Information Assurance and Auditing – IE4040

4th Year, 1st Semester

Mid Term Individual Assignment – 2020

Submitted to

Sri Lanka Institute of information Technology

Student Registration Number	Student Name with Initials
IT17007016	C.S. Wijesinghe

In partial fulfillment of the requirement for the

Bachelor of Science Special Honors Degree in Information Technology

Abstract

This is the era that information technology is a most important part of the daily life. In every service that man has, depend on the information technology. When we using an Information technology system, we has to audit the system that we used daily. [5] IT auditing is the examination and evaluation of an organization's information technology infrastructure, policies and operations [5]. As well as every IT auditor, there were certain major aspects to concern about.

For a company, organization or personnel activities, security is very important thing to concern. Because in every organization, there are sensitive data, critical sections and other things may use to illegal activities. If there were, any vulnerability of the system may lead to use those tings illegally. Therefore, company must take relevant security measures before anything illegal happened. That is why these tools build to identify those things and make the network, system or website better place

Contents

1. Introduction

These are the days that Information Technology is an essential part of a human life. Now days, information is a very factor in every field. With the development of the information technology, using of information also increase. Later with the arrival of internet, people will share information with remote users. Then website are created as GUI **(Graphic User Interface)** to access information through the internet. [1] A website is a collection of public accessible, interlinked Web pages that share a single domain name. They can create and maintain as individual or by a group of members or as an organizational manner. However, every public accessible websites are constitute to the **World Wide Web**. There are vast number of verities include in websites. Educational, News, Forum, social media and more. Within a website, media and other text are mixed-up. That is because there are no limits in form of websites. Therefore, any person can create a website as he wish to create it [1].

Therefore, we must make sure maintain website very well to improve the performance of the website and maintain it further. For that, we have to do an audit on website. [2] A website audit is an examination of page performance prior to large-scale **Search Engine Optimization (SEO)** or a website redesign. By auditing, we can determine our website whether optimized to handle good traffic or how to improve my website performance to that level. You can get several benefits by auditing the website. They are,

- **Optimization of Performance of the website**
  Web audit evaluate both technical performance as well as its contents. Therefore, audit will inspect the strength of your website's technical framework and infrastructures check whether how the website will work smoothly with search engine and more.

- **Optimization of the Search Engine**
  You can able to find any missed search engine optimization and action that take place to correct the misguided or poorly executed risks.

- **Optimization Conversion Rate**
  Website audit enable the effectiveness of the website. Therefore, you can spot any previously overlooked opportunities to convert visitors into leads so you can add relevant CTAs [2].

