Information Assurance & Auditing

4th Year - 1st Semester

Mid Assignment

Registration No – IT17094900

Name – Gunathunga P.I.N

Batch :CSN-WE

Abstract

In modern world auditing is very important process to give assurance to the IT systems are adequately protected and to provide reliable information to information technology. Every system begins using networks such as Internet. So, it is very important to audit networks to protect the system. We must audit our Information systems daily. Information Technology Auditing means examine and evaluate of an organization's information technology infrastructure, policies, and operations [1]. Management in the Organization must realize the need to ensure IT systems are reliable and secure from attacks. For an organization security is very important thing to concern. Because whole organization depends on their security infrastructure. Valuable data can be siphoned off for fraud or other illegal activities like treats. So, security measurements do a specific task to the organizations. That is why we should audit our Information system daily. Then we can safeguard our organization and can go to the targets easily.

Table of Contents

1. Introduction

In modern world Information Technology do a major role. Many systems based on the Information technology. Basically, Information technology combined with the data and information. We can analyze most of the Information technologies as web-based technologies. When we are analyzing the Information technology, web sites do a major role in all around. In the digital world, a website is crucial part for any organization. If an organization do not have a website, it can probably lose out on performance on the organization. So, we must keep the web site up and running with the security scenario. And we must monitor as well as regular audits to web sites.

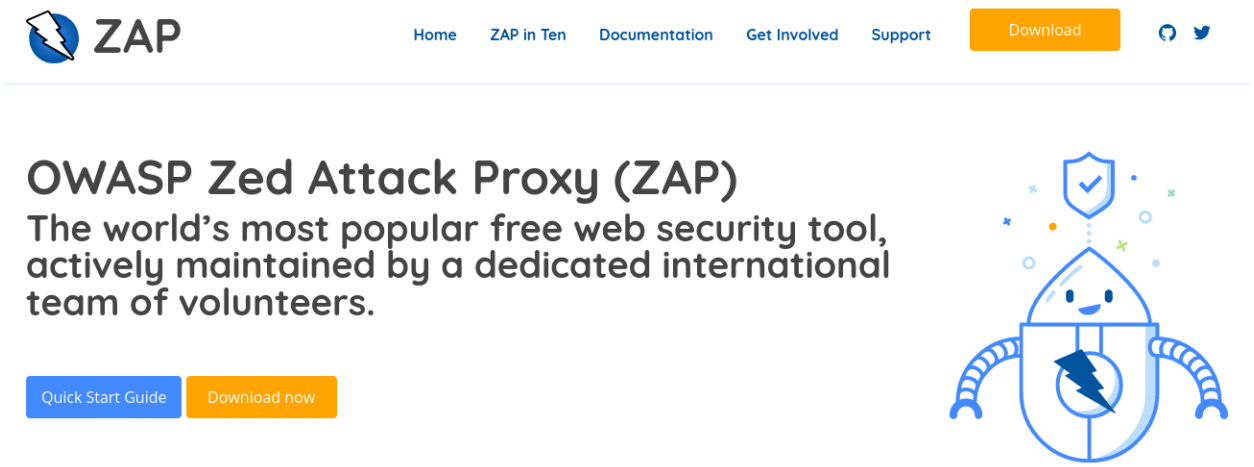
Website audit means the process of evaluating the search engine of a website in multiple areas and presenting the site's overall performance. It keeps growing and changing continuously. Web site audit is one of the most powerful activities an SEO to generate higher search visibility [2]. So, let us see why website auditing is important to an organization. Website audit process include: User engagement, User experience, Traffic, Functionality, Site health and Website performance [3]. By auditing we can ensure Proper User Experience, can optimize website performance, search engine optimization, it helps to find tags and functionalities, Conversion Rate Optimization and ensure data protection in website. And you can improve your site for the opportunity to rank. So, there are some elements requiring an audit. They are Site health audit, Site security audit, Conversion rate optimization audit, Google penalty and recovery audit, Competitor website audit and Content and SEO audit [2].

Now we discuss about the benefits of website auditing. There are some benefits by auditing our website.

1. To Keep Up with Changes in the Search Landscape.
2. To Optimize the Site Further.
3. To Identify New SEO Opportunities.
4. To Boost Conversions.

2. Introduction to OWASP Zed Attack Proxy (ZAP)

The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tool which is used for security testing. It is an open source project and is contributed to and maintained by OWASP. Zed Attack Proxy is a Java-based tool [5]. By using ZAP, you can find the security vulnerabilities in a web application. So, we can recommend it as a great tool for manual security testing. There are some security testing concepts and terminology included in this tool. When we talk about the Software security testing, it means the process of assessing and testing a system to identify security risks and vulnerabilities of the web site [4].

