ZAP Penetration Testing Tutorial to Detect Vulnerabilities

Toobler Follow
Jul 13, 2018 · 3 min read

By Geethu Alexander

Penetration testing (otherwise known as pen testing, or the more general security testing) is the process of testing your applications for vulnerabilities, and answering a simple question: “What could a hacker do to harm my application, or organization, out in the real world?”

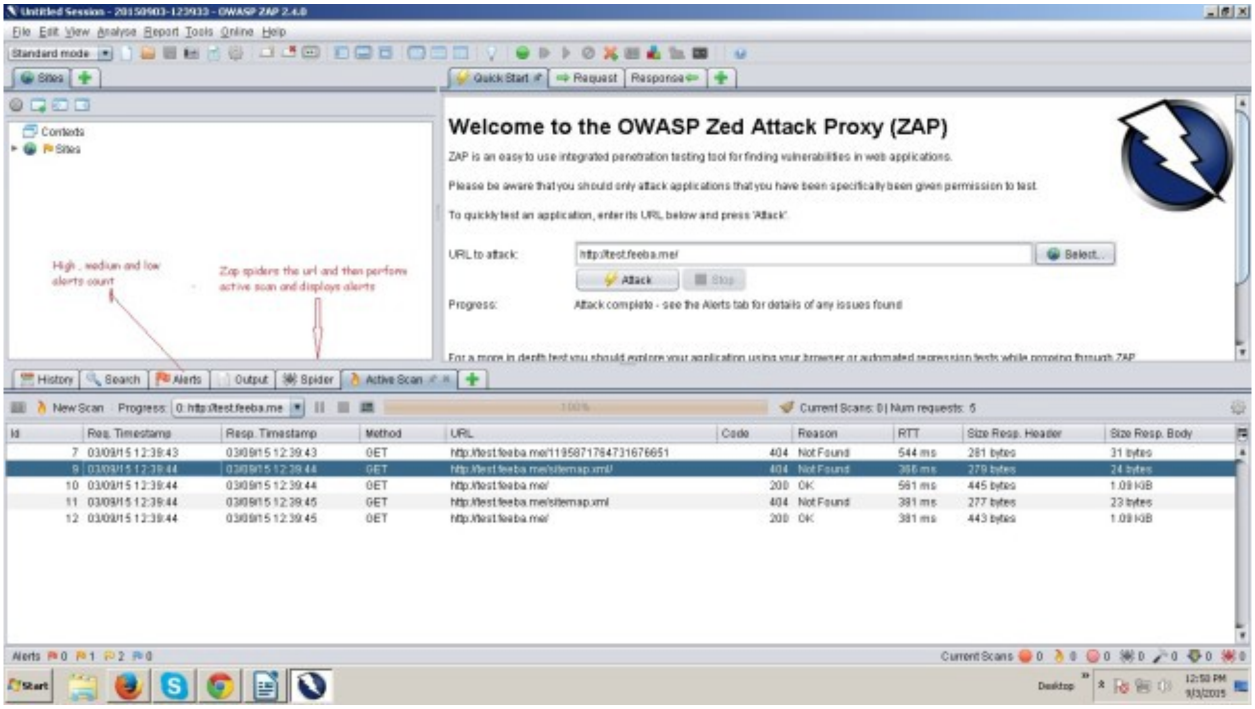
Recently I came across a tool, Zed Attack Proxy (ZAP). Its main goal is to allow easy penetration testing to find vulnerabilities in web applications. It is ideal for developers and functional testers as well as security experts. Let's check out how ZAP penetration testing works.

Installation and configuration of ZAP:

Download Link:
https://github.com/zaproxy/zaproxy/wiki/Downloads

Step1Adding a site to the testing scope

By telling ZAP what the target site is, ZAP can limit the scope of the scan and only scan the target site for vulnerabilities.
1. Open the web application that you want to test.
2. In Zap you will find your website/application displayed under sites. ZAP will spider that URL, then perform an active scan and display the results.



High , medium and low alerts count

Zap spiders the url and then perform active scan and displays alerts

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://test.feeba.me/

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 proxying through ZAP

Progress: 0: http://test.feeba.me

Current Scans: 0 | Num requests: 5

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
7	03/09/15 12:39:43	03/09/15 12:39:43	GET	http://test.feeba.me/1195871764731676651	404	Not Found	544 ms	281 bytes	31 bytes
9	03/09/15 12:39:44	03/09/15 12:39:44	GET	http://test.feeba.me/sitemap.xml/	404	Not Found	366 ms	279 bytes	24 bytes
10	03/09/15 12:39:44	03/09/15 12:39:44	GET	http://test.feeba.me/	200	OK	561 ms	445 bytes	1.09 KiB
11	03/09/15 12:39:44	03/09/15 12:39:45	GET	http://test.feeba.me/sitemap.xml	404	Not Found	381 ms	277 bytes	23 bytes
12	03/09/15 12:39:44	03/09/15 12:39:45	GET	http://test.feeba.me/	200	OK	381 ms	443 bytes	1.09 KiB

Zap runs on proxy, to set up the proxy in ZAP:

Close all active Firefox browser sessions
ZAP tool -> Tools Menu -> Options -> Local Proxy -> Change Address = 127.0.0.1 Port = 8080.
Mozilla browser -> Tools Menu -> Options -> Advanced tab -> Network -> Settings -> Select Manual Proxy configuration:- HTTP Proxy = 127.0.0.1 Port = 8080.

Now try to connect to your application using your browser.
If you can't connect to it then check your proxy settings again. You will need to check your browser's proxy settings, and ZAP's proxy settings. It's also worth checking that the application that you are trying to test is running!

When you have successfully connected to your application you will see one or more lines in ZAP's Sites and History tabs.
Note that most of ZAP's tabs provide additional functionality that could be accessed via 'right click' menus.

Right click on the HTML -> Attack -> Active scan
ZAP will perform active scan on all the pages and display the results.

Save the ZAP session

Once you have manually explored the application it would be a good time to save the ZAP session so that you can look at it again.
If your application has multiple roles then you should explore it with each role and save the sessions in separate files.

Generating a Report:

ZAP tool -> Report -> Generate HTML report (Any other options listed) -> Save and share the report.

Authentication , session and User management using ZAP

1) Context: Represents a Web application
2) Session Management Method: How are the web Sessions identified by the server and handle requests

Example: cookie based using query parameters
3) Authentication Method: How is a new session established?
It could be either Form based authentication method, HTTP based or oath methods.
4) User Management: Handling users of web application that could be used for executing actions
Example: user name/password pair

Steps to follow:

1. Set proxy in local browser/access url: https://pr-uat.iptquote.com Now include web app in context.

Read More at