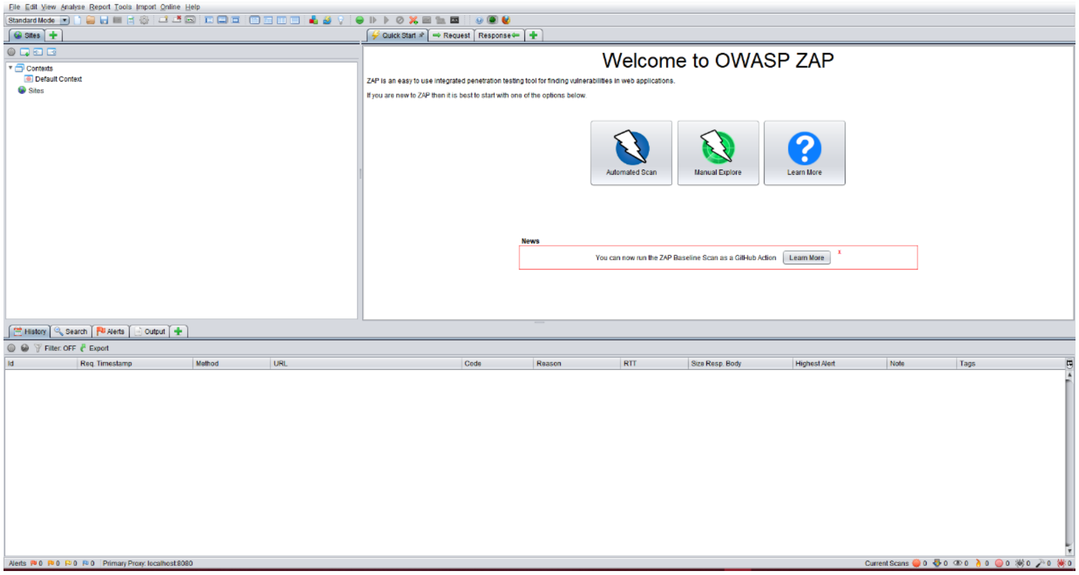
2. Overview OWASP Zap Audit tool

OWASP Zap audit is the tool we used in this auditing scenario. The OWASP foundation is the developer on this tool. They are an organization, which work to improve the security of software through open source software projects. [6]This is based on java with user-friendly interface that help to allow the web application security testers to perform fuzzing, scripting, spidering and proxying to attack the web apps. Because this is a java tool, this tool run in many operating systems. In **Kali Linux**, Zap is a default tool.

[3]This is a **proxy server**, which allow the users to manipulate the traffic that passes through it. Even https traffic. It can run in a daemon mode also that controlled via **REST API** [3]. Paros penetration tool also may help to make this tool.

There are several built-in feature will see. [4]Some of them are,

- Intercepting proxy server
- Traditional and AJAX Web crawlers
- Automated scanner and Passive scanner
- Forced browsing
- Web Socket support and Scripting languages
- Plug-n-Hack support



Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

You can now run the ZAP Baseline Scan as a GitHub Action

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags

Primary Proxy: localhost:8080

Figure 2. 1

3. GUI Overview of ZAP

When we open the ZAP, GUI has three major sections.

- **Left section**
  This section shows the **Context** and **Sites** dropdown buttons. When you have to scan multiple sites, they are appear under the Sites dropdown. However, when there were specific website that interest, it must be specified under Context section.

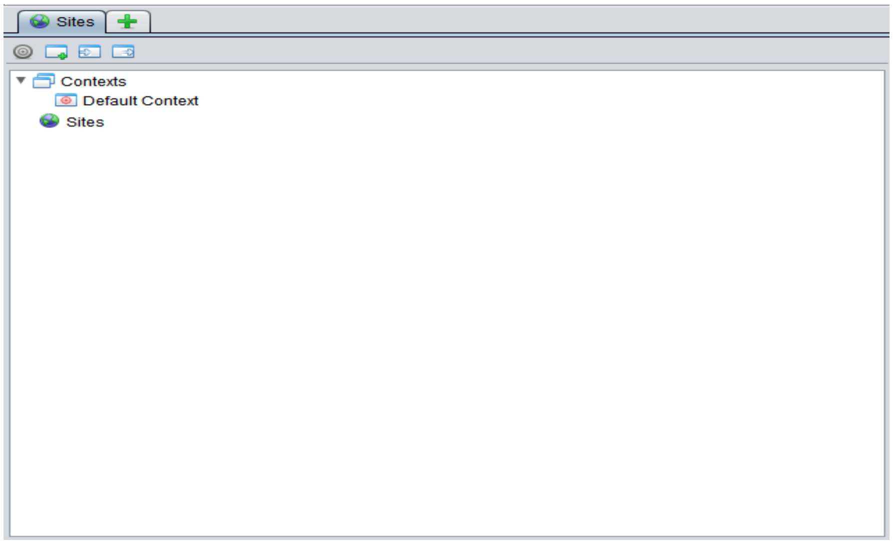
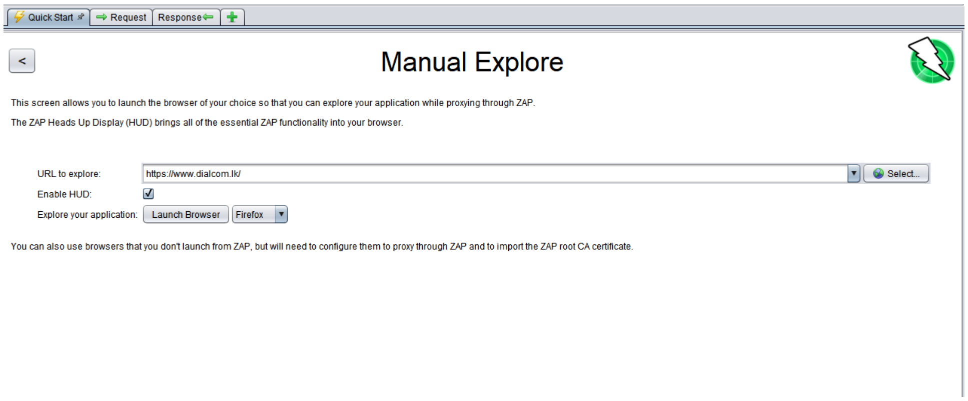