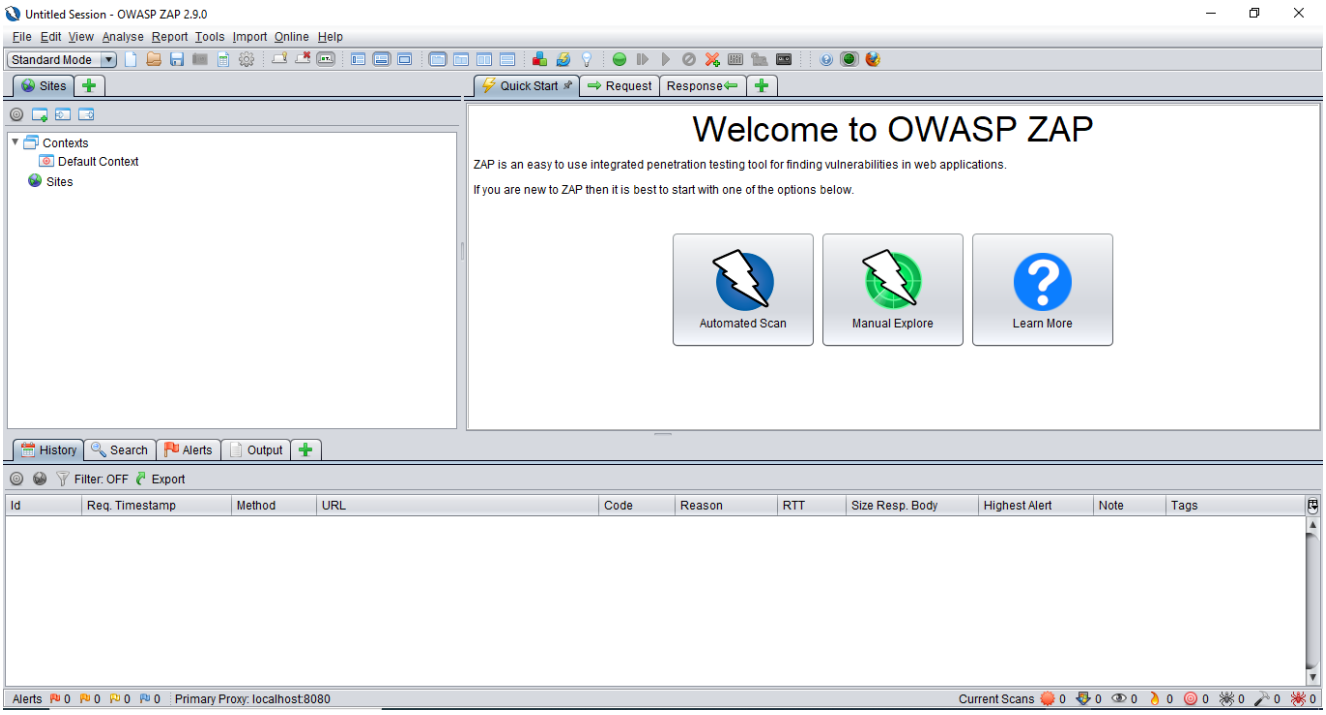


We can identify a common breakout structure in ZAP proxy server as follows.

- Vulnerability Assessment – scan and analysis for security issues.
- Penetration Testing – analysis and attack from simulated malicious attackers.
- Runtime Testing – analysis and security testing from an end-user.
- Code Review – give detailed review and analysis of the security vulnerabilities.

When installing ZAP proxy server, it requires JDK run environment and web browser (Google Chrome or Firefox).

After the installation we can run the ZAP proxy server.



ZAP home page

Now let us see about the GUI of the ZAP proxy server.

- **Left Section**

It shows the "Context" and "Sites" buttons. In here multiple websites can be targeted for scan under sites. For a special website must be specified under the "Context" section [5].

- **Right Section**

In here we can see two types called Automated Scan and Manual Explore. And it provided with a URL section for the target for scanning. From the "Attack" button can the attack on the target and the "Stop" button can stop the attack for scan. In manual explore security tester might be interested websites for vulnerabilities. And ZAP allows to launch the browser of choice with the loaded URL in manual explore. It can be achieved by clicking "Launch Browser" [5].

- **Bottom Section**

This section contains six tabs called History, Search, Alerts and Output. Detected issues are still logged and sent onto the bottom section. And history tab displays the tested activities [5].

3. Auditing Lankasathosa.lk Using ZAP proxy server

So, lets audit lankasathosa.lk site using ZAP and see the vulnerabilities it found.

