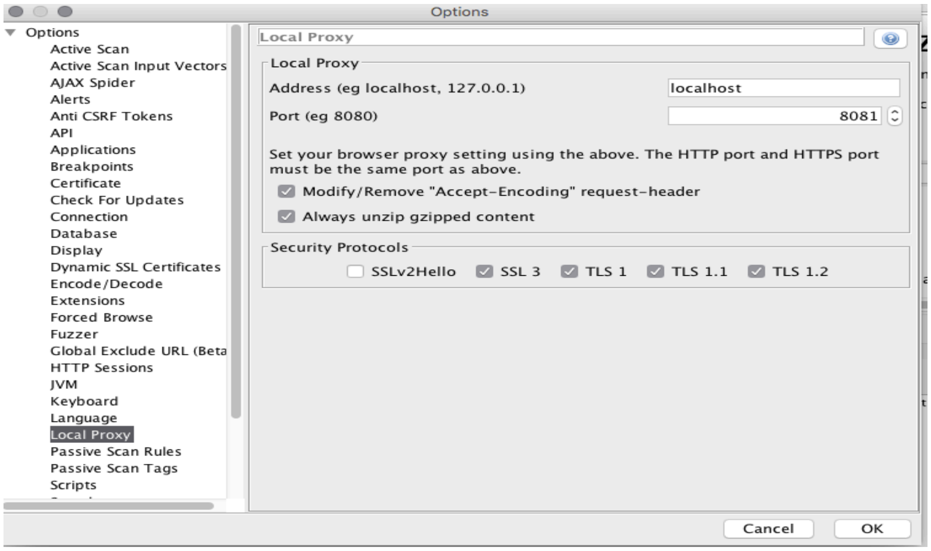
Questions and Solutions as screenshots : OWASP ZAP

1. Setting ZAP as an Intercepting proxy server :

In options menu on home page of application, in local proxy, port number can be changed for the proxy.



Local Proxy

Local Proxy

Address (eg localhost, 127.0.0.1) localhost

Port (eg 8080) 8081

Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.

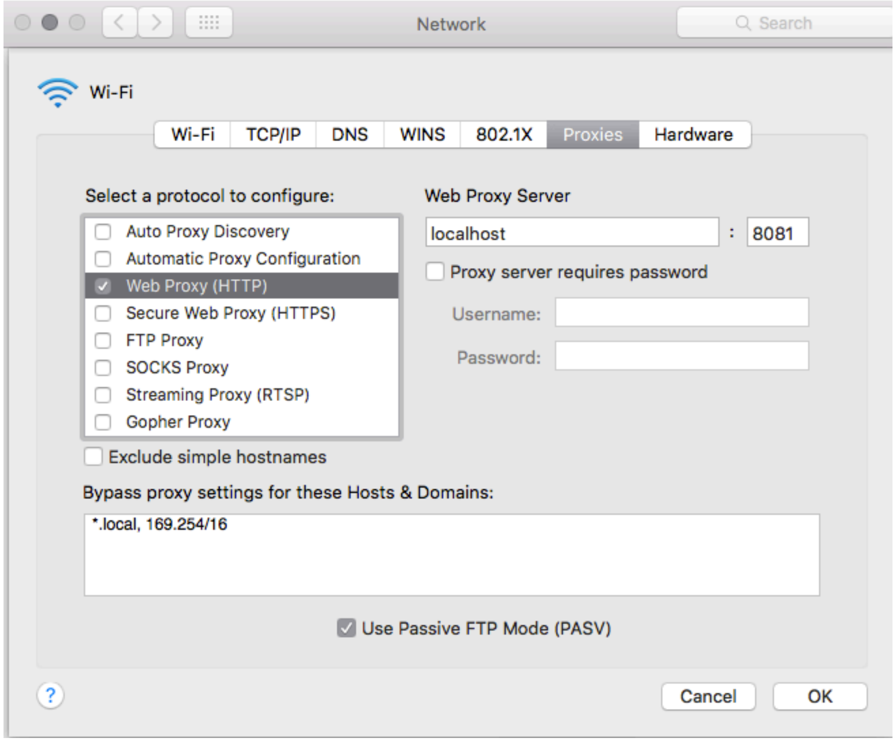
☑ Modify/Remove "Accept-Encoding" request-header

☑ Always unzip gzipped content

Security Protocols

□ SSLv2Hello ☑ SSL 3 ☑ TLS 1 ☑ TLS 1.1 ☑ TLS 1.2

In network setting of browser, proxy should be enabled.



Select a protocol to configure:

□ Auto Proxy Discovery
□ Automatic Proxy Configuration
☑ Web Proxy (HTTP)
□ Secure Web Proxy (HTTPS)
□ FTP Proxy
□ SOCKS Proxy
□ Streaming Proxy (RTSP)
□ Gopher Proxy

Web Proxy Server

localhost : 8081

□ Proxy server requires password

Username:

Password:

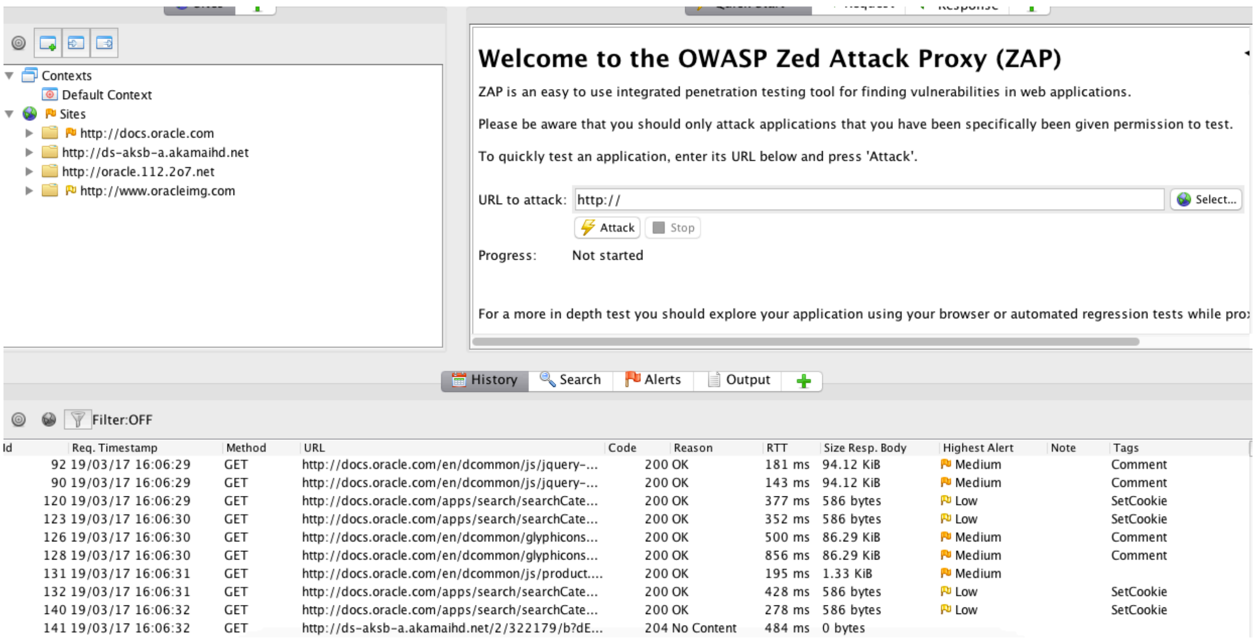
□ Exclude simple hostnames

Bypass proxy settings for these Hosts & Domains:

*.local, 169.254/16

☑ Use Passive FTP Mode (PASV)

In the history tab, all the requests, responses can be seen when requests are made through the browser then and the application acts as a proxy listening and recording all the requests. Also, alerts and tags like cookies can be seen.



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

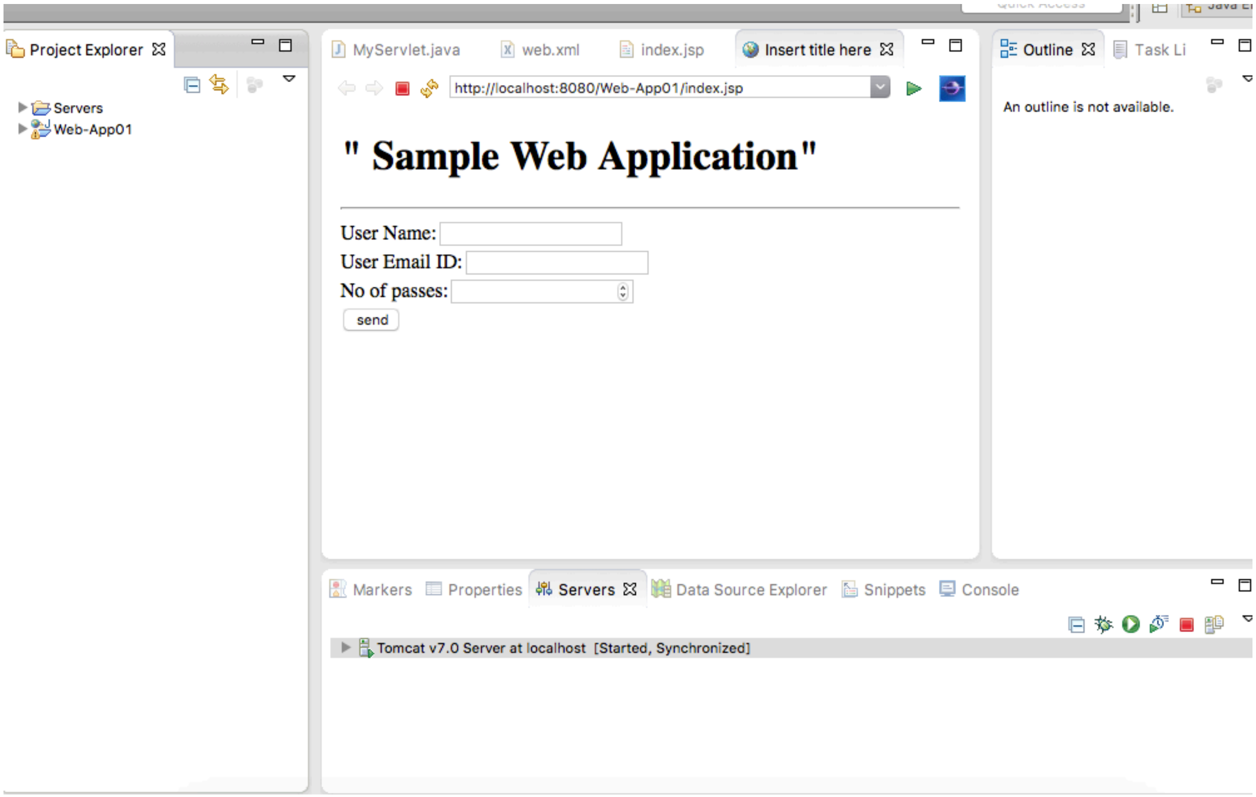
To quickly test an application, enter its URL below and press 'Attack'.

