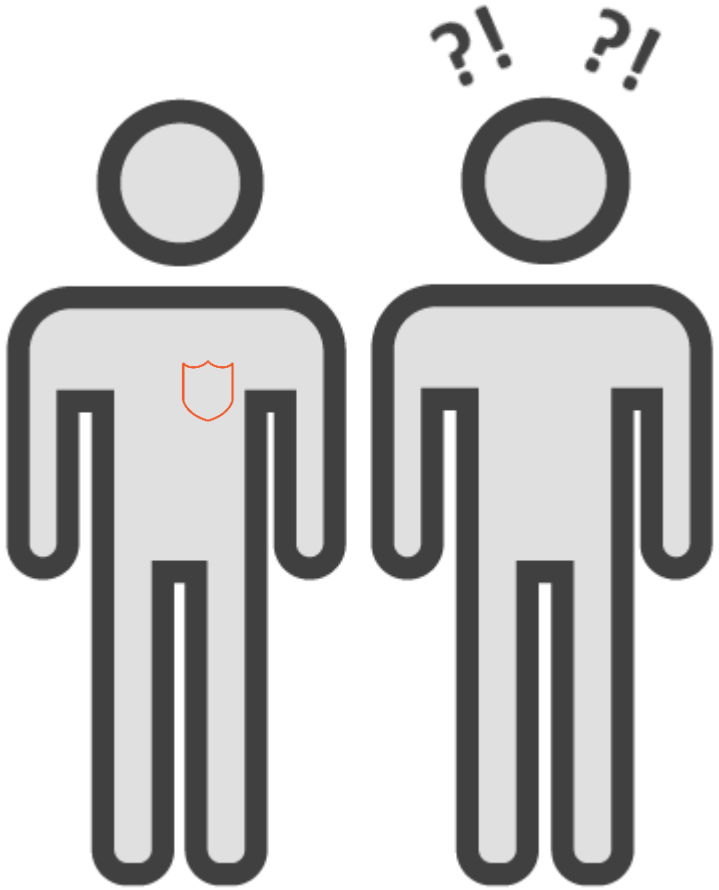
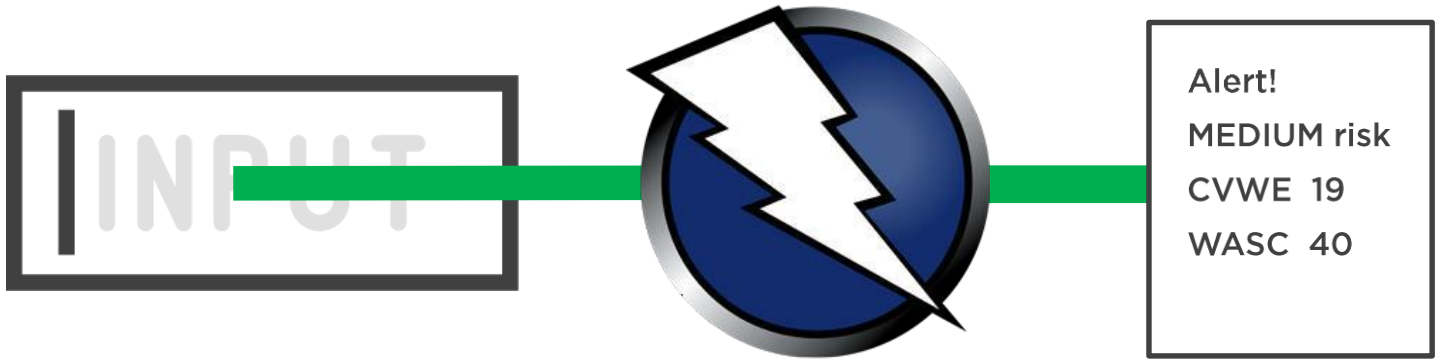
Documenting Found Vulnerabilities