1. Run the ZAP tool. Then we can see the GUI.

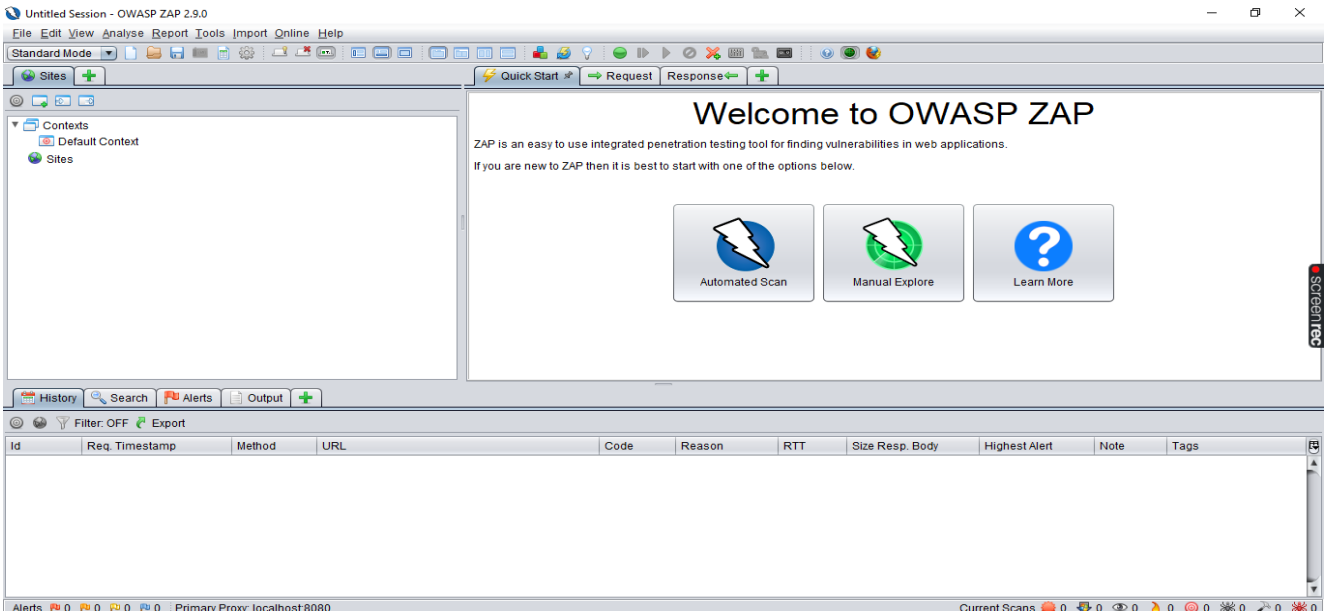


Figure 1

2. Click Manual Explore and type the URL that we want to audit. And choose the browser and click launch.

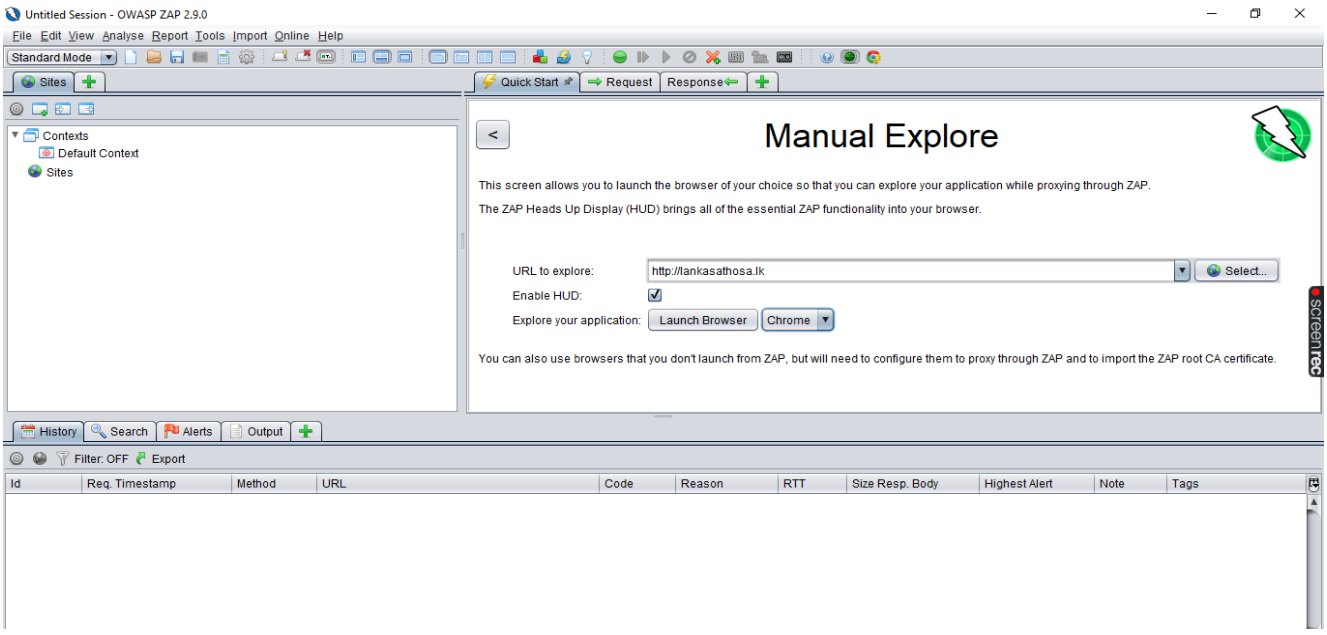


