSS scanner
- Plugable extensions
- Reveal hidden fields
- Some of the Watcher checks
- Lots of bug fixes!

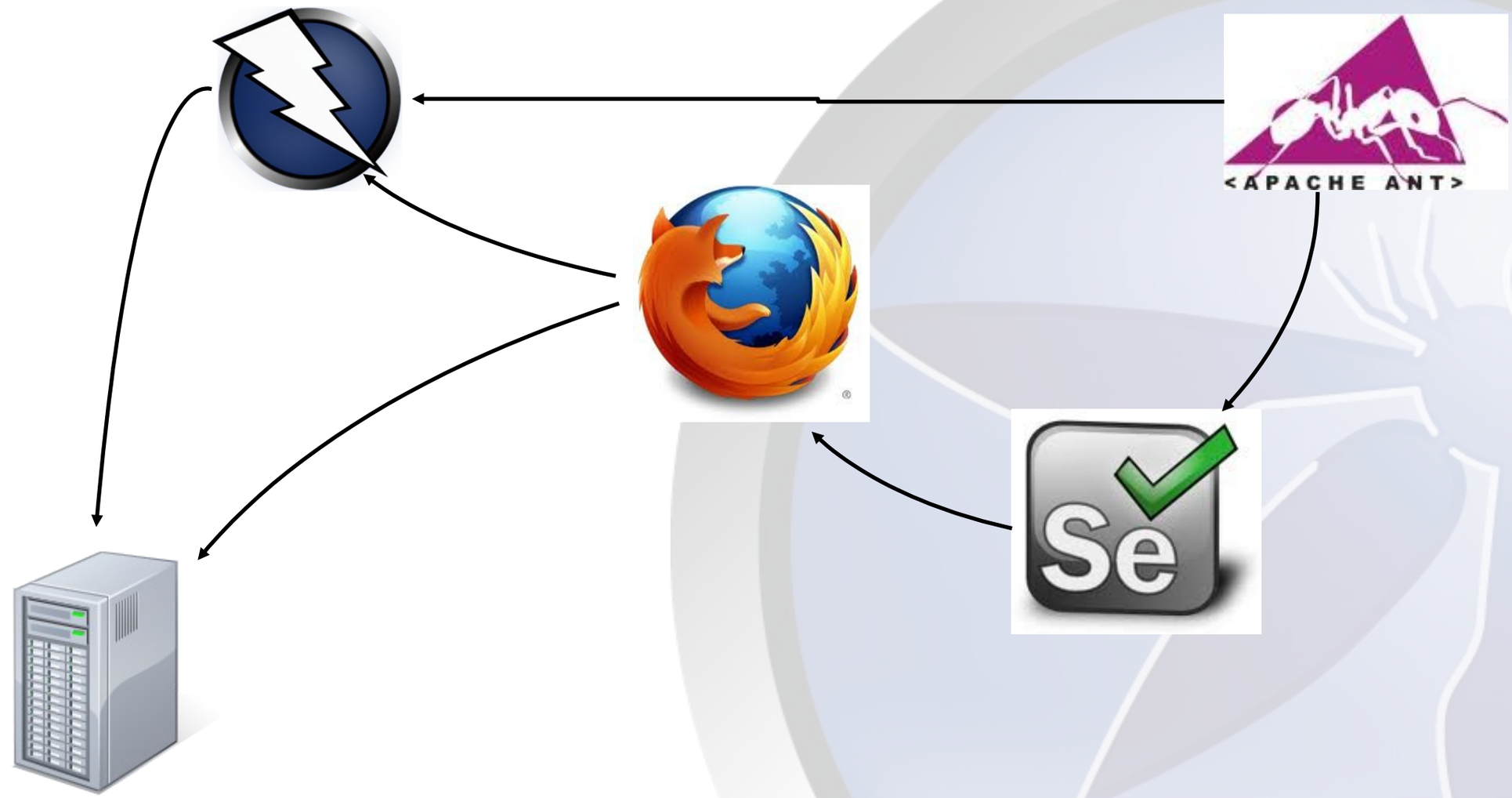
Extending ZAP

- Invoking applications directly
- REST API
- Filters
- Active Scan Rules
- Passive Scan Rules
- Full Extensions



https://code.google.com/p/zap-extensions/

Security Regression Tests



http://code.google.com/p/zaproxy/wiki/SecRegTests

Collaborations

- Dradis – ZAP upload plugin
- OWASP ModSecurity Core Rule Set script – SpiderLabs
- ThreadFix – Denim Group
- Ultimate Obsolete File Detection – Hacktics ASC, Ernst & Young
- Grey-box plugin – BCC Risk Advisory