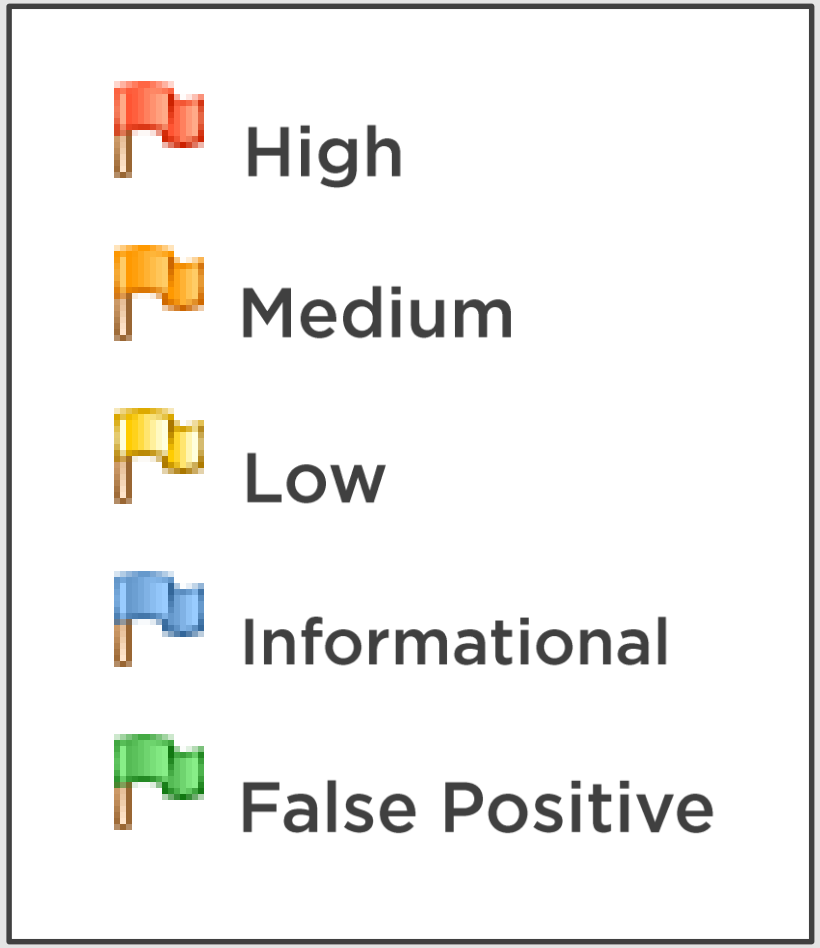
Alerts


?!
?!