Figure 2

3. Then it will launch the web page and select Active scan and click start.

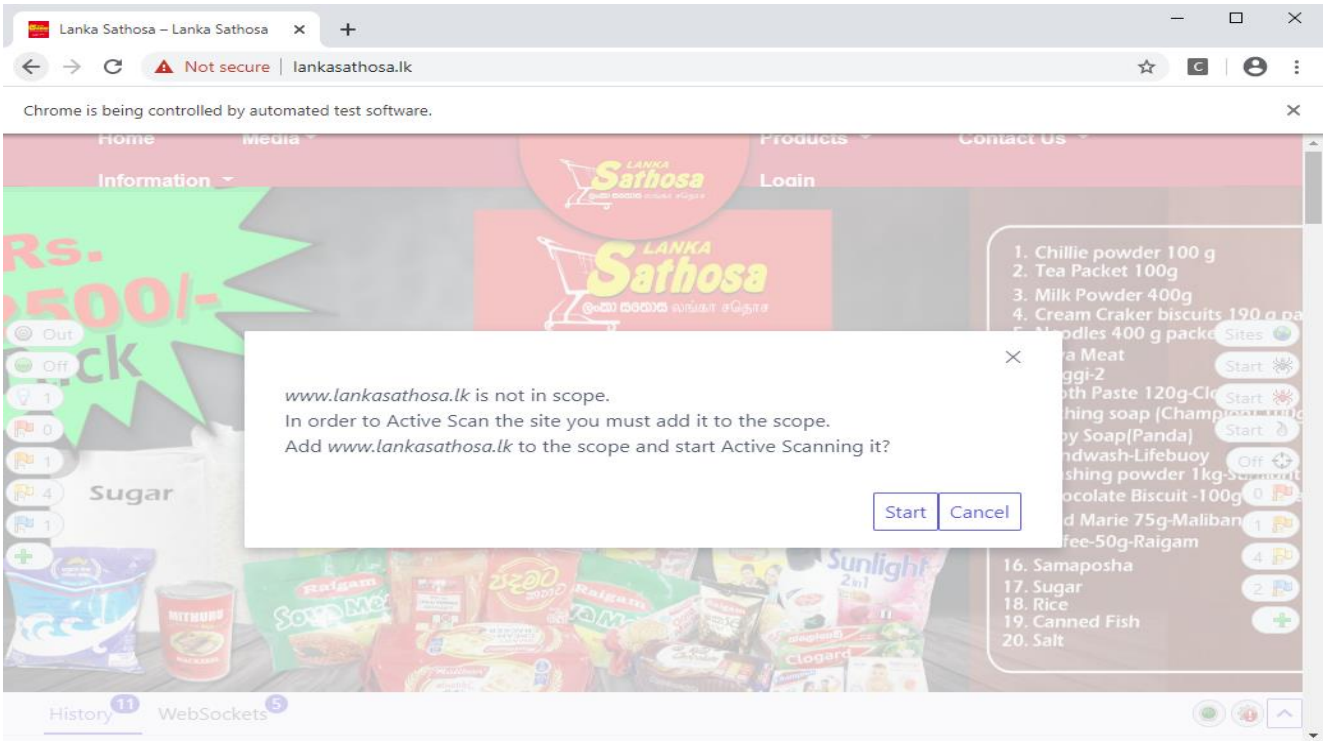


Figure 3

4. Then go to the ZAP server again and we can see the scan is started.

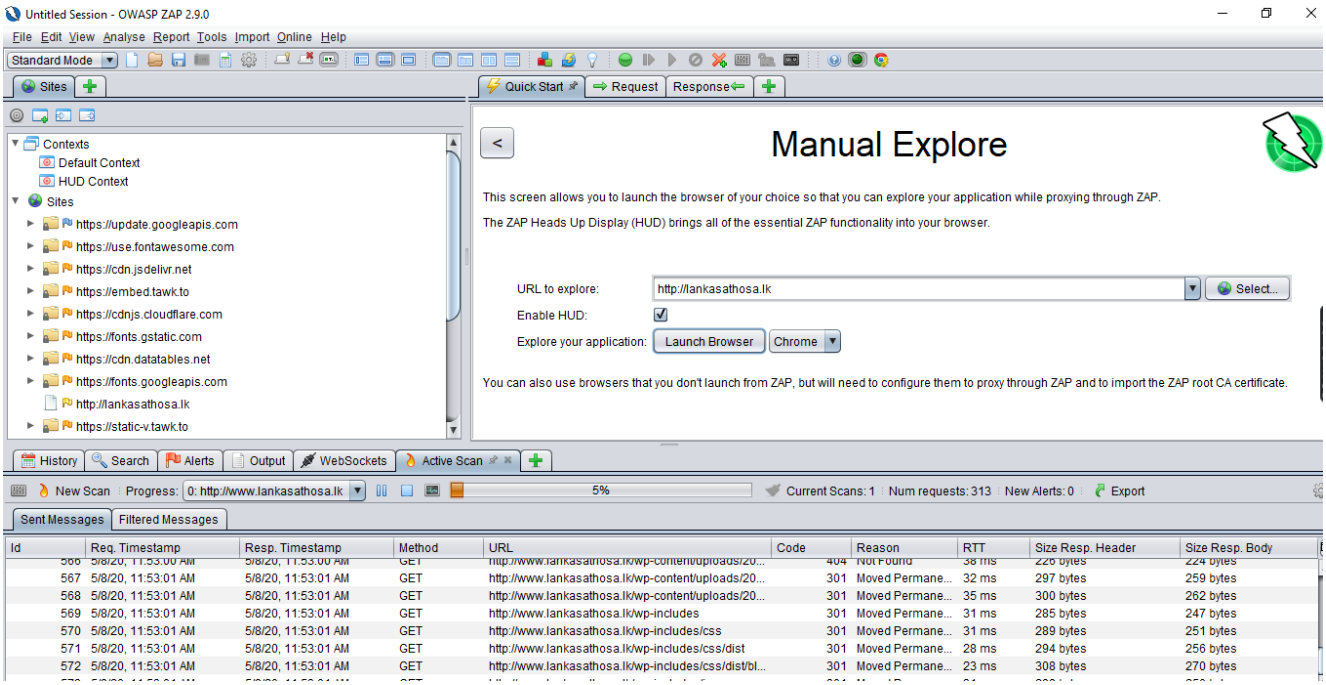


