Security Testing - OWASP ZED Attack Proxy

Version: 1.0

16th May 2019

Vipul Salpekar

Prepared by Infogen Labs Inc.

Revision History

Date	Description	Author	Comments
16/05/2019	1.0	Vipul Salpekar	

Document Approval

The following OWASP ZAP document has been accepted and approved by the following:

Signature	Printed Name	Title	Date
Rohini	Rohini Jadhav	Lead Software Eng.	17/05/2019

Table of Contents

Introduction

Security testing is an approach which detects the security mechanisms of a system that protects their data and maintains a proper functionality as intended. Due to the logical limitations of security testing, passing security testing is not an indication that no flaws exist or that the system adequately satisfies the security requirements.

In order to make applications tested at Infogen Labs Inc. Security Compliance applications, we use OWASP ZED Attack Proxy (ZAP) tool
With the use of this tool, security threats to the applications are omitted at early stages of Application life cycle.
In addition to this, ZAP is developed by OWASP which itself is a major security compliance community who publish a list of top 10 vulnerabilities every year that are found globally across all domains.

Purpose

The purpose of this document is to give a detailed description of OWASP ZAP tool so that a beginner to Security Testing can perform Security Scan and do manual Pentest in order to validate the detected Vulnerabilities.

OWASP Zed Attack Proxy

OWASP ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing as well as experienced security professionals.
ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.

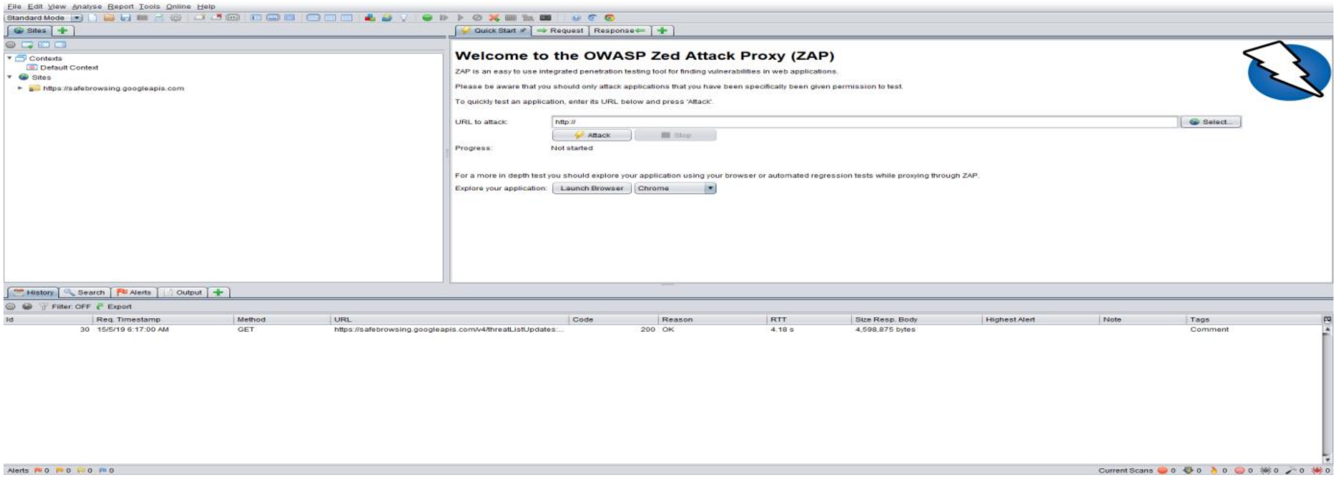
ZAP User Interface

By default, ZAP displays:

- A top-level menu which gives access to many of the automated and manual tools
- A top-level toolbar which includes buttons for commonly used features
- A ‘tree’ window on the left-hand side which displays the Sites tree and the Scripts tree
- A ‘workspace’ window on the top right-hand side, which allows you to display and edit requests, responses and scripts,
- An ‘information’ window underneath workspace window, which displays details of the automated and manual tools
- A footer which displays a summary of the alerts found and the status of the main automated tools

By default, only a small number of tabs are shown when ZAP starts. Other tabs appear when you run the related tools or can be added manually via the 'green plus' tabs.
You can 'pin' tabs so that they are always shown when you restart ZAP.

Note: - In order to reduce the complexity of the UI many of ZAPs features are only shown via context sensitive right-click menus. There are right-click menus throughout ZAP: on the nodes of the Sites and Script trees, on the tables displayed in the information tabs and in the workspace tabs. Some menus are only displayed when you highlight text - for example the ‘Fuzz...’ menu is only shown if you right click a highlighted string in the Request tab.