Security Prioritization


INPUT
Alert!
MEDIUM risk
CVWE 19
WASC 40

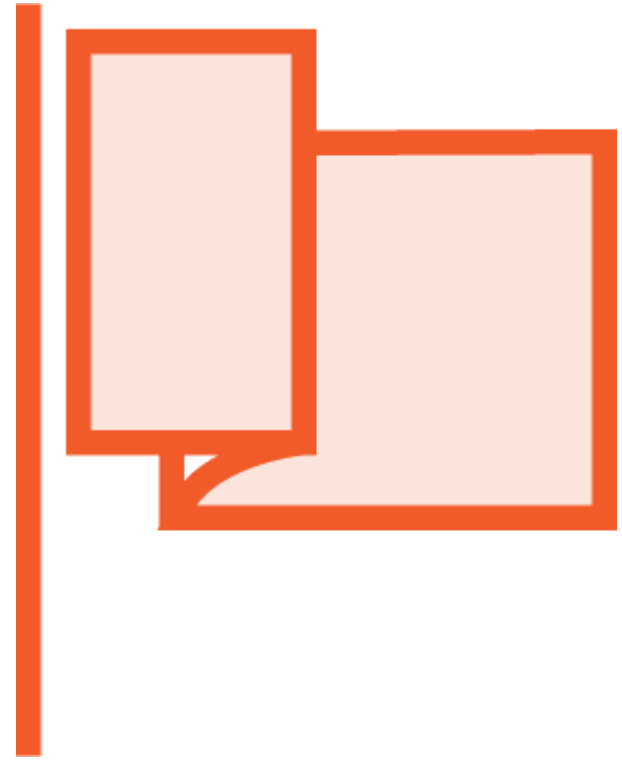

Alerts
CSRF Token is Miss
Source Code Discl
SQL Injection



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

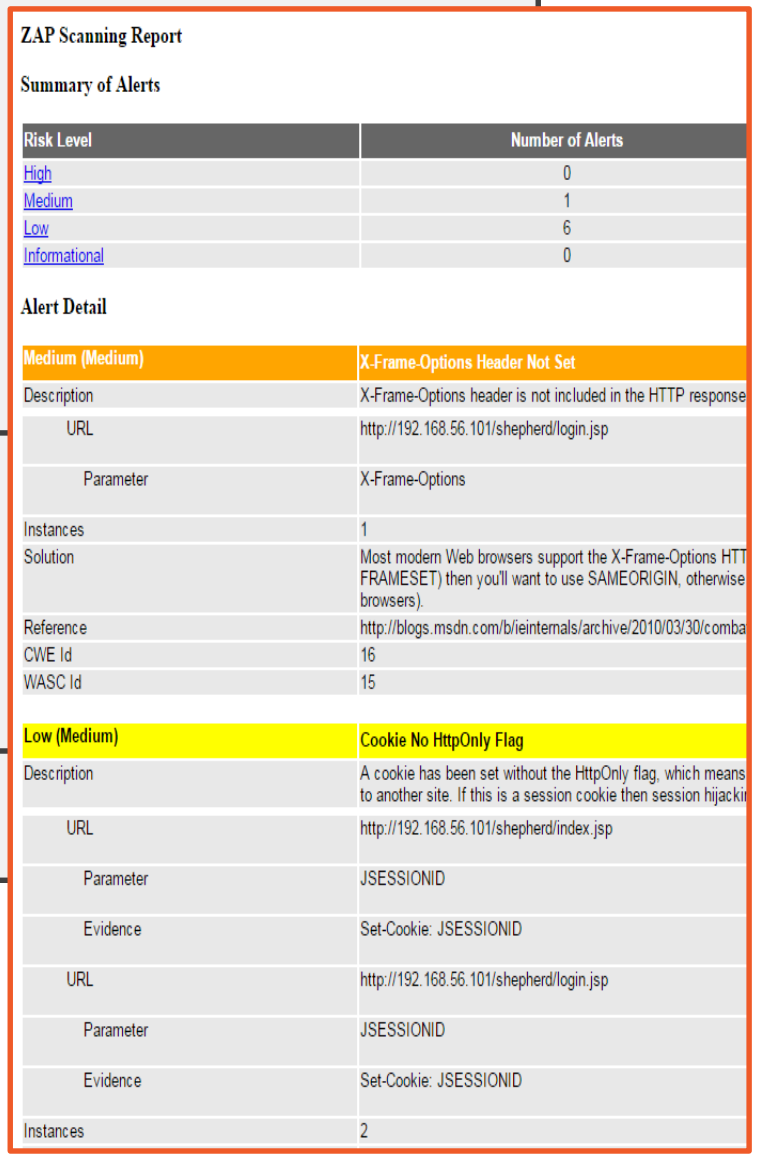
Generating a Report and Reviewing Results

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 HTT FRAMESET) then you'll want to use SAMEORIGIN, otherwise browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/comba