Progress: Not started

For a more in depth test you should explore your application using your browser or automated regression tests while pro

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
92	19/03/17 16:06:29	GET	http://docs.oracle.com/en/dcommon/js/jquery-...	200	OK	181 ms	94.12 KiB	Medium		Comment
90	19/03/17 16:06:29	GET	http://docs.oracle.com/en/dcommon/js/jquery-...	200	OK	143 ms	94.12 KiB	Medium		Comment
120	19/03/17 16:06:29	GET	http://docs.oracle.com/apps/search/searchCate...	200	OK	377 ms	586 bytes	Low		SetCookie
123	19/03/17 16:06:30	GET	http://docs.oracle.com/apps/search/searchCate...	200	OK	352 ms	586 bytes	Low		SetCookie
126	19/03/17 16:06:30	GET	http://docs.oracle.com/en/dcommon/glyphicons...	200	OK	500 ms	86.29 KiB	Medium		Comment
128	19/03/17 16:06:30	GET	http://docs.oracle.com/en/dcommon/glyphicons...	200	OK	856 ms	86.29 KiB	Medium		Comment
131	19/03/17 16:06:31	GET	http://docs.oracle.com/en/dcommon/js/product....	200	OK	195 ms	1.33 KiB	Medium		
132	19/03/17 16:06:31	GET	http://docs.oracle.com/apps/search/searchCate...	200	OK	428 ms	586 bytes	Low		SetCookie
140	19/03/17 16:06:32	GET	http://docs.oracle.com/apps/search/searchCate...	200	OK	278 ms	586 bytes	Low		SetCookie
141	19/03/17 16:06:32	GET	http://ds-aksb-a.akamaihd.net/2/322179/b?dE...	204	No Content	484 ms	0 bytes			

To crawl a website or launch active attacks, a sample web application was created. This web application runs on jetty and is a simple user form



http://localhost:8080/Web-App01/index.jsp

" Sample Web Application"

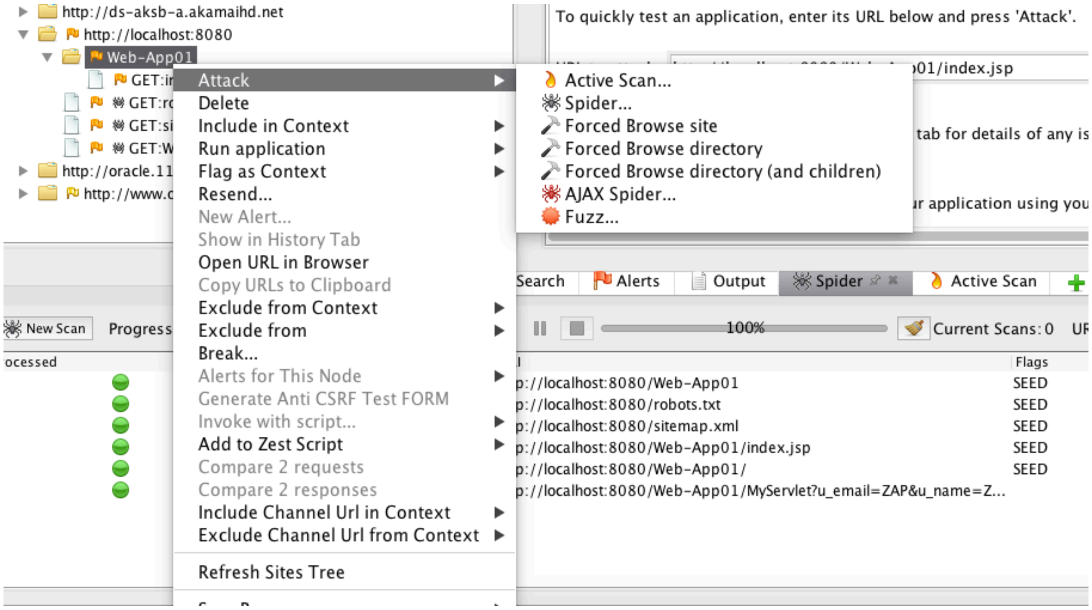
User Name:
User Email ID:
No of passes:

An outline is not available.

Tomcat v7.0 Server at localhost [Started, Synchronized]

2. Crawling your web application :

Spider option is now selected after right clicking the web application, which crawls the website and displays results



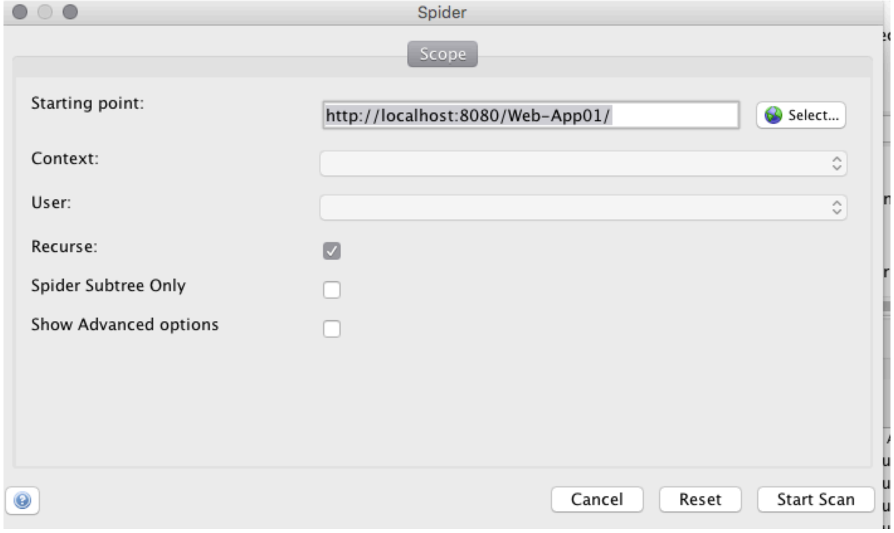
To quickly test an application, enter its URL below and press 'Attack'.