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:// [Select...]

[Attack] [Stop]

Progress: Not started

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

Explore your application: [Launch Browser] [Chrome]

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
30	15/5/19 6:17:00 AM	GET	https://safebrowsing.googleapis.com/v4/threatListUpdates:...	200	OK	4.18 s	4,598,875 bytes			Comment

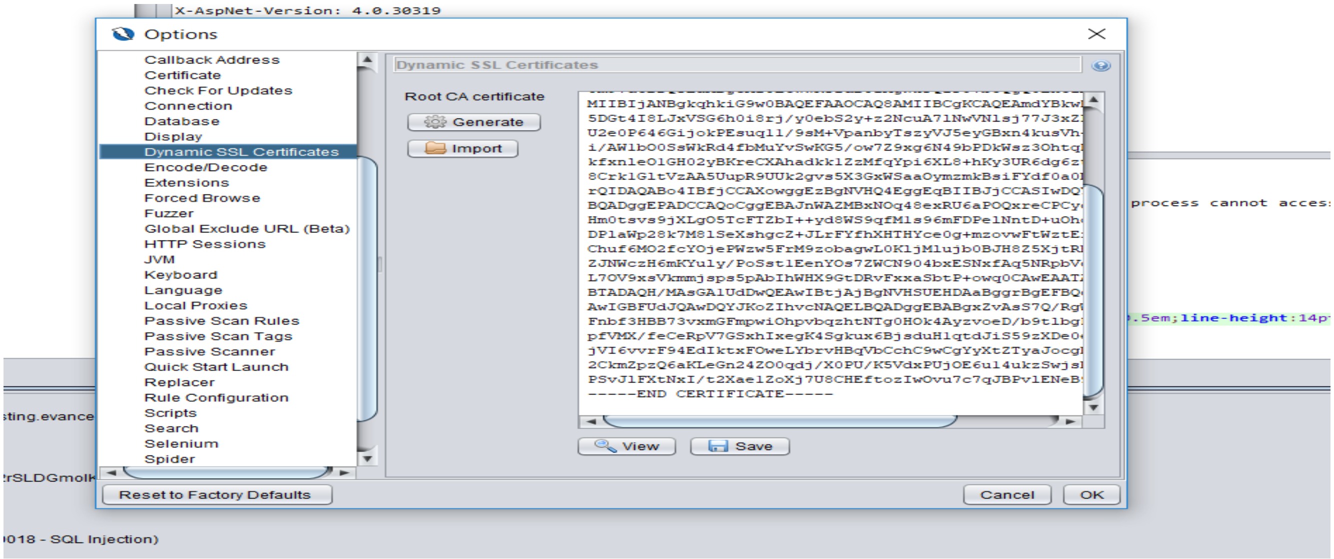
ZAP Installation

Zap tool is easy to install and use. Please follow below steps to install an application –

Step 1 Download and install JAVA from the URL - https://www.java.com/en/download/

Step 2 Download and Install ZAP from the URL - https://github.com/zaproxy/zaproxy/wiki/Downloads