ZAP 2.0

- New Spider plus Session awareness
  Cosmin Stefan

Untitled Session - OWASP ZAP

File Edit View Analyse Report Tools Help

Standard mode

Sites

Request Response Break

Header: Text Body: Text

```
GET http://localhost:8080/bodgeit HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Proxy-Connection: keep-alive
Referer: http://localhost:8080/bodgeit/search.jsp?q=rdsred
Cookie: JSESSIONID=5F7B6BCB5B8B50C3A01F24B222E10D5E; b_id=3
Content-length: 0
```

- Sites
  - http://localhost:8080
    - bodgeit
      - GET:home.jsp
      - GET:product.jsp(typeid)
      - GET:product.jsp(prodid)
      - POST:basket.jsp(price,productid,quan
      - GET:search.jsp
      - GET:search.jsp(q)
      - GET:basket.jsp
      - POST:basket.jsp(quantity_10,quantity_
      - GET:login.jsp
      - POST:login.jsp(password,username)
      - GET:logout.jsp
      - GET:contact.jsp
      - POST:contact.jsp(anticsrf,comments,r
      - GET:about.jsp
      - GET:advanced.jsp
      - GET:admin.jsp
      - POST:basket.jsp(update)
      - POST:advanced.jsp(description,pri
    - images
    - js

History Search Break Points Alerts Active Scan Spider Brute Force Port Scan Fuzzer Params Http Sessions WebSockets Output

Site: localhost:8080 New Session

Active	Name	Session Tokens' Values	Messages Matched
	Session 0	jsessionid=C8EF59FB5A94A6ED4427CE465F8A42DD	1
	Session 1	jsessionid=5F7B6BCB5B8B50C3A01F24B222E10D5E	25
	Session 2	jsessionid=BCBF99565EEAD8628F20BE6FEB614AAB	4
✔	Session 3	jsessionid=6A35F3FD2E3FC02D3141F130207FA274	70

Alerts 0 1 3 1 Current Scans 6 0 0 0 0 0

- New Spider plus Session awareness
  Cosmin Stefan

- New Spider plus Session awareness
  Cosmin Stefan
- Ajax Spider via Crawljax
  Guifre Ruiz

Mozilla Firefox

http://caos.uab....uiz/test/wivet/

caos.uab.es/~gruiz/test/wivet/

Google

WIVET - Web Input Vector Extractor Teaser v2
Bedirhan Urgun, urgunb at hotmail dot com, <www.webguvenligi.org>

Coverage : **%72**
Started at : **2012 08 08 12:34:27**
Details :

purple rows indicate missed cases, other rows indicate hit.

URI	Description	Number of Accesses	IP Address	User Agent
1_2.php	link creation after button click	1	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
2_1.php	self referencing link	2	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
4_1.php	link href js protocol	1	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
5_1.php	div onmouseover window.open	1	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
6_1.php	form submit thru select onchange w/ simple alert	1	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
7_1.php	form submit button onclick	1	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
9_13.php	td onclick window.location.href	1	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
9_15.php	td onmousedown window.location.href	1	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
9_16.php	td onmouseup window.location.href	1	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
9_17.php	tr onclick window.location.href	2	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101 Firefox/14.0.1
9_19.php	tr onmousedown window.location.href	2	2.137.83.245	Mozilla/5.0 (Macintosh; I ... o/20100101

WebDriver

- New Spider plus Session awareness
  Cosmin Stefan
- Ajax Spider via Crawljax
  Guifre Ruiz

- New Spider plus Session awareness
  Cosmin Stefan
- Ajax Spider via Crawljax
  Guifre Ruiz
- WebSockets support
  Robert Kock

Untitled Session - OWASP ZAP

File Edit View Analyse Report Tools Help

Standard mode

Sites

- Sites
  - http://178.79.166.11
  - http://178.79.178.215
  - http://browserquest.mozilla.org
    - css
    - img
    - js
  - http://cdn.mozilla.net
    - browserquest
      - audio
        - music
        - sounds
      - fonts
        - GET:graphicpixel-webfont.woff
        - GET:advocut-webfont.woff
      - img
        - 1
        - 3
      - maps
        - GET:world_client.js
  - http://statse.webtrendslive.com

Request | Response | Break

Text | #2.25 - 29/08/12 12:31:47.83 - TEXT

[[2,929,61,19,233],[2,11920,2,38,237,4],[2,11921,2,38,237,3],[2,12120,2,25,235,2],[2,12121,2,24,235,1],[2,810235,42,10,235]]

Filter WebSocket messages

Select the required filters below. You can select multiple rows in each element. An element is not used for filtering if none of the rows in it are selected

Opcode:
- -- All Opcodes --
- TEXT
- BINARY
- CLOSE
- PING
- PONG

Direction: [x] Outgoing Messages [x] Incoming Messages

Cancel | Clear | Apply

History | Search | Break Points | Alerts | Active Scan | Spider | Brute Force | Port Scan | Fuzzer | Params | Http Sessions | WebSockets | Output