)01/index.jsp

tab for details of any is

ır application using you

```
ocessed                                                    Flags
         p://localhost:8080/Web-App01                        SEED
         p://localhost:8080/robots.txt                       SEED
         p://localhost:8080/sitemap.xml                      SEED
         p://localhost:8080/Web-App01/index.jsp              SEED
         p://localhost:8080/Web-App01/                       SEED
         p://localhost:8080/Web-App01/MyServlet?u_email=ZAP&u_name=Z...
```



Starting point: http://localhost:8080/Web-App01/

Context:

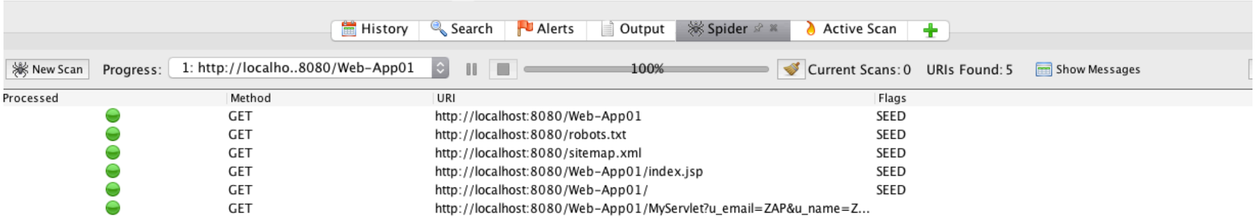
User:

Recurse: ☑

Spider Subtree Only ☐

Show Advanced options ☐

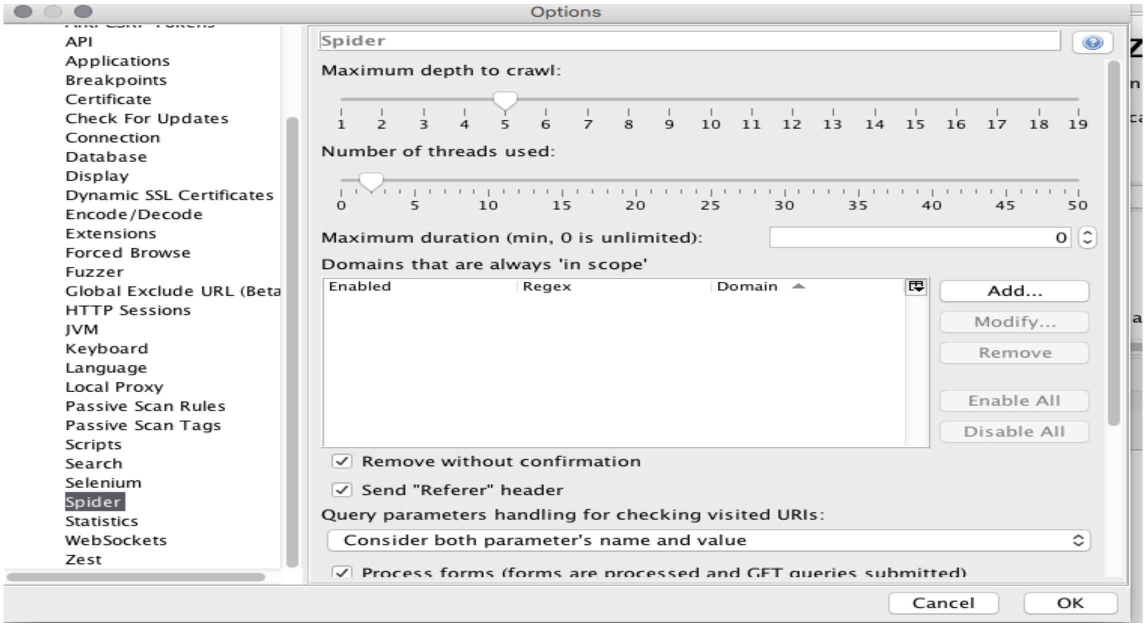
These are the results obtained after crawling :



Progress: 1: http://localho..8080/Web-App01 100% Current Scans: 0 URIs Found: 5

Processed	Method	URI	Flags
●	GET	http://localhost:8080/Web-App01	SEED
●	GET	http://localhost:8080/robots.txt	SEED
●	GET	http://localhost:8080/sitemap.xml	SEED
●	GET	http://localhost:8080/Web-App01/index.jsp	SEED
●	GET	http://localhost:8080/Web-App01/	SEED
●	GET	http://localhost:8080/Web-App01/MyServlet?u_email=ZAP&u_name=Z...	