Figure 3. 1

- **Right Section**
  This is the section where we provide URL when we specify the target foe scanning or we can enter the saved site by clicking select button. Then there is a dropdown to select the browser, which we want to run the website. We can select the browser as wish. The **Launch Browser** button is used to start the action.



Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: https://www.dialcom.lk/ Select...

Enable HUD: ☑

Explore your application: Launch Browser Firefox

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

Figure 3. 2

- **Bottom Section**
  This section contain four tabs that showing actions by default three tabs. They are **History** tab, **Search** tab, **Alerts** tab. Further, you can add tabs like **Active Scan** tab, **Spider** tabs when you use those scans and tools in audit. The **History** tab display the websites that we tested. You can see that in figure 3 3

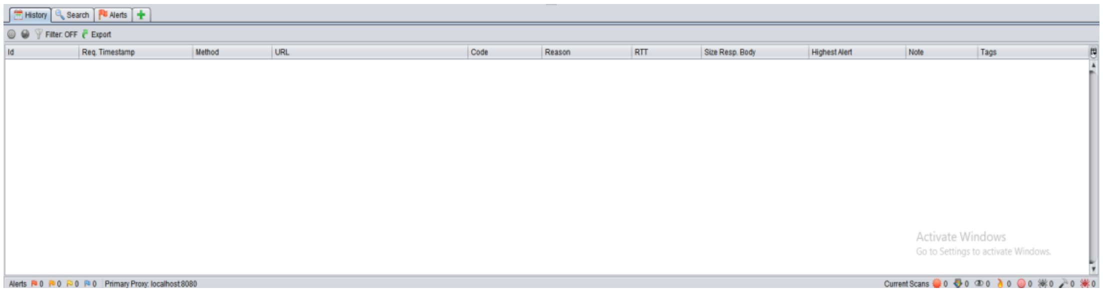
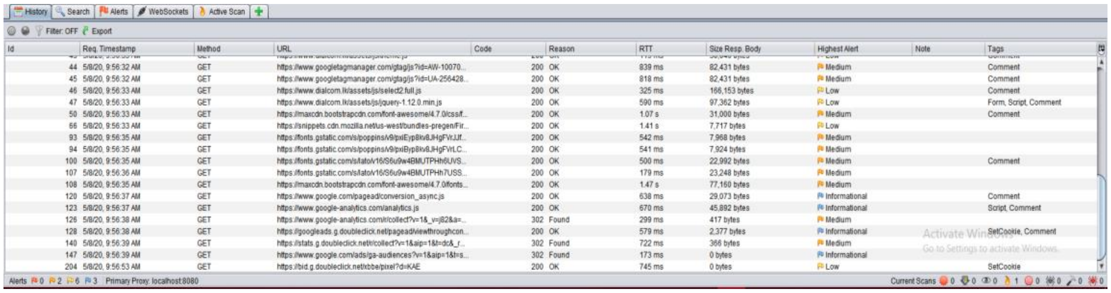


Figure 3. 3


History
Search
Alerts
WebSockets
Active Scan
Filter: OFF
Export
Alerts 0 2 6 3 Primary Proxy: localhost:8080
Current Scans 0 0 0 1 0 0 0 0
Activate Windows
Go to Settings to activate Windows.

