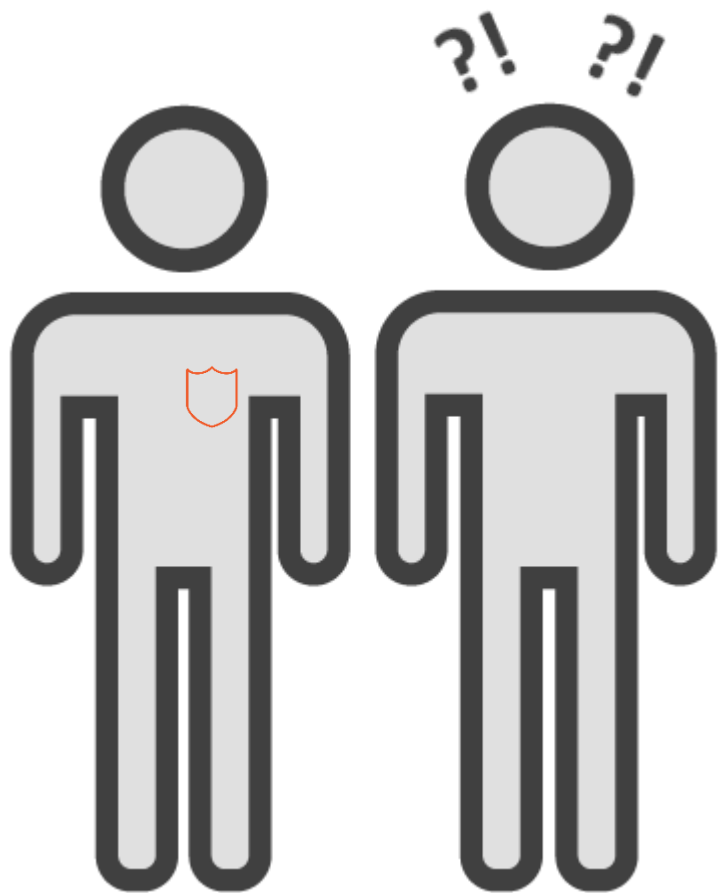


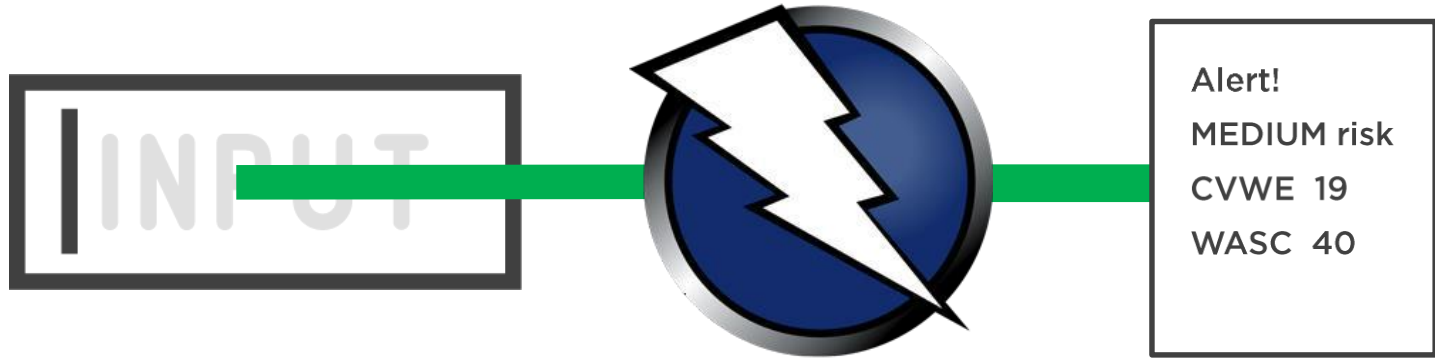
Documenting Found Vulnerabilities



Alerts







Alerts

-  CSRF Token is Miss
-  Source Code Discl
-  SQL Injection





High



Medium



Low



Informational



False Positive

Alert Risk Levels

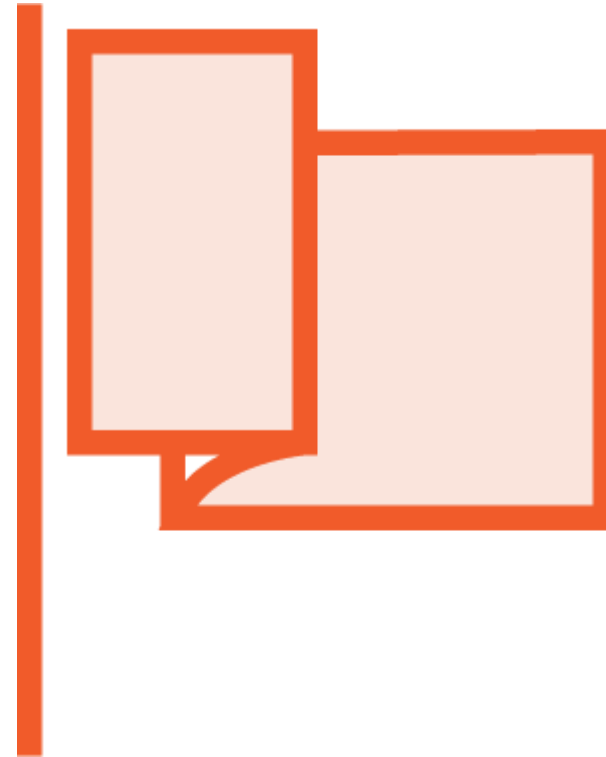
◀ Where are alerts raised?

- Active Scanning
 - *Quick start scan*
- Passive Scanning
- Manual Addon

◀ False Positive can only be set manually



Demo



Alerts



Generating a Report and Reviewing Results



Report

Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...

Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

Compare with Another Session...

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	6
Informational	0

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response
URL	http://192.168.56.101/shepherd/login.jsp
Parameter	X-Frame-Options
Instances	1
Solution	Most modern Web browsers support the X-Frame-Options HTTP header (X-Frame-Options: SAMEORIGIN). If you're using a web browser that supports X-Frame-Options, then you'll want to use SAMEORIGIN, otherwise browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combat
CWE Id	16
WASC Id	15

Low (Medium)	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means to another site. If this is a session cookie then session hijacking is possible.
URL	http://192.168.56.101/shepherd/index.jsp
Parameter	JSESSIONID
Evidence	Set-Cookie: JSESSIONID
URL	http://192.168.56.101/shepherd/login.jsp
Parameter	JSESSIONID
Evidence	Set-Cookie: JSESSIONID
Instances	2



Report

Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...

Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

Compare with Another Session...

```
<?xml version="1.0"?>
- <OWASPZAPReport generated="January 2017" version="2.5.0">