Figure 4

5. After scan finished, we can see the vulnerabilities in the Alerts tab.

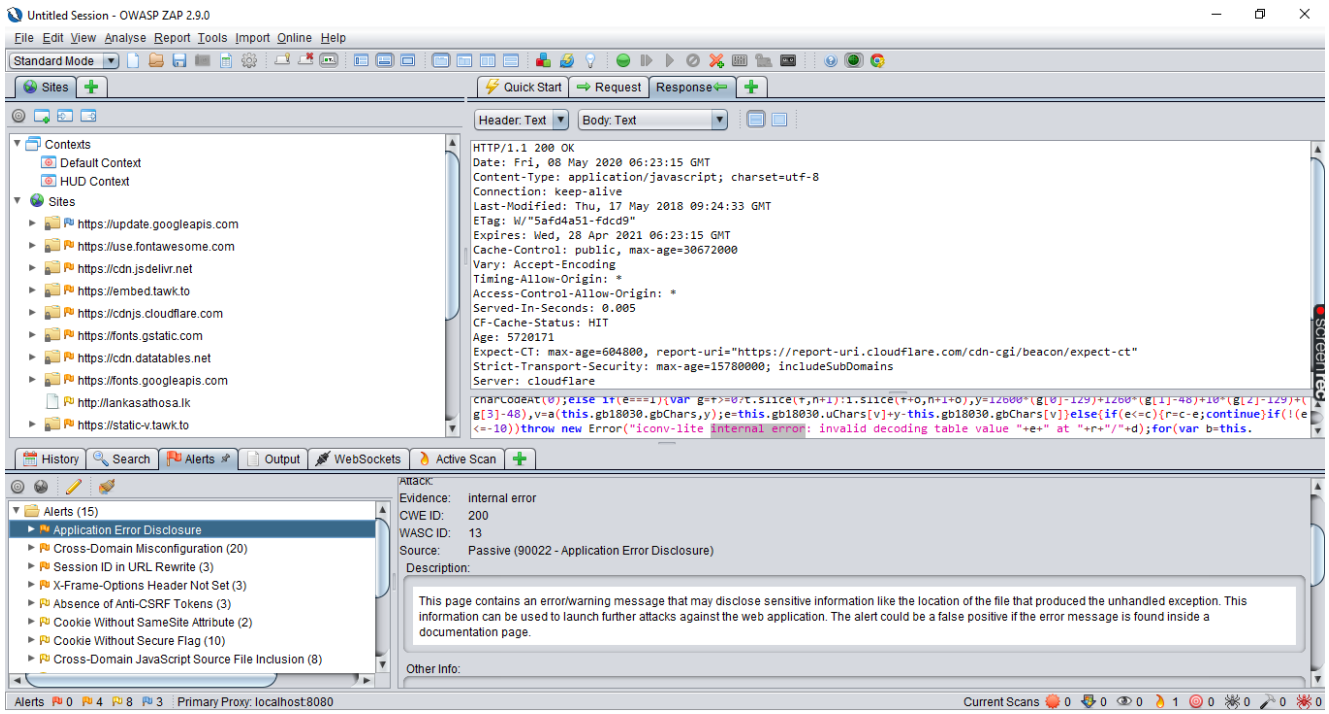


Figure 5

By clicking an alerts we can see the details such as problem level, description, solutions, references… etc.