Options for crawling like depth, threads can be set up in options menu :



Spider

Maximum depth to crawl: 5

Number of threads used:

Maximum duration (min, 0 is unlimited): 0

Domains that are always 'in scope'

Enabled	Regex	Domain

☑ Remove without confirmation

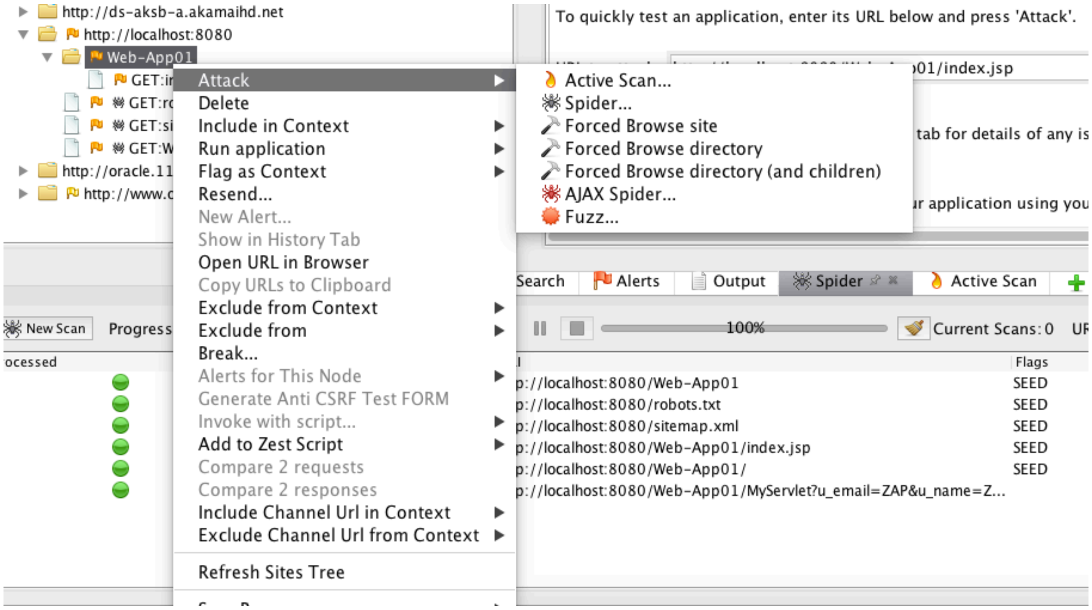
☑ Send "Referer" header

Query parameters handling for checking visited URIs: Consider both parameter's name and value

☑ Process forms (forms are processed and GET queries submitted)

3. Active attacks on web application to look for unhandled alerts:

Active scan will scan the web application and display possible alerts

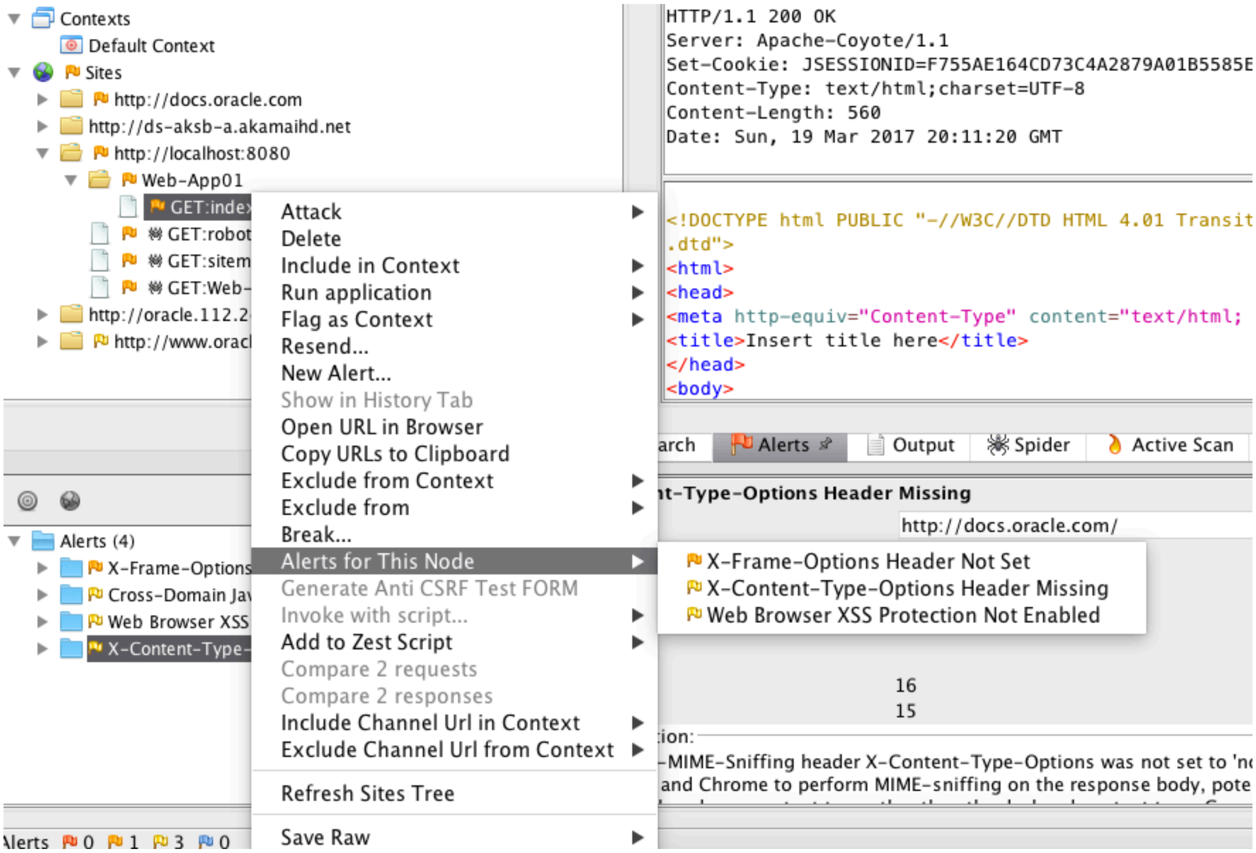


To quickly test an application, enter its URL below and press 'Attack'.