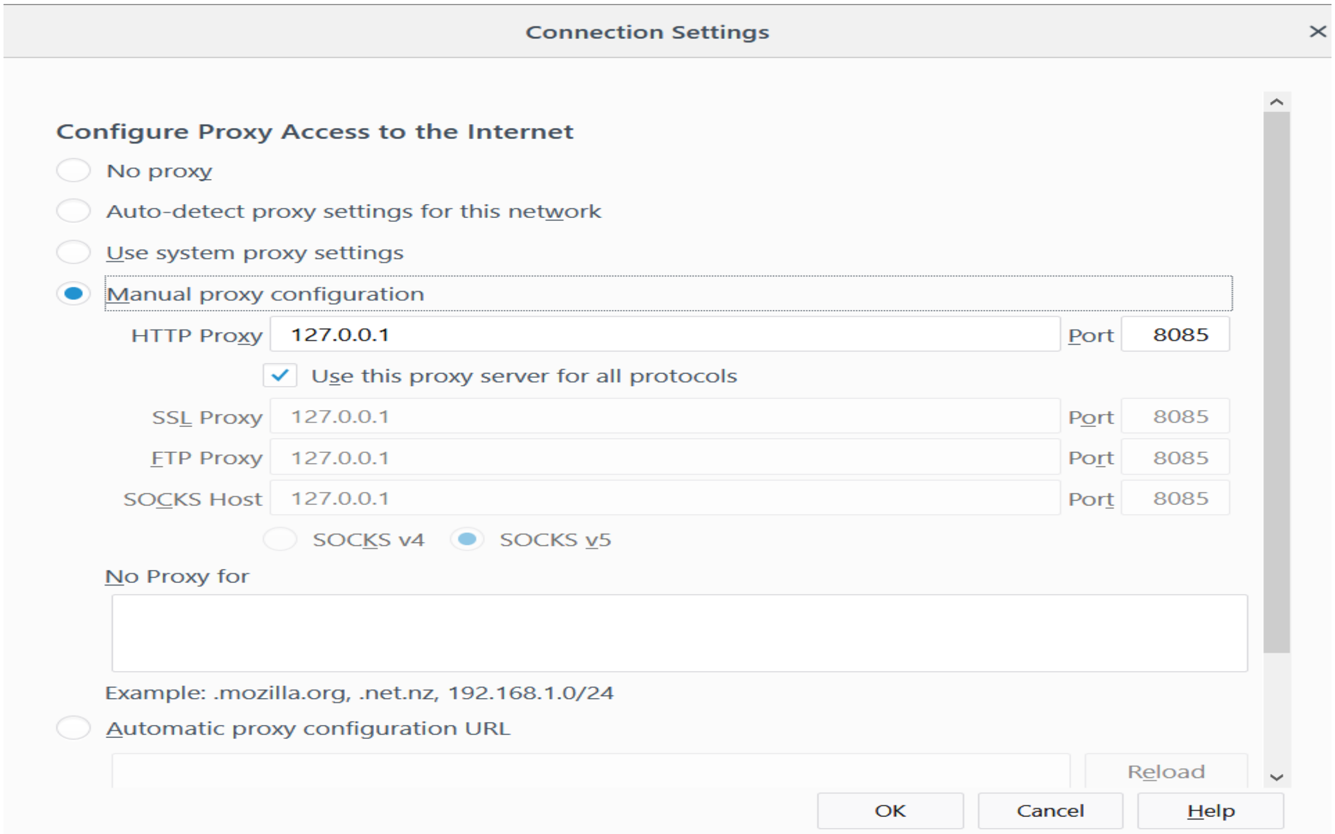
Step 3 In ZAP go to Tools -> options -> Dynamic SSL certificates -> Save the certificate in your system.



```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmdYBkwl
5DGt4I8LJxVSG6h0i8rj/y0ebS2y+z2NcuA71NwVNlsj77J3xZ
U2e0P646GijokPEsuql1/9sM+VpanbyTszyVJ5eyGBxn4kusVh
i/AW1bO0SsWkRd4fbMuYvSwKG5/ow7Z9xg6N49bPDkWsz3Ohtq
kfxnleO1GH02yBKreCXAhadkklZzMfqYpi6XL8+hKy3UR6dg6z
8Crk1G1tVzAA5UupR9UUk2gvs5X3GxWSaaOymzmkBsiFYdf0a0
rQIDAQABo4IBfjCCAXowggEzBgNVHQ4EggEqBIIBJjCCASIwDQ
BQADggEPADCCAQoCggEBAJnWAZMBxNOq48exRU6aPOQxreCPCy
Hm0tsvs9jXLgO5TcFTZbI++yd8WS9qfMls96mFDPelNntD+uOh
DPlaWp28k7M81SeXshgcZ+JLrFYfhXHTHYce0g+mzovwFtWztE
Chuf6MO2fcYOjePWzw5FrM9zobagwL0KljMlujb0BJH8Z5XjtR
ZJNWczH6mKYuly/PoSstlEenYOs7ZWCN904bxESNxfAq5NRpbV
L7OV9xsVkmmjsps5pAbIhWHX9GtDRvFxxaSbtP+owq0CAwEAAT
BTADAQH/MAsGA1UdDwQEAwIBtjAjBgNVHSUEHDAaBggrBgEFBQ
AwIGBFUdJQAwDQYJKoZIhvcNAQELBQADggEBABgxZvAsS7Q/Rg
Fnbf3HBB73vxmGFmpwiOhpvbqzhtNTg0HOk4AyzvoeD/b9tlbg
pfVMX/feCeRpV7GSxhIxegK4Sgkux6BjsduH1qtdJiS59zXDe0
jVI6vvrF94EdIktxFOweLYbrvHBqVbCchC9wCgYyXtZTyaJocg
2CkmZpzQ6aKLeGn24Z00qdj/X0PU/K5VdxPUjOE6ul4ukzSwjs
PSvJ1FXtNxI/t2Xae1ZoXj7U8CHEftozIwOvu7c7qJBPvlENeB
-----END CERTIFICATE-----
```

Step 4 In your browser, Go to View certificates -> Click on import and browse for the saved certificate -> import the certificate in your browser.