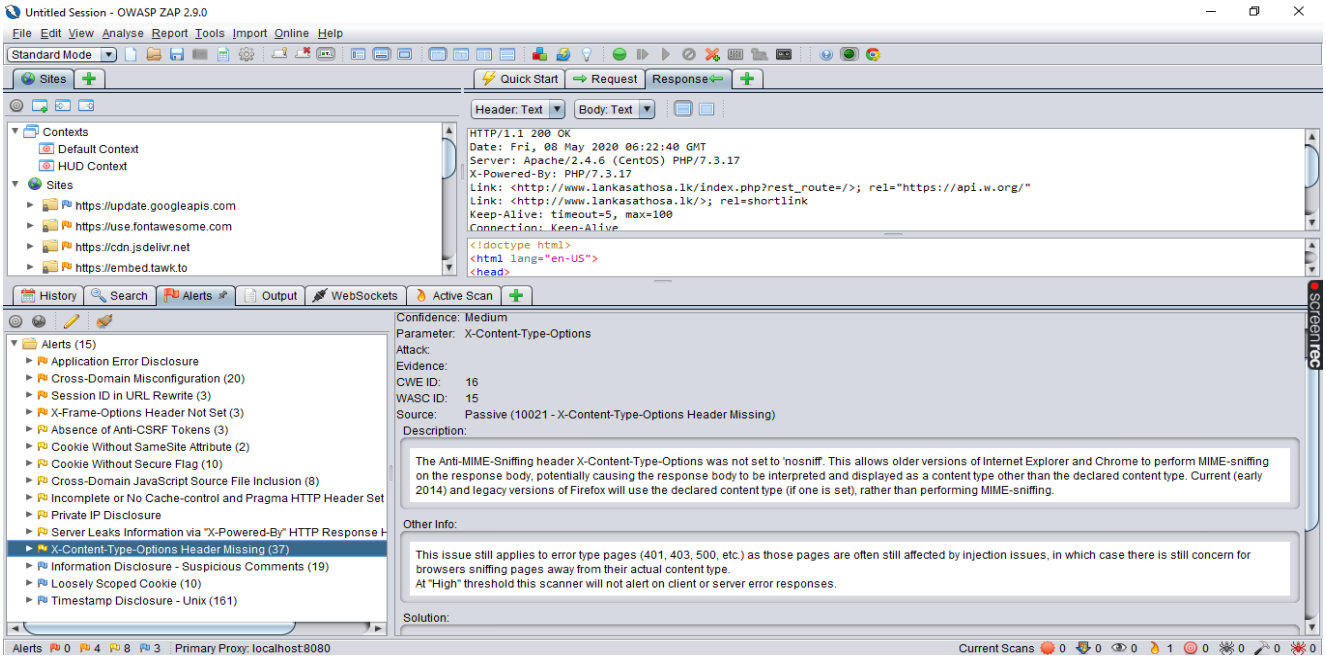


Figure 6

6. In active scan tab, we can see the progress and Response chart in our scanning.

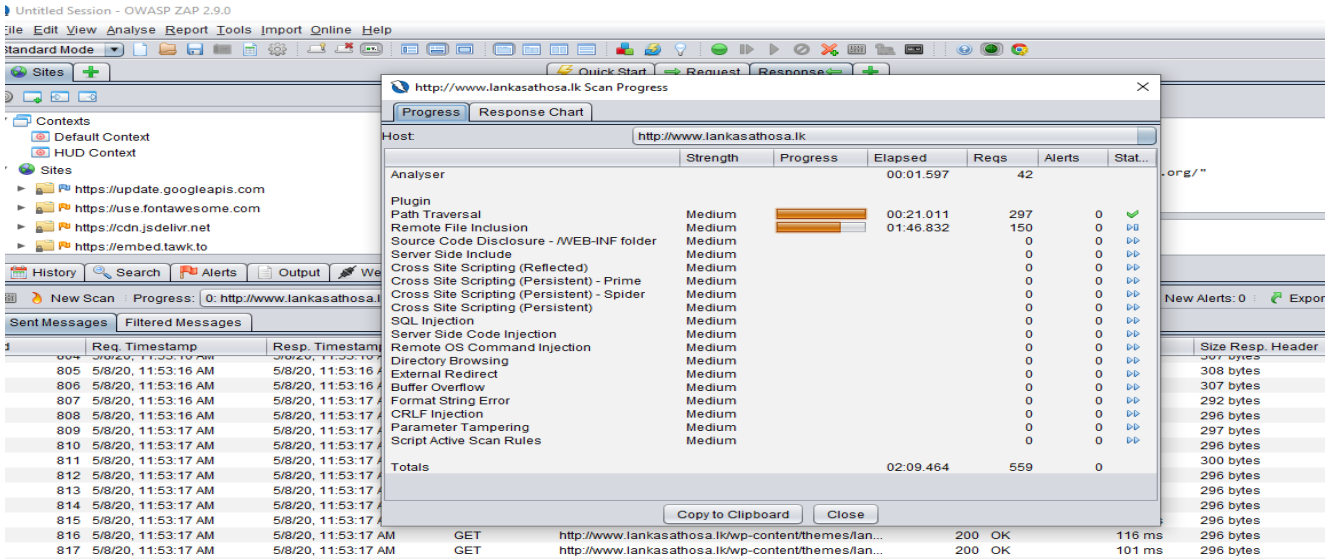


Figure 7