CWE Id	16
WASC Id	15

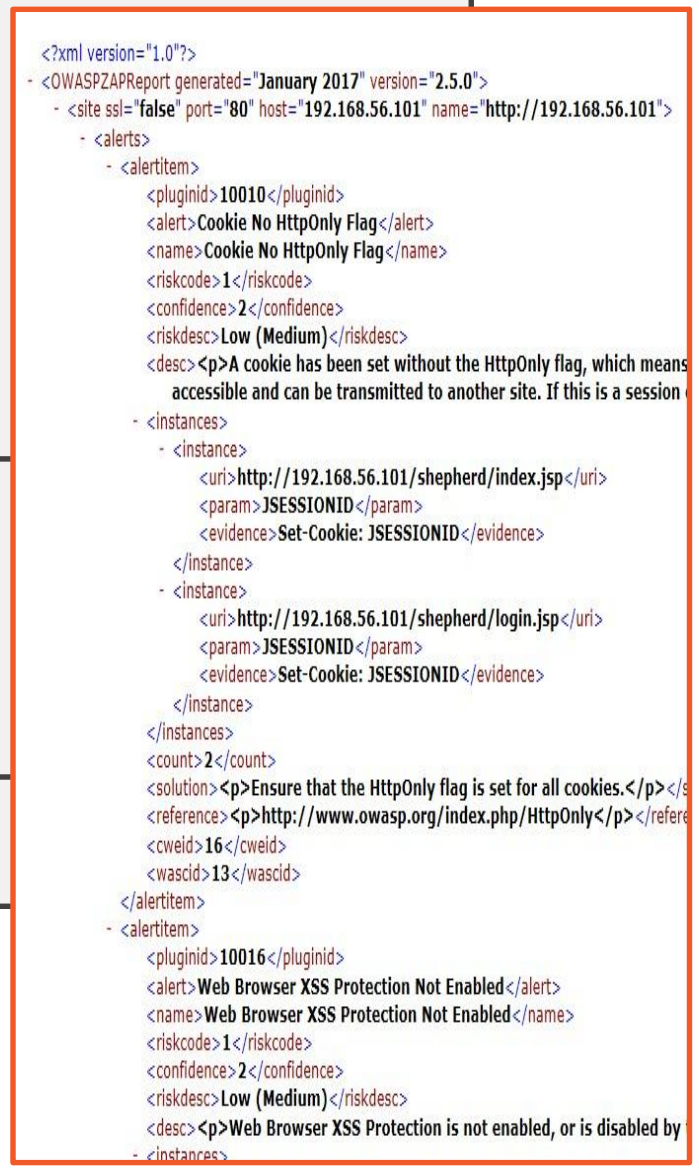
Low (Medium)	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means to another site. If this is a session cookie then session hijackir
URL	http://192.168.56.101/shepherd/index.jsp
Parameter	JSESSIONID
Evidence	Set-Cookie: JSESSIONID
URL	http://192.168.56.101/shepherd/login.jsp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