Channel: -- All Channels -- | Filter:OFF

Channel	↔	Timestamp	Opcode	Bytes	Payload
#2.19	→	29/08/12 12:31:42.841	1=TEXT	11	[12,997378]
#2.20	→	29/08/12 12:31:44.465	1=TEXT	10	[4,21,214]
#2.21	→	29/08/12 12:31:46.583	1=TEXT	10	[4,20,217]
#2.22	→	29/08/12 12:31:46.976	1=TEXT	4	[21]
#2.23	←	29/08/12 12:31:47.22	1=TEXT	122	[[19,927,929,1020,1021,1120,1121,1122,1220,1221,1222,1320,1321,1322,11920,11921,12120,12121,810235,815222,818209,5704799]]
#2.24	→	29/08/12 12:31:47.41	1=TEXT	39	[20,929,11920,11921,12120,12121,810235]
#2.25	←	29/08/12 12:31:47.83	1=TEXT	124	[[2,929,61,19,233],[2,11920,2,38,237,4],[2,11921,2,38,237,3],[2,12120,2,25,235,2],[2,12121,2,24,235,1],[2,810235,42,10,235]]
#2.26	→	29/08/12 12:31:50.599	1=TEXT	10	[4,16,222]
#2.27	←	29/08/12 12:31:52.986	1=TEXT	12	[[17,22,22]]
#2.28	←	29/08/12 12:31:55.503	1=TEXT	12	[[17,21,21]]

Alerts 0 1 2 1 | Current Scans 0 0 0 0 0 0

- New Spider plus Session awareness
  Cosmin Stefan
- Ajax Spider via Crawljax
  Guifre Ruiz
- WebSockets support
  Robert Kock

All now available in the Weekly Releases!

MORE planned 2.0 features

- 5 Session Scope
- 5 Modes

Untitled Session - OWASP ZAP

File Edit View Analyse Report Tools Help

Standard mode

Sites | Request | Response | Break | Script Console

Header: Text | Body: Text

```
GET http://localhost:8080/bodgeit HTTP/1.1
Host: localhost:8080
Use
Acc
Acc
Pro
Ref
Coo
Con
```

- Sites
  - http://localhost:8080
    - bodgeit
      - GET:home.jsp
      - GET:product.jsp(typeid)
      - GET:about.jsp
      - GET:contact.jsp
      - GET:logout.jsp
      - GET:basket.jsp
      - GET:search.jsp
      - GET:advanced.jsp
      - js
        - GET:encryption.js
    - GET:wivet
    - wavsep
      - GET:index-active.jsp
    - wivet
      - GET:header.php
      - GET:style.css
      - GET:body.php
      - GET:menu.php
      - innerpages
      - offscanpages
      - pages

Session Properties

- Session
  - General
  - Include in Scope
  - Exclude from Scope
  - Exclude from proxy
  - Exclude from scanner
  - Exclude from spider
  - Exclude from WebSockets
  - Authentication

Include in Scope

URLs which will be included in the scope unless also excluded

URL regexs
\Qhttp://localhost:8080/bodgeit\E.*

OK | Cancel

History | Search | Break Points | Alerts | Ac | Sockets | Output

Filter:OFF

1	GET	http://localhost:8080/bodgeit/home.jsp				
4	GET	http://localhost:8080/bodgeit/product.jsp?typeid=6				
5	GET	http://localhost:8080/bodgeit/product.jsp?typeid=2				
6	GET	http://localhost:8080/bodgeit/product.jsp?typeid=4	200	OK	5ms	Script, Comment
7	GET	http://localhost:8080/bodgeit/about.jsp	200	OK	10ms	Script, Comment
8	GET	http://localhost:8080/bodgeit/contact.jsp	200	OK	8ms	Form, Hidden, Script, Comment, AntiCSRF
9	GET	http://localhost:8080/bodgeit/logout.jsp	200	OK	6ms	Script, Comment
10	GET	http://localhost:8080/bodgeit/basket.jsp	200	OK	8ms	Form, Script, SetCookie, Comment
11	GET	http://localhost:8080/bodgeit/search.jsp	200	OK	5ms	Form, Script, Comment
12	GET	http://localhost:8080/bodgeit/advanced.jsp	200	OK	4ms	Form, Hidden, Script, Comment
13	GET	http://localhost:8080/bodgeit/js/encryption.js	200	OK	129ms	Comment

Alerts 0 2 2 1 | Current Scans 0 0 0 0 0 0

MORE planned 2.0 features

- Session Scope
- Modes
- Script Console

savesession - bodgeit-2012-05-31-11-40-51 - OWASP ZAP

File Edit View Analyse Report Tools Help

Sites

- Sites
  - http://localhost:8080
    - bodgeit
      - GET:bodgeit
      - GET:docs
      - GET:bodgeit(q)
    - docs
      - GET:examples
    - host-manager
    - manager