  - <site ssl="false" port="80" host="192.168.56.101" name="http://192.168.56.101">
    - <alerts>
      - <alertitem>
        <pluginid>10010</pluginid>
        <alert>Cookie No HttpOnly Flag</alert>
        <name>Cookie No HttpOnly Flag</name>
        <riskcode>1</riskcode>
        <confidence>2</confidence>
        <riskdesc>Low (Medium)</riskdesc>
        <desc><p>A cookie has been set without the HttpOnly flag, which means
          accessible and can be transmitted to another site. If this is a session
        </p></desc>
        - <instances>
          - <instance>
            <uri>http://192.168.56.101/shepherd/index.jsp</uri>
            <param>JSESSIONID</param>
            <evidence>Set-Cookie: JSESSIONID</evidence>
          </instance>
          - <instance>
            <uri>http://192.168.56.101/shepherd/login.jsp</uri>
            <param>JSESSIONID</param>
            <evidence>Set-Cookie: JSESSIONID</evidence>
          </instance>
        </instances>
        <count>2</count>
        <solution><p>Ensure that the HttpOnly flag is set for all cookies.</p></s>
        <reference><p>http://www.owasp.org/index.php/HttpOnly</p></refer>
        <cweid>16</cweid>
        <wascid>13</wascid>
      </alertitem>
      - <alertitem>
        <pluginid>10016</pluginid>
        <alert>Web Browser XSS Protection Not Enabled</alert>
        <name>Web Browser XSS Protection Not Enabled</name>
        <riskcode>1</riskcode>
        <confidence>2</confidence>
        <riskdesc>Low (Medium)</riskdesc>
        <desc><p>Web Browser XSS Protection is not enabled, or is disabled by
        </p></desc>
        - <instances>
```



Report

Generate HTML Report...
Generate XML Report...
 Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...

Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

Compare with Another Session...

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	19
Informational	14

Alert Detail

Cross-Domain Misconfiguration
Medium (Medium)



Report

Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
 Generate JSON Report...
Export Messages to File...
Export Response(s) to File...

Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

Compare with Another Session...

```
unt": "1", "solution": "<p>Manually confirm  
reference": "<p>https://www.owasp.org/in  
{, {      : \"10021\", \"alert\": \"X-Conte  
s was not set to 'nosniff'. This allows  
declared content type. Current (early 2  
onfig.      _/json?      =2716459&u  
m\": \"X-Content-Type-Options\"}], \"count\":  
ble, ensure that the end user uses a st  
is issue still applies to error type pa  
\\\"High\\\" threshold this scanner will no  
useful_HTTP_headers</p>\", \"cweid\": \"16\",  
\": \"Low (Medium)\", \"desc\": \"<p>A cookie ha  
onfig/v1/config/json\"      &u  
m\": \"__cfduid\", \"evidence\": \"Set-Cookie: _  
is set for cookies containing such sens  
\"}}], {\"@name\": \"https://www      .om\",  
st\": \"stats.g      .net\", \"@port\": \"  
2\", \"riskdesc\": \"Medium (Medium)\", \"desc\":
```



Report

Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
 Export Messages to File...
Export Response(s) to File...

Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

Compare with Another Session...

```
==== 8 =====  
GET http://192.168.56.1  
Proxy-Connection: keep-  
Cache-Control: max-age=  
Upgrade-Insecure-Request  
User-Agent: Mozilla/5.0  
Chrome/55.0.2883.87 Saf  
Accept: text/html,application/javascript  
DNT: 1  
Referer: http://192.168  
Accept-Encoding: sdch  
Accept-Language: en-US,  
Cookie: token=-34126136  
acopendivids=swingset,j  
JSESSIONID=D9691D8BDD3D  
Host: 192.168.56.101
```

```
HTTP/1.1 200 OK  
Date: Mon, 23 Jan 2017  
Server: Apache-Coyote/1  
Content-Type: text/html  
Via: 1.1 127.0.1.1
```



Report

Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
 Export Response(s) to File...

Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

Compare with Another Session...

```
index.jsp
1
2
3
4 <html xmlns="http://www.w3.org/1999/xhtml">
5 <head>
6 <meta http-equiv="content-type" content="text/html; charset=utf-8">
7 <title>OWASP Security Shepherd</title>
8
9 <!-- You are currently looking at the core server
10      Nothing related to the levels in Security Shepherd
11      You might be looking for the iframe embedded in
12      Try a tool like Firebug to make this stuff easier -->
13
14      Security Shepherd Version: 2.4 -->
15
16 <link href="css/theCss.css" rel="stylesheet" type="text/css">
17 <link rel="shortcut icon" href="css/images/flavico.ico">
18
19 </head>
20 <body>
21 <script type="text/javascript" src="js/jquery.js"></script>
22 <div id="wrapper">
23 <div id="header">
24 <h1>Security Shepherd</h1>
25 <div style="position: absolute; right: 100px; top: 0px;">
26 <p>
27 <strong>Welcome admin</strong><br />
28 <strong><a href="logout?csrfToken=-34126136">Logout</a></strong>
29 </p>
30 </div>
31 </div>
```



Report

Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...



Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

GET	http://192.168.56.101/shephe
GET	http://192.168.56.101/shephe
POST	http://192.168.56.101/shephe
GET	http://192.168.56.101/shephe
GET	http://192.168.56.101/shephe
POST	https://clients4.google.com/
POST	https://clients4.google.com/

Compare with Another Session...



Report

Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...

Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

 Compare with Another Session...



Demo



Reporting



Putting It All Together for a Test



Demo



- ZAP Application
- Virtualbox -> BWA
- Browser
- Proxy (foxyproxy)
- BWA homepage



Putting it all together
Setup and test



Course Summary



Course Key Points



Legal reminder

Proxy

Marketplace

Place in context

Break



Course

Key Points



Spider / Force Browse

Passive vs active scanning

Quick start

Fuzzer

OWASP