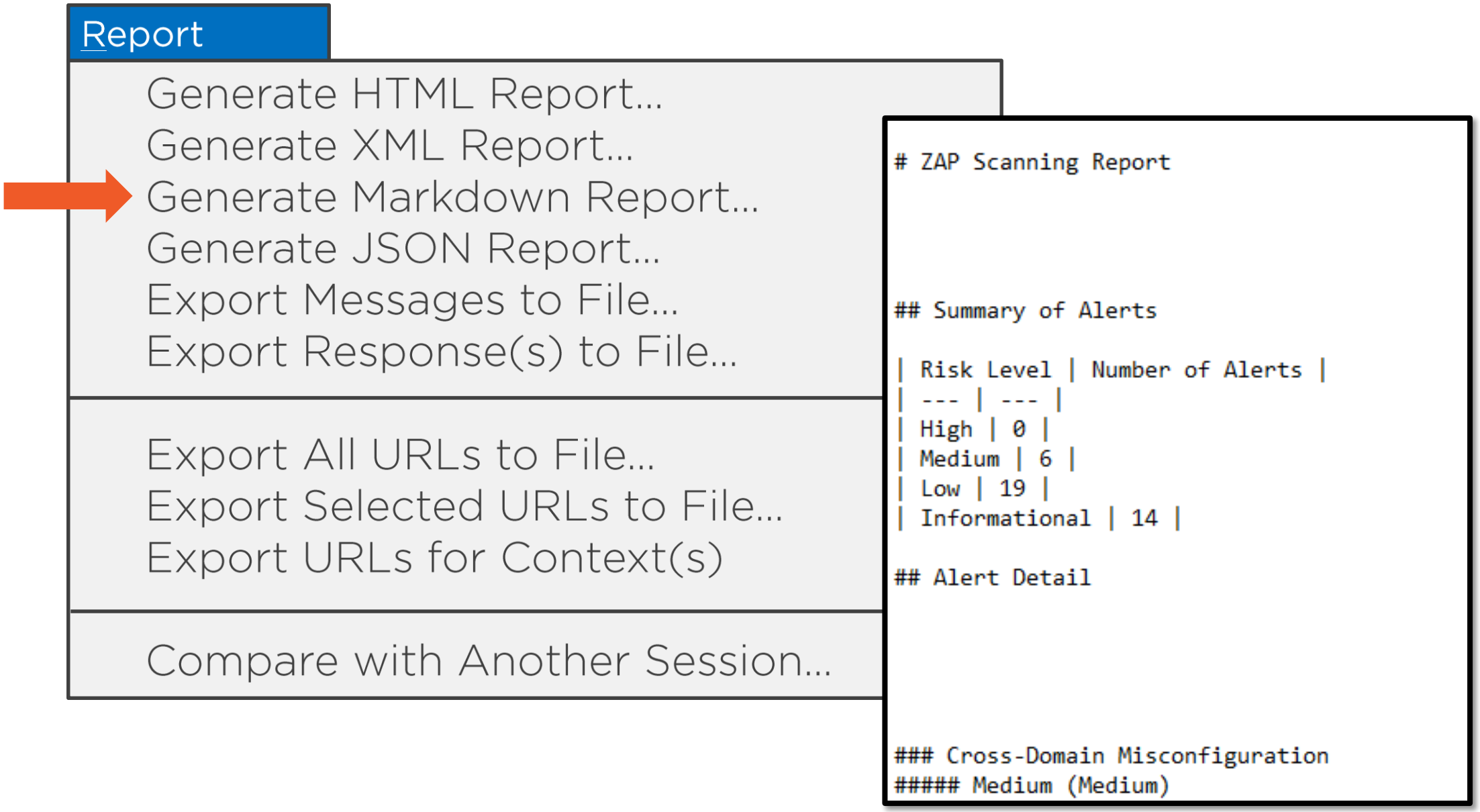
Report

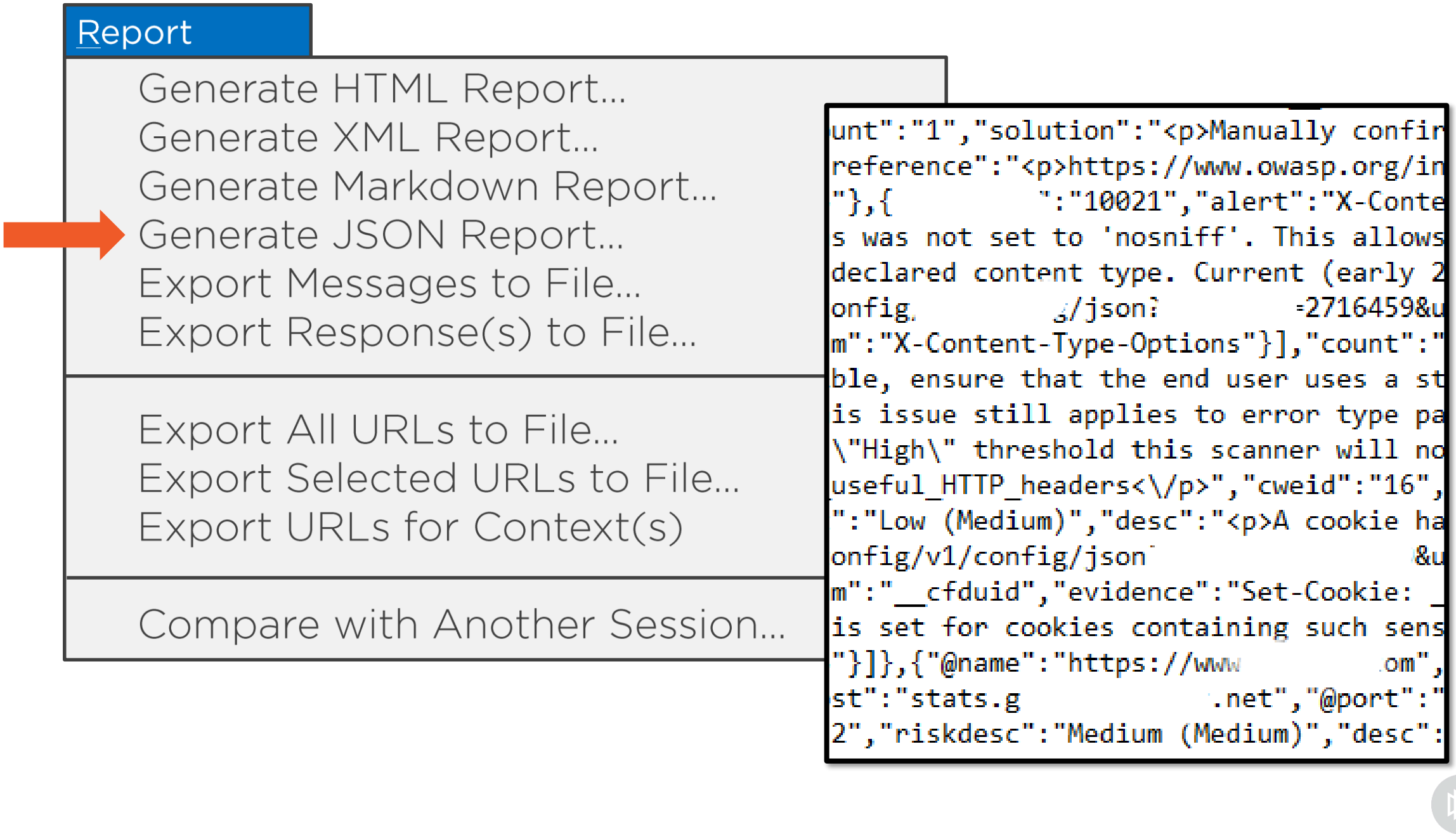
Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...