Request | Response | Break | Script Console

ECMAScript : Mozilla Rhino | Run

ECMAScript : Mozilla Rhino
Groovy : Groovy Scripting Engine
python : jython
ruby : JSR 223 JRuby Engine

```
5 hr = org.parosproxy.paros.control.Control.getSingleton().getExtensionLoader().getExtension("ExtensionHistory")
6     .getHistoryList().getHistoryReference(13)
7
8 if (hr) {
9     print("Got " + hr.getHttpMessage().getRequestHeader().getURI())
10 }
```

Got http://localhost:8080/bodgeit/home.jsp

History | Search | Break Points | Alerts | Active Scan | Spider | Brute Force | Port Scan | Fuzzer | Params | Output

Filter:OFF

1	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	35ms		Script, SetCookie, Comment
4	GET	http://localhost:8080/bodgeit/js/util.js	200	OK	55ms		Upload
5	GET	http://localhost:8080/bodgeit/style.css	200	OK	55ms		
8	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	15ms		Script, Comment
9	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	10ms		Script, Comment
10	GET	http://localhost:8080/bodgeit/about.jsp	200	OK	30ms		Script, Comment
11	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	5ms		Script, Comment
12	GET	http://localhost:8080/bodgeit/contact.jsp	200	OK	95ms		Form, Hidden, Script, Comment, AntiCSRF
13	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	10ms		Script, Comment
14	GET	http://localhost:8080/bodgeit/login.jsp	200	OK	50ms		Form, Password, Script, Comment
15	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	10ms		Script, Comment
16	GET	http://localhost:8080/bodgeit/basket.jsp	200	OK	75ms		Form, Script, SetCookie, Comment

Alerts 1 2 3 1 | Current Scans 0 0 0 0 0

MORE planned 2.0 features

- Session Scope
- Modes
- Script Console
- Authentication management

Untitled Session - auth - OWASP ZAP

File Edit View Analyse Report Tools Help

Standard mode

Sites

Request Response Break

Header: Text Body: Text

```
GET http://localhost:8080/bodgeit HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

- Sites
  - http://localhost:8080
    - bodgeit
      - GET:home.jsp
      - GET:login.jsp
      - GET:register.jsp
      - POST:register.jsp(password1,password2
      - GET:logout.jsp
      - POST:login.jsp(password,username
      - GET:product.jsp(typeid)
      - GET:about.jsp
      - GET:contact.jsp
      - POST:contact.jsp(anticsrf,comments,null
      - GET:basket.jsp
      - POST:basket.jsp(update)
      - GET:search.jsp
      - GET:search.jsp(q)
  - http://safebrowsing-cache.google.com
  - http://safebrowsing.clients.google.com

Session Properties

- Session
  - General
  - Include in Scope
  - Exclude from Scope
  - Exclude from proxy
  - Exclude from scanner
  - Exclude from spider
  - Exclude from WebSockets
  - Authentication

Authentication

Login URL: http://localhost:8080/bodgeit/login.jsp

Login POST data: username=test%40test.com&password=tester

Logged in indicator regex:

Logout URL: http://localhost:8080/bodgeit/logout.jsp

Logout POST data:

Logged out indicator regex: Login

OK Cancel

History Search Break Points Alerts ebSockets Output

Filter:OFF

1	GET	http://localhost:8080/bodgeit/home.jsp				okie, Comment
4	GET	http://localhost:8080/bodgeit/login.jsp				vord, Script, Comment
5	GET	http://localhost:8080/bodgeit/register.jsp				vord, Script, Comment
6	POST	http://localhost:8080/bodgeit/register.jsp				okie, Comment
7	GET	http://localhost:8080/bodgeit/logout.jsp				nent
8	GET	http://localhost:8080/bodgeit/login.jsp				vord, Script, Comment
9	POST	http://localhost:8080/bodgeit/login.jsp	200	OK	7ms	Script, Comment
10	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	15ms	Comment, Script
11	GET	http://localhost:8080/bodgeit/product.jsp?typeid=2	200	OK	38ms	Comment, Script
12	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	71ms	Comment, Script
13	GET	http://localhost:8080/bodgeit/logout.jsp	200	OK	9ms	Comment, Script
14	GET	http://localhost:8080/bodgeit/home.jsp	200	OK	44ms	Script, Comment

Alerts 0 2 3 1 Current Scans 0 0 0 0 0 0

MORE planned 2.0 features

- Session Scope
- Modes
- Script Console
- Authentication management
- New / updated scanner rules
- Extension Marketplace?
- Full Scripting support?
- Configurable actions?

Any Questions?

http://www.owasp.org/index.php/ZAP