Step 5 Go to Network settings of your browser make the settings as per the below screenshot.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8085

☑ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8085

FTP Proxy 127.0.0.1 Port 8085

SOCKS Host 127.0.0.1 Port 8085

○ SOCKS v4 ● SOCKS v5

No Proxy for

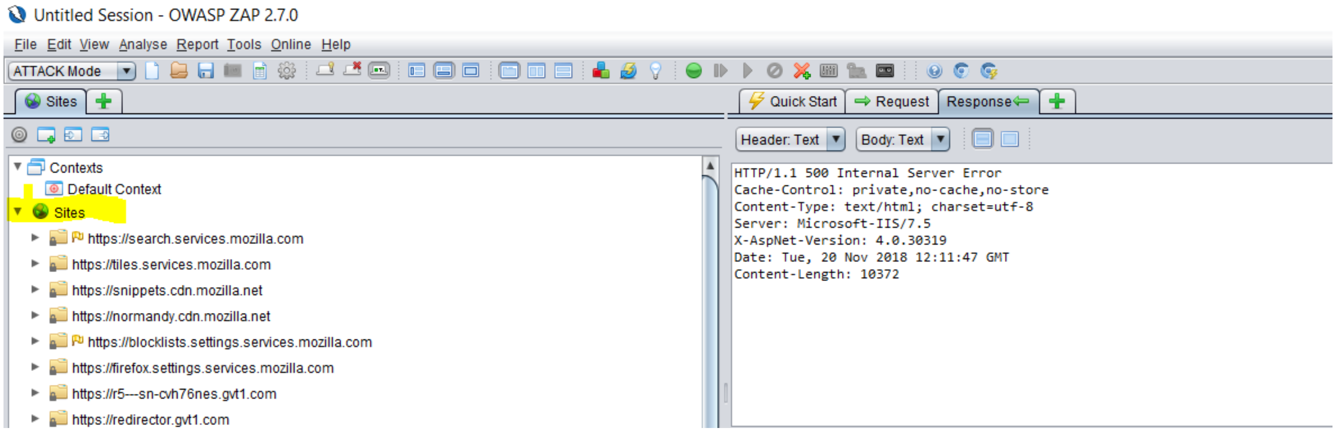
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL

Step 6 Go to ZAP → tools → Options → Local proxies and do the changes as per the below screenshot.

Note: - Port number in ZAP tool as well as in browser should be same.

After this, any URL that you hit in the browser should be visible under site menu of ZAP tool as shown below: -


Untitled Session - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
ATTACK Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text

Contexts
Default Context
Sites
https://search.services.mozilla.com
https://tiles.services.mozilla.com
https://snippets.cdn.mozilla.net
https://normandy.cdn.mozilla.net
https://blocklists.settings.services.mozilla.com
https://firefox.settings.services.mozilla.com
https://r5---sn-cvh76nes.gvt1.com
https://redirector.gvt1.com