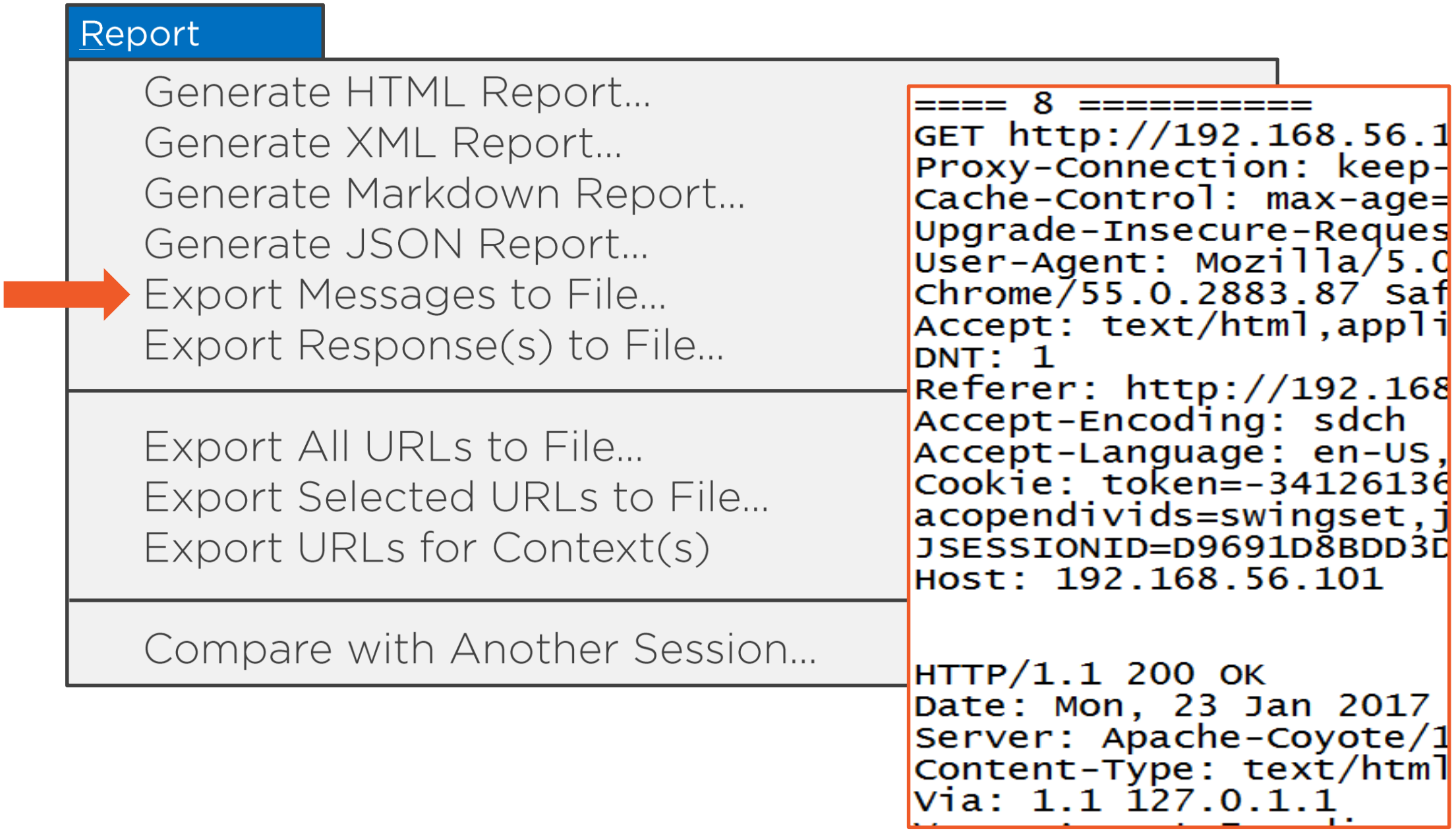
Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)

Compare with Another Session...