7. Then go to report tab and select the report type. In my case I selected the html report. And you can save it.

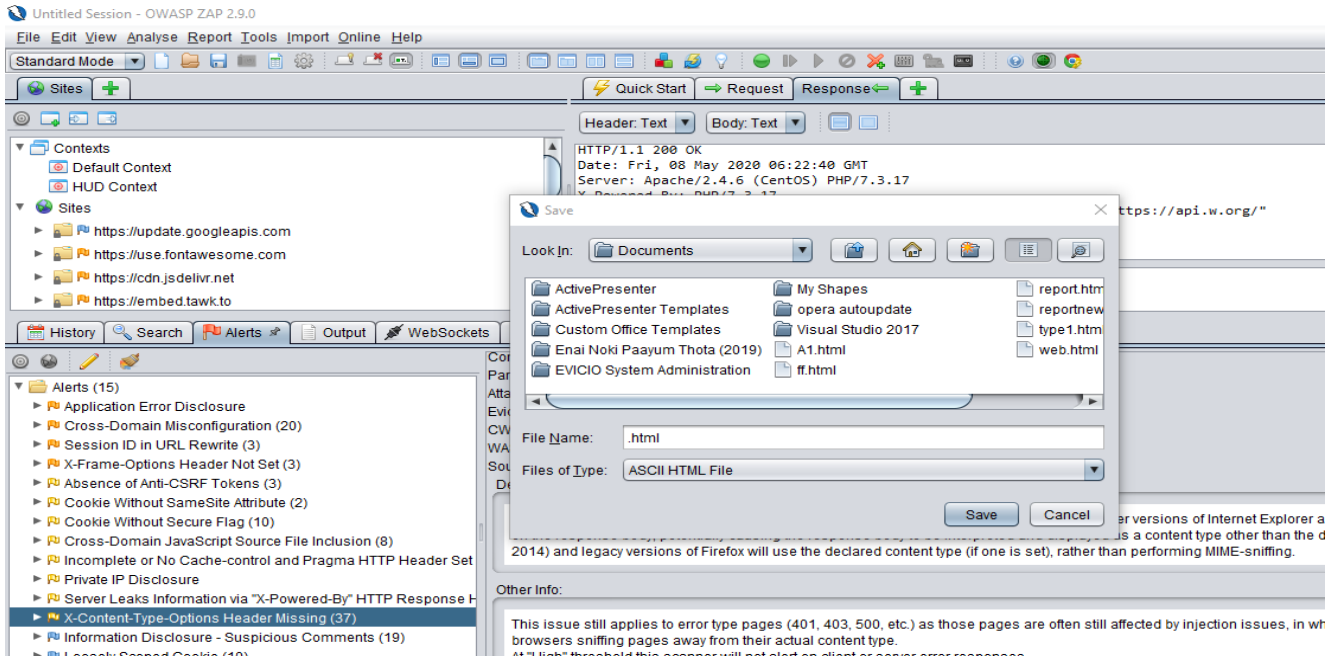
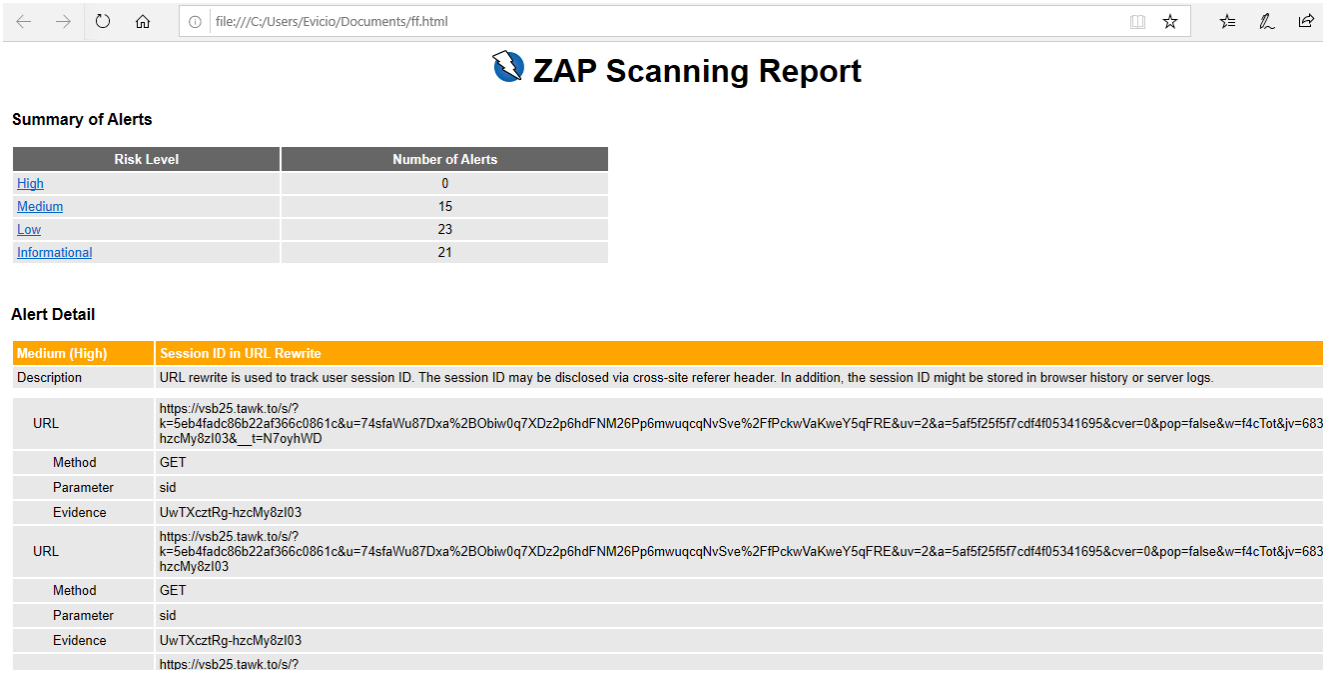