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private,no-cache,no-store
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
Date: Tue, 20 Nov 2018 12:11:47 GMT
Content-Length: 10372
```

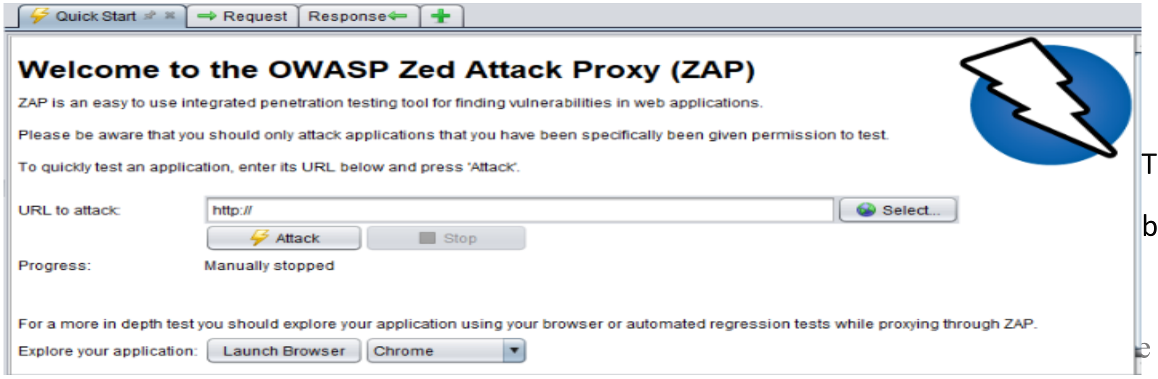
Active & Passive Scanning in ZAP

ZAP passively scans all of the requests and responses that it discovers via the spiders or that are proxied through it from your browser. Passive scanning does not change the responses in any way and is therefore always safe to use. Scanned is performed in a background thread to ensure that it does not slow down the exploration of an application. Passive scanning is good for finding a limited number of potential vulnerabilities, such as missing security related HTTP headers. It can be an effective way to get a sense of the state of security in a given web application, and clues for where to focus more invasive manual testing.
Active scanning attempts to find potential vulnerabilities by using known attacks against the selected
targets. As active scanning is an attack on those targets it is completely under user control and should only be used against applications that you have permission to test. Active scanning can be started via the Active Scan tab or the right click 'Attack' menu.

Scanning process in ZAP

ZAP has mainly two ways to perform an Active Scan.

1. The most straightforward of these is to use the *Quick Start* welcome screen that is displayed by default when ZAP is launched.



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://

Progress: Manually stopped

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

Explore your application: Launch Browser Chrome

To

begi

n, enter the URL you want to scan in the *URL to attack* field, and then press the *Attack* button.

This will launch a twostep process:

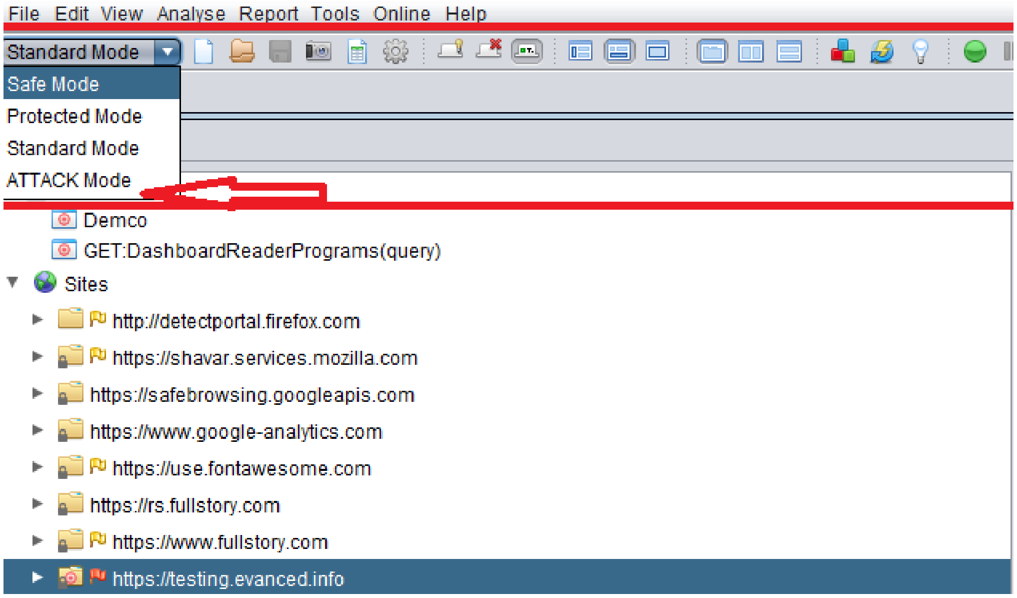