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 confir
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":

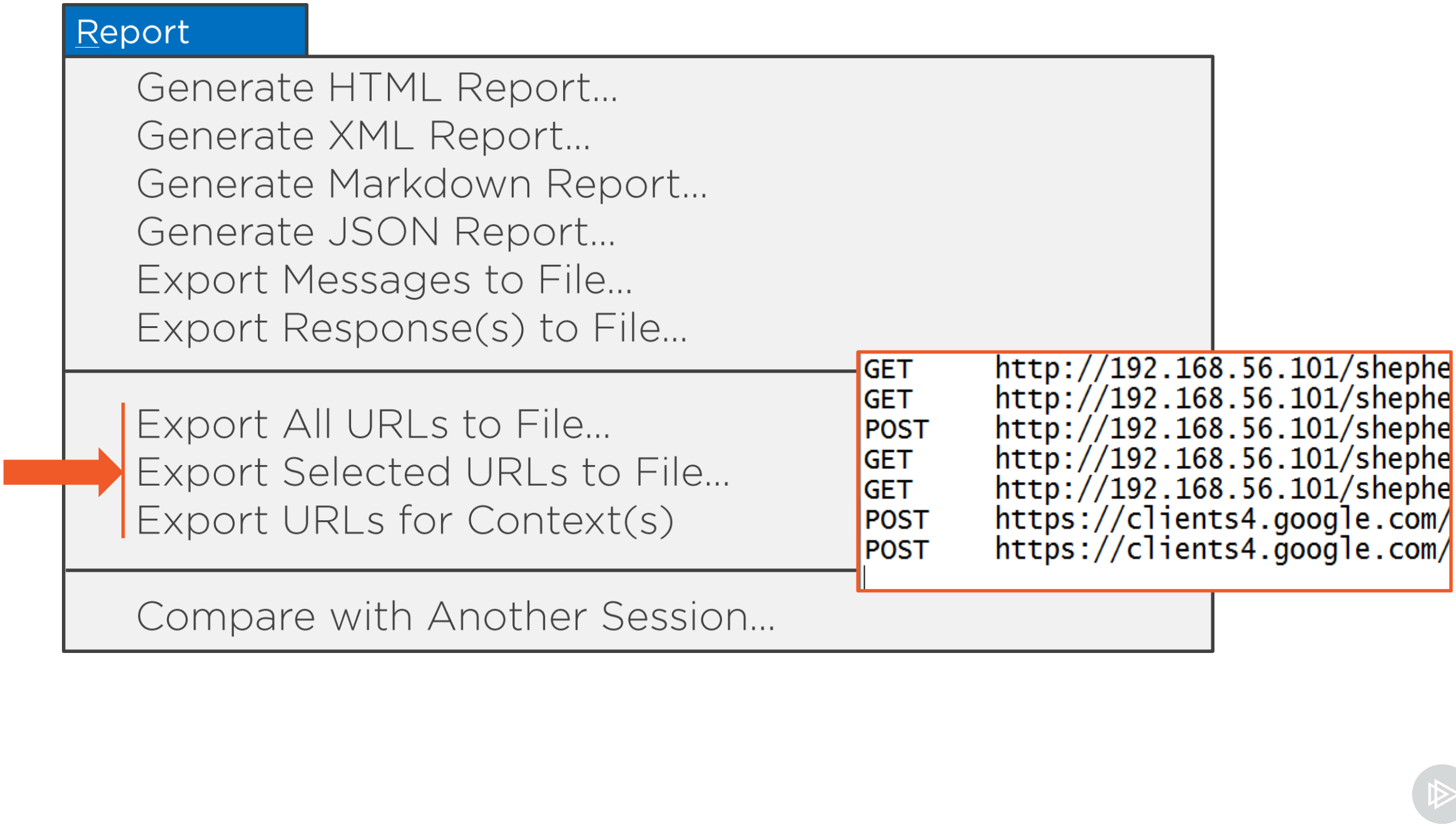

Report
Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...
Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)
Compare with Another Session...
==== 8 ==========
GET http://192.168.56.1
Proxy-Connection: keep-
Cache-Control: max-age=
Upgrade-Insecure-Reques
User-Agent: Mozilla/5.0
Chrome/55.0.2883.87 Saf
Accept: text/html,appli
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