tab for details of any is

r application using you

	Flags
p://localhost:8080/Web-App01	SEED
p://localhost:8080/robots.txt	SEED
p://localhost:8080/sitemap.xml	SEED
p://localhost:8080/Web-App01/index.jsp	SEED
p://localhost:8080/Web-App01/	SEED
p://localhost:8080/Web-App01/MyServlet?u_email=ZAP&u_name=Z...	



```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F755AE164CD73C4A2879A01B5585E
Content-Type: text/html;charset=UTF-8
Content-Length: 560
Date: Sun, 19 Mar 2017 20:11:20 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transit
.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
<title>Insert title here</title>
</head>
<body>
```

nt-Type-Options Header Missing

http://docs.oracle.com/

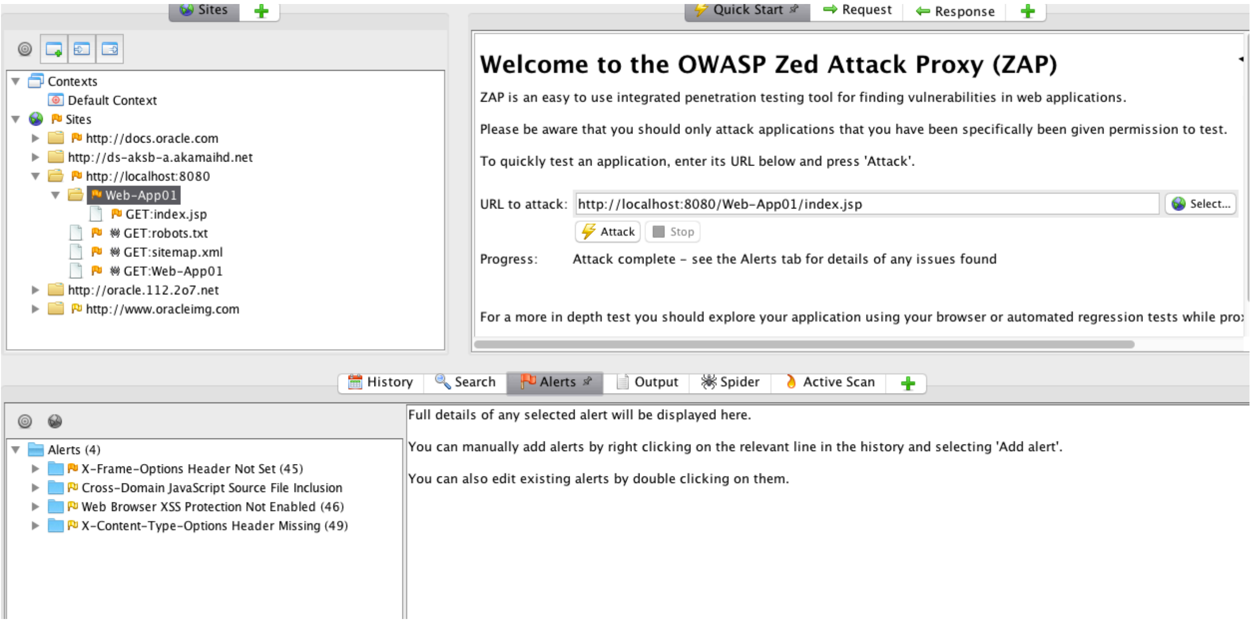
16

15

ion:

-MIME-Sniffing header X-Content-Type-Options was not set to 'nc
and Chrome to perform MIME-sniffing on the response body, pote

As explained in the slides, different alerts can be checked in bottom left corner :



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://localhost:8080/Web-App01/index.jsp

Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tests while pro

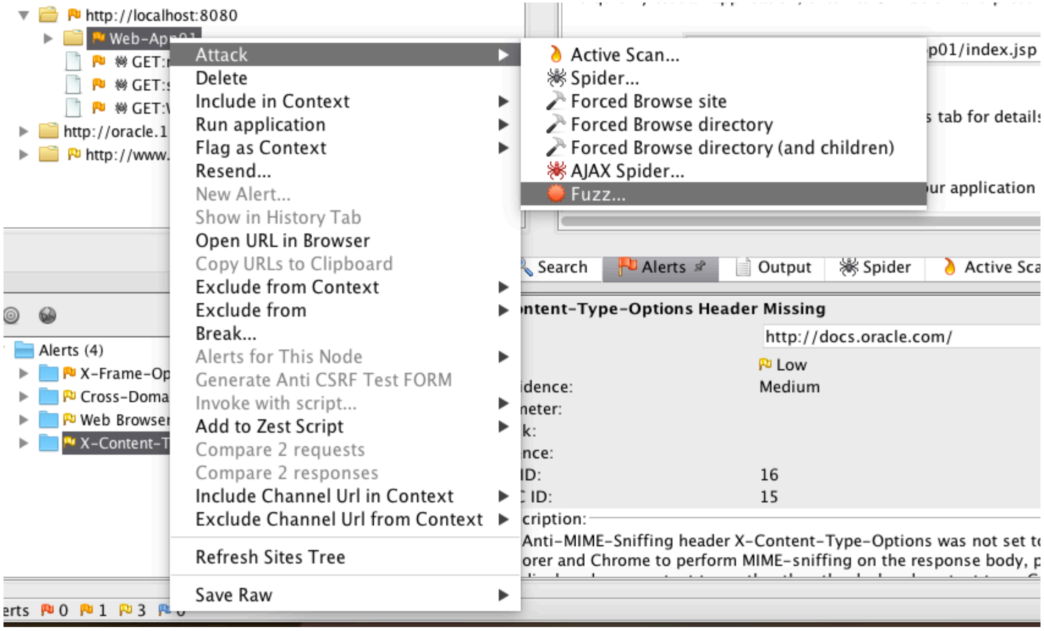
Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