Firstly, a spider will be used to crawl the website: ZAP will use the supplied URL as a starting point to explore the website to determine all the hyperlinks within it (links that direct outside the domain will be ignored). The *Spider* tab at the bottom of the ZAP window will display the links as they are found. While this is happening, ZAP will simultaneously passively scan the links.

Secondly, the Active Scan will launch once the crawl is complete the active scan will start. ZAP will launch a variety of attack scenarios at the URLs listed in the *Spider* tab. The attack progress will be displayed in the *Active Scan* tab.

Once the active scan has finished, the results will be displayed in the *Alerts* tab. This will contain all the security issues found during both the Spider and Active scan. They will be flagged according to their risk - red for High Priority, and green and yellow for Medium to Low Priority, respectively.

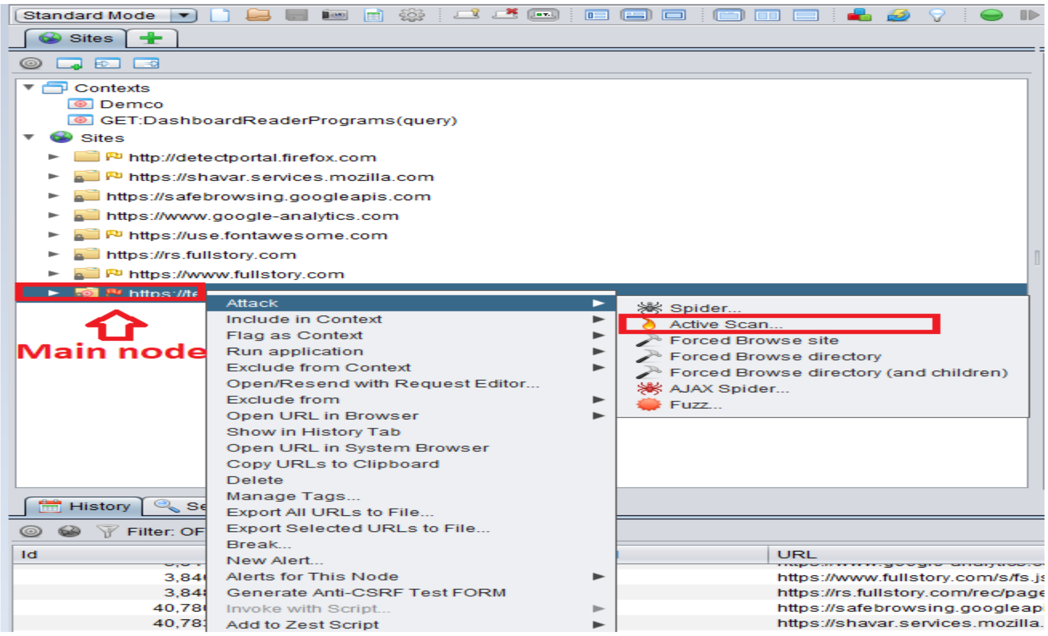
2. The other way to perform Active Scan in ZAP is to manually crawl the application and as all the URLS visited in the browser gets captured in the "Sites" section through proxy.

Note: - Before capturing the application URL's through manual crawling, you should select the ZAP to the "Attack mode".


File Edit View Analyse Report Tools Online Help
Standard Mode
Safe Mode
Protected Mode
Standard Mode
ATTACK Mode
Demco
GET:DashboardReaderPrograms(query)
Sites
http://detectportal.firefox.com
https://shavar.services.mozilla.com
https://safebrowsing.googleapis.com
https://www.google-analytics.com
https://use.fontawesome.com
https://rs.fullstory.com
https://www.fullstory.com
https://testing.evanced.info

We can

start the active scanning by right clicking on the Main node of site to be scanned.


Standard Mode
Sites
Contexts
Demco
GET:DashboardReaderPrograms(query)