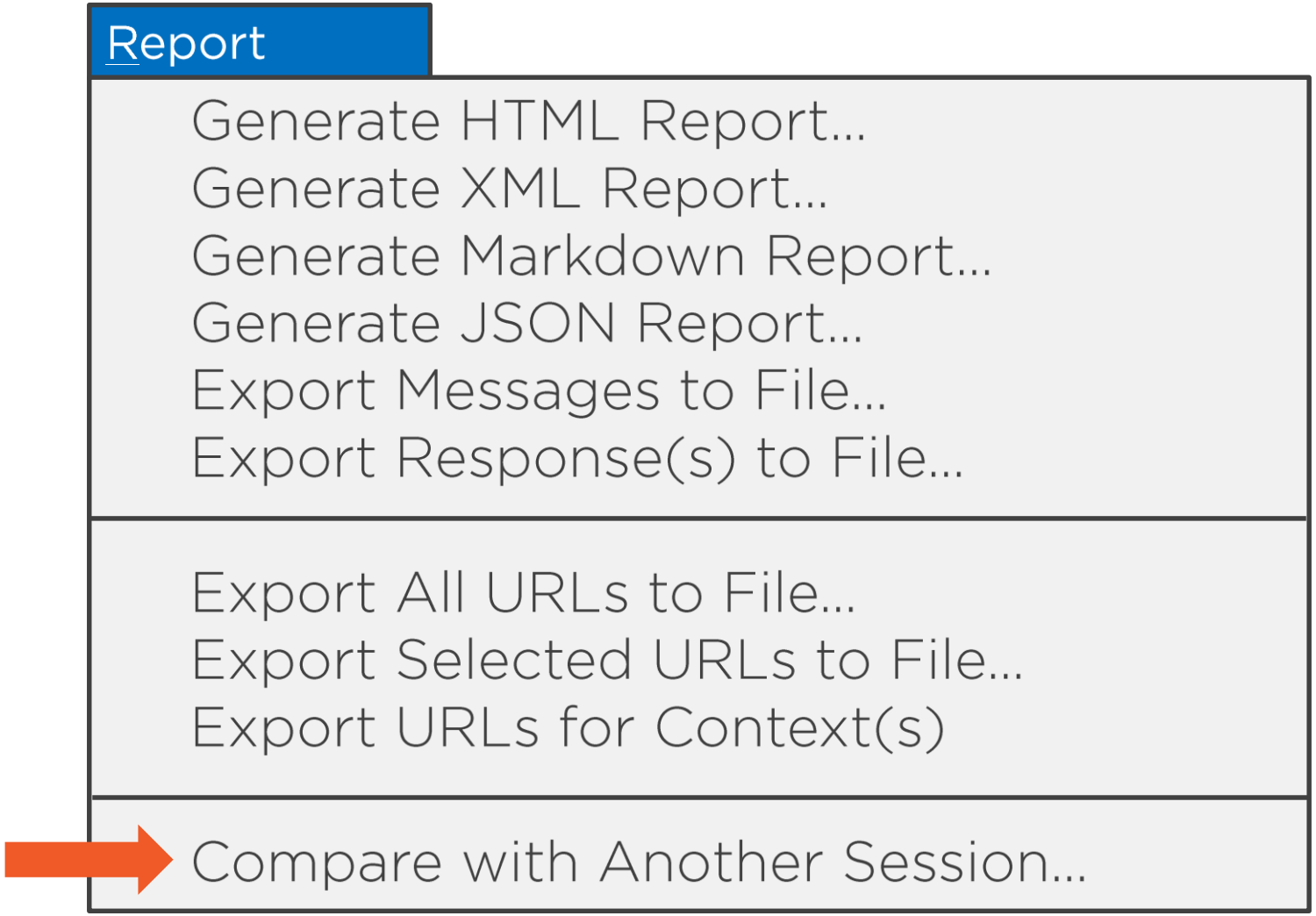
Report

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...


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...
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/


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