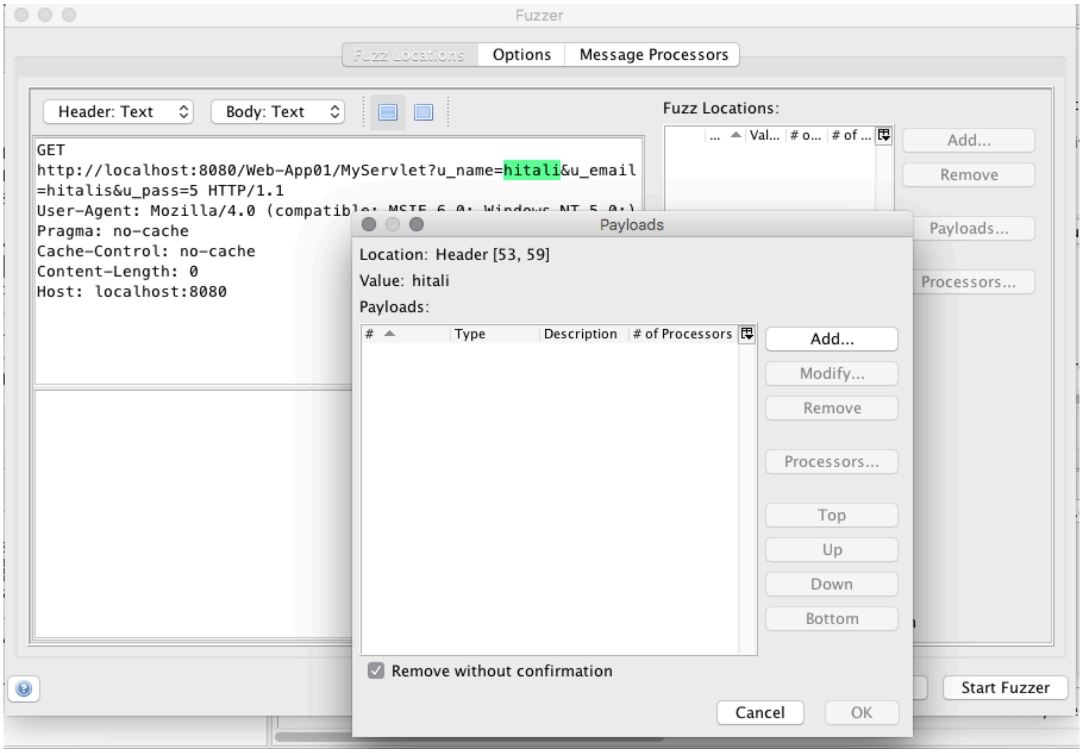
You can also edit existing alerts by double clicking on them.

4. Fuzz test web application for a specific parameter:

Select Fuzz testing for your web application



Then highlight the parameter, you want to fuzz test on, like in the below case it is username, and select add payload



```
GET
http://localhost:8080/Web-App01/MyServlet?u_name=hitali&u_email
=hitalis&u_pass=5 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: localhost:8080
```

Location: Header [53, 59]

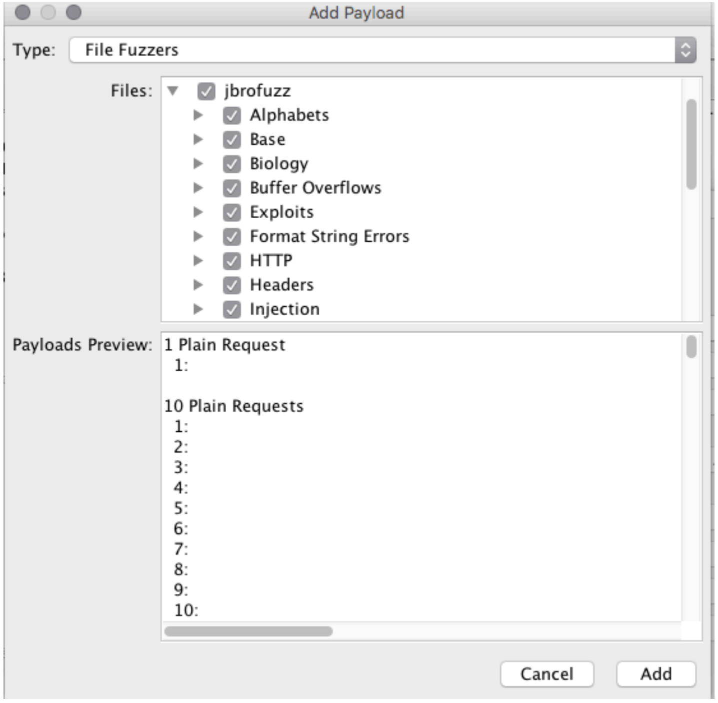
Value: hitali

Payloads:

#	Type	Description	# of Processors

☑ Remove without confirmation

Select file fuzzer and choose different fuzz testers available. You can choose all to perform extensive testing or just a few selected payloads