Sites
http://detectportal.firefox.com
https://shavar.services.mozilla.com
https://safebrowsing.googleapis.com
https://www.google-analytics.com
https://use.fontawesome.com
https://rs.fullstory.com
https://www.fullstory.com
https://te
Main node
Attack
Include in Context
Flag as Context
Run application
Exclude from Context
Open/Resend with Request Editor...
Exclude from
Open URL in Browser
Show in History Tab
Open URL in System Browser
Copy URLs to Clipboard
Delete
Manage Tags...
Export All URLs to File...
Export Selected URLs to File...
Break...
New Alert...
Alerts for This Node
Generate Anti-CSRF Test FORM
Invoke with Script...
Add to Zest Script
Spider...
Active Scan...
Forced Browse site
Forced Browse directory
Forced Browse directory (and children)
AJAX Spider...
Fuzz...
History
Filter: OF
Id
URL
3,84
3,84
40,78
40,78
https://www.fullstory.com/s/fs.js
https://rs.fullstory.com/rec/page
https://safebrowsing.googleap
https://shavar.services.mozilla.

The attack progress will be displayed in the *Active Scan* tab.

Once the active scan has finished, the results will be displayed in the *Alerts* tab. This will contain all the security issues found during Active scan.

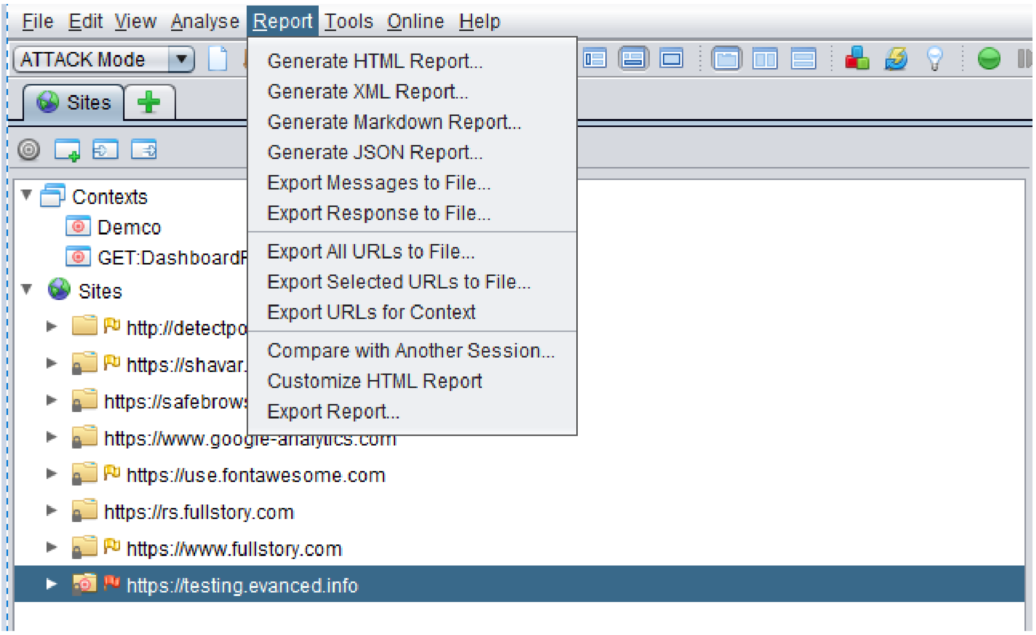
They will be flagged according to their risk - red for High Priority, and green and yellow for Medium to Low Priority, respectively.

ZAP Report

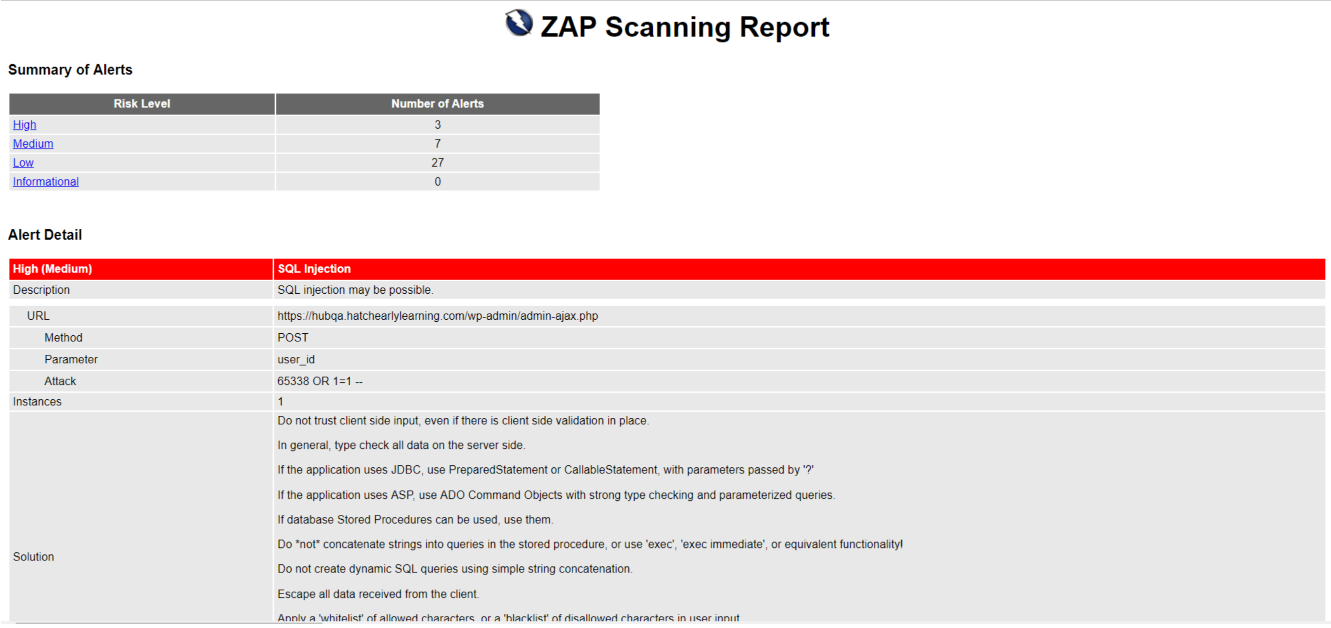
Zap gives the scanning report in XML, XHTML and HTML formats.

Below are the steps to generate Scanning report in OWASP ZAP: -

- Select the Main node of the site which is scanned from the Site section.
- Click on the Reports and Select the format in which you want to generate the report.
- Give appropriate path and save it.


File Edit View Analyse Report Tools Online Help
ATTACK Mode
Sites
Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response to File...
Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context
Compare with Another Session...
Customize HTML Report
Export Report...
Contexts
Demco
GET:DashboardF
Sites
http://detectpo
https://shavar.
https://safebrows
https://www.google-analytics.com
https://use.fontawesome.com
https://rs.fullstory.com
https://www.fullstory.com
https://testing.evanced.info

Below is the glance of report in HTML format generated by OWASP ZAP tool: -



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	3
Medium	7
Low	27
Informational	0

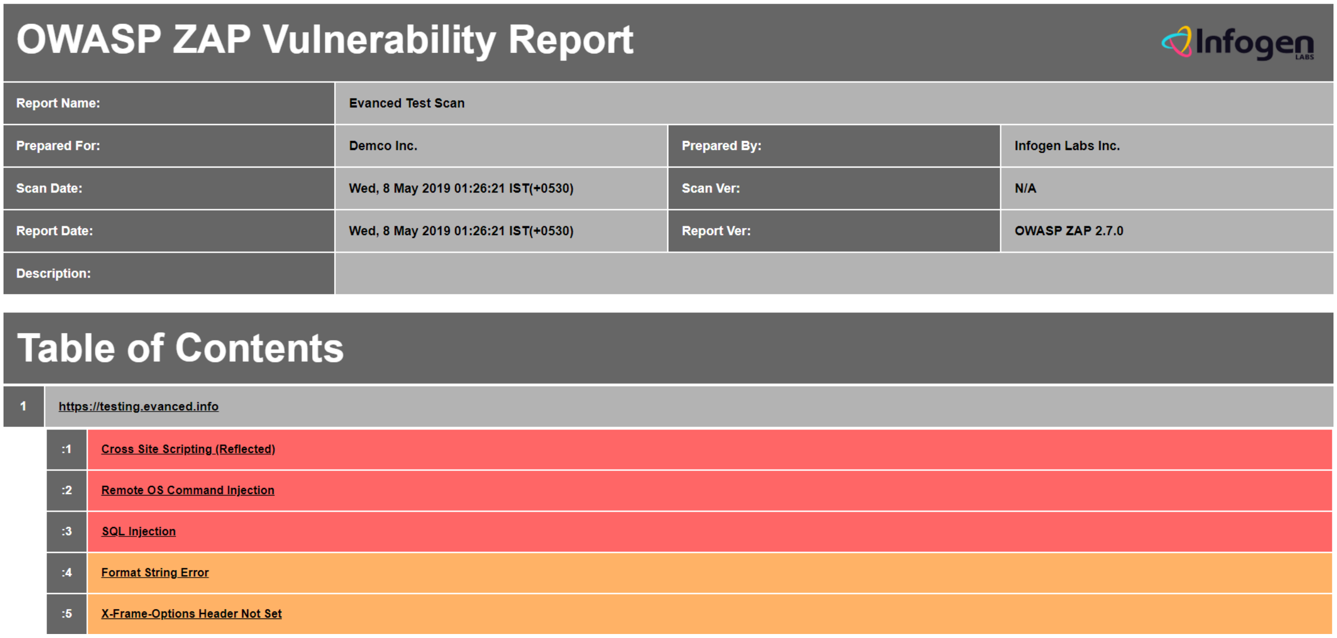
Alert Detail

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	https://hubqa.hatchearlylearning.com/wp-admin/admin-ajax.php
Method	POST
Parameter	user_id
Attack	65338 OR 1=1 --
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input

Please refer detailed report here:

ZAP Scanning Report.pdf

Below is the quick view of the report developed by Infogen Labs: -



OWASP ZAP Vulnerability Report

Report Name:	Evanced Test Scan		
Prepared For:	Demco Inc.	Prepared By:	Infogen Labs Inc.
Scan Date:	Wed, 8 May 2019 01:26:21 IST(+0530)	Scan Ver:	N/A
Report Date:	Wed, 8 May 2019 01:26:21 IST(+0530)	Report Ver:	OWASP ZAP 2.7.0
Description:			

Table of Contents

1	https://testing.evanced.info
:1	Cross Site Scripting (Reflected)
:2	Remote OS Command Injection
:3	SQL Injection
:4	Format String Error
:5	X-Frame-Options Header Not Set

Please refer detailed report here:

OWASP ZAP
Vulnerability Report

Summary

Security Testing is somewhat which assures the customer that their product is sanitized from the security threats.
Infogen Labs Inc. implements the Scanning process present in OWASP ZAP for the applications under test to make sure the primary OWASP top 10 vulnerabilities are removed.

References

https://github.com/zaproxy/zaproxy/wiki/Introduction