Figure 8

8. Then launch the ZAP report and we can see all the details in here as follows.



file:///C:/Users/Evicio/Documents/ff.html

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	15
Low	23
Informational	21

Alert Detail

Medium (High)	Session ID in URL Rewrite
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	https://vsb25.tawk.to/s/?k=5eb4fadc86b22af366c0861c&u=74sfaWu87Dxa%2BObiw0q7XDz2p6hdFNM26Pp6mwuqcqNvSve%2FfPckwVaKweY5qFRE&uv=2&a=5af5f25f5f7cdf4f05341695&cver=0&pop=false&w=f4cTot&jv=683hzcMy8zI03&__t=N7oyhWD
Method	GET
Parameter	sid
Evidence	UwTXcztRg-hzcMy8zI03
URL	https://vsb25.tawk.to/s/?k=5eb4fadc86b22af366c0861c&u=74sfaWu87Dxa%2BObiw0q7XDz2p6hdFNM26Pp6mwuqcqNvSve%2FfPckwVaKweY5qFRE&uv=2&a=5af5f25f5f7cdf4f05341695&cver=0&pop=false&w=f4cTot&jv=683hzcMy8zI03
Method	GET
Parameter	sid
Evidence	UwTXcztRg-hzcMy8zI03
	https://vsb25.tawk.to/s/?

Figure 9

4. Problem Identification

After the web scan in lankasathosa.lk, We can see there are 15 alerts. They are 4 medium priority alerts, 8 low priority alerts and 4 Informational alerts. We can list them as follows.

- **Medium Priority Alerts**
    1. Application Error Disclosure
    2. Cross-Domain Misconfiguration
    3. Session ID in URL Rewrite
    4. X-Frame-Options Header Not Set

- **Low Priority Alerts**
    1. Absence of Anti-CSRF Tokens
    2. Cookie Without SameSite Attribute
    3. Cookie Without Secure Flag
    4. Cross-Domain JavaScript Source File Inclusion
    5. Incomplete or No Cache-control and Pragma HTTP Header Set
    6. Private IP Disclosure
    7. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
    8. X-Content-Type-Options Header Missing

- **Informational Priority Alerts**

    1. Information Disclosure - Suspicious Comments
    2. Loosely Scoped Cookie
    3. Timestamp Disclosure - Unix

5. Conclusion and Recommendation

The best way to conduct regular audits, we can keep the site safe and less risky by monitoring websites regularly. So, we can minimize and identify the risk and can expect a higher performance for websites. There are number of tools it audits in nowadays. Zed Attack Proxy (ZAP) is a free, open-source website security testing tool developed by the Open Web Application Security Project (OWASP). ZAP is designed specifically for auditing web applications. And we can describe ZAP as a man-in-the-middle proxy. ZAP provides functionality for a range of skill levels. For example, developers, to testers new to security testing. When Scanning using ZAP, it represents the alerts messages for the site with brief details. It presents the proposed solutions and reference as well. Then anyone can volunteer to work on ZAP to fix bugs, add features, create, and control requests and other security tastings easily.

6. References

[1]"What is IT audit (information technology audit)? - Definition from WhatIs.com", SearchCompliance. [Online]. Available: https://searchcompliance.techtarget.com/definition/IT-audit-information-technology-audit. [Accessed: 06- May- 2020].

[2]K. Guard, "What is a Site Audit?", seoClarity. [Online]. Available: https://www.seoclarity.net/resources/knowledgebase/what-is-a-site-audit. [Accessed: 06- May- 2020].

[3]"What is a Website Audit and Why is it Necessary in 2019?", Pedestal. [Online]. Available: https://pedestalsearch.com/what-is-website-audit-why-necessary/. [Accessed: 06- May- 2020].

[4]"OWASP ZAP – Getting Started", Zaproxy.org. [Online]. Available: https://www.zaproxy.org/getting-started/. [Accessed: 06- May- 2020].

[5]"Introduction to OWASP ZAP for Web Application Security Assessments", Infosec Resources. [Online]. Available: https://resources.infosecinstitute.com/introduction-owasp-zap-web-application-security-assessments/#gref. [Accessed: 06- May- 2020].