Type: File Fuzzers

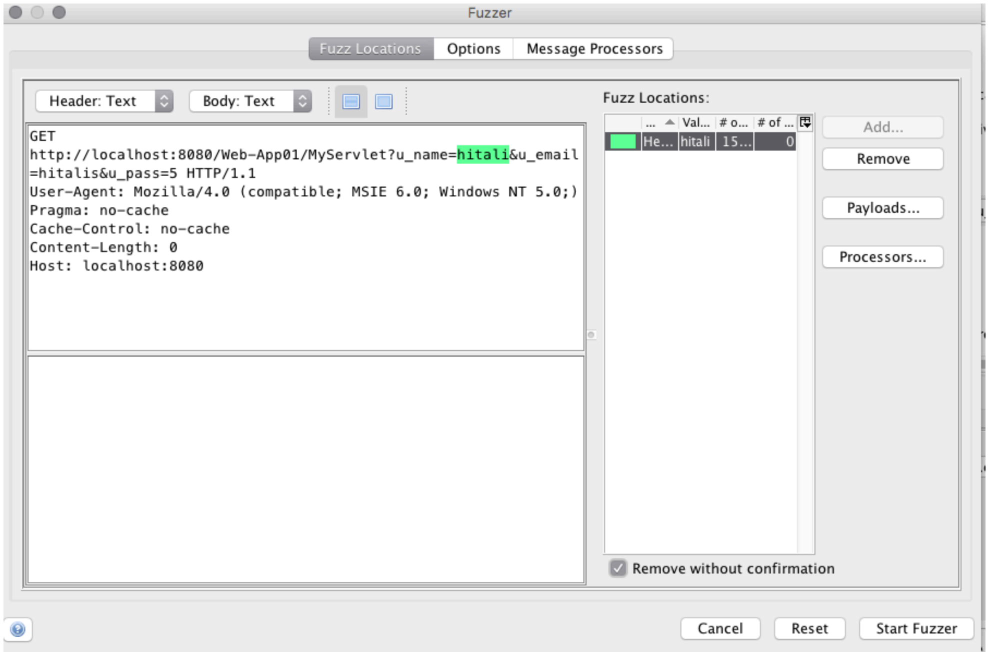
Files:

- ☑ jbrofuzz
  - ☑ Alphabets
  - ☑ Base
  - ☑ Biology
  - ☑ Buffer Overflows
  - ☑ Exploits
  - ☑ Format String Errors
  - ☑ HTTP
  - ☑ Headers
  - ☑ Injection

Payloads Preview:

```
1 Plain Request
  1:

10 Plain Requests
  1:
  2:
  3:
  4:
  5:
  6:
  7:
  8:
  9:
  10:
```

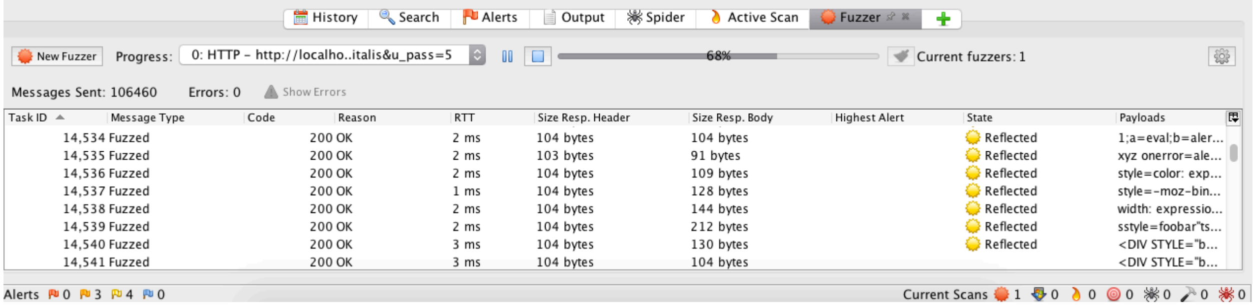


```
GET
http://localhost:8080/Web-App01/MyServlet?u_name=hitali&u_email
=hitalis&u_pass=5 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: localhost:8080
```

	...	Val...	# o...	# of ...
🟩	He...	hitali	15...	0

☑ Remove without confirmation

You can then see the results for different payloads. Requests and responses can be seen, and different payloads can thus be tested easily. Reflected state indicates that the response in correct, and that payload is handled by the application.



Progress: 0: HTTP – http://localho..italis&u_pass=5 68% Current fuzzers: 1

Messages Sent: 106460 Errors: 0

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
14,534	Fuzzed	200	OK	2 ms	104 bytes	104 bytes		Reflected	1;a=eval;b=aler...
14,535	Fuzzed	200	OK	2 ms	103 bytes	91 bytes		Reflected	xyz onerror=ale...
14,536	Fuzzed	200	OK	2 ms	104 bytes	109 bytes		Reflected	style=color: exp...
14,537	Fuzzed	200	OK	1 ms	104 bytes	128 bytes		Reflected	style=-moz-bin...
14,538	Fuzzed	200	OK	2 ms	104 bytes	144 bytes		Reflected	width: expressio...
14,539	Fuzzed	200	OK	2 ms	104 bytes	212 bytes		Reflected	sstyle=foobar"ts...
14,540	Fuzzed	200	OK	3 ms	104 bytes	130 bytes		Reflected	<DIV STYLE="b...
14,541	Fuzzed	200	OK	3 ms	104 bytes	104 bytes			<DIV STYLE="b...

Alerts 0 3 4 0 Current Scans 1 0 0 0 0 0 0