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
44	5/8/20, 9:56:32 AM	GET	https://www.googletagmanager.com/gtag/js?id=AW-10070...	200	OK	839 ms	82,431 bytes	Medium		Comment
45	5/8/20, 9:56:32 AM	GET	https://www.googletagmanager.com/gtag/js?id=UA-256428...	200	OK	818 ms	82,431 bytes	Medium		Comment
46	5/8/20, 9:56:33 AM	GET	https://www.dialcom.lk/assets/js/select2.full.js	200	OK	325 ms	166,153 bytes	Low		Comment
47	5/8/20, 9:56:33 AM	GET	https://www.dialcom.lk/assets/js/jquery-1.12.0.min.js	200	OK	590 ms	97,362 bytes	Low		Form, Script, Comment
50	5/8/20, 9:56:33 AM	GET	https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/f...	200	OK	1.07 s	31,000 bytes	Medium		Comment
66	5/8/20, 9:56:33 AM	GET	https://snippets.cdn.mozilla.net/us-west/bundles-pregen/Fir...	200	OK	1.41 s	7,717 bytes	Low		
93	5/8/20, 9:56:35 AM	GET	https://fonts.gstatic.com/s/poppins/v9/pxiEyp8kv8JHgFVrJJf...	200	OK	542 ms	7,968 bytes	Medium		
94	5/8/20, 9:56:35 AM	GET	https://fonts.gstatic.com/s/poppins/v9/pxiByp8kv8JHgFVrLC...	200	OK	541 ms	7,924 bytes	Medium		
100	5/8/20, 9:56:35 AM	GET	https://fonts.gstatic.com/s/lato/v16/S6u9w4BMUTPHh6UVS...	200	OK	500 ms	22,992 bytes	Medium		Comment
107	5/8/20, 9:56:36 AM	GET	https://fonts.gstatic.com/s/lato/v16/S6u9w4BMUTPHh7USS...	200	OK	179 ms	23,248 bytes	Medium		
108	5/8/20, 9:56:35 AM	GET	https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts...	200	OK	1.47 s	77,160 bytes	Medium		
120	5/8/20, 9:56:37 AM	GET	https://www.google.com/pagead/conversion_async.js	200	OK	638 ms	29,073 bytes	Informational		Comment
123	5/8/20, 9:56:37 AM	GET	https://www.google-analytics.com/analytics.js	200	OK	670 ms	45,892 bytes	Informational		Script, Comment
126	5/8/20, 9:56:38 AM	GET	https://www.google-analytics.com/r/collect?v=1&_v=j82&a=...	302	Found	299 ms	417 bytes	Medium		
128	5/8/20, 9:56:38 AM	GET	https://googleads.g.doubleclick.net/pagead/viewthroughcon...	200	OK	579 ms	2,377 bytes	Informational		SetCookie, Comment
140	5/8/20, 9:56:39 AM	GET	https://stats.g.doubleclick.net/r/collect?v=1&aip=1&t=dc&_r...	302	Found	722 ms	366 bytes	Medium		
147	5/8/20, 9:56:39 AM	GET	https://www.google.com/ads/ga-audiences?v=1&aip=1&t=s...	302	Found	173 ms	0 bytes	Informational		
204	5/8/20, 9:56:53 AM	GET	https://bid.g.doubleclick.net/xbbe/pixel?d=KAE	200	OK	745 ms	0 bytes	Low		SetCookie

Figure 3. 4

The Search tab display the patterns that you want to find. When you type the thing that you want to find in the scanning process, you can them display in this section. Figure 3.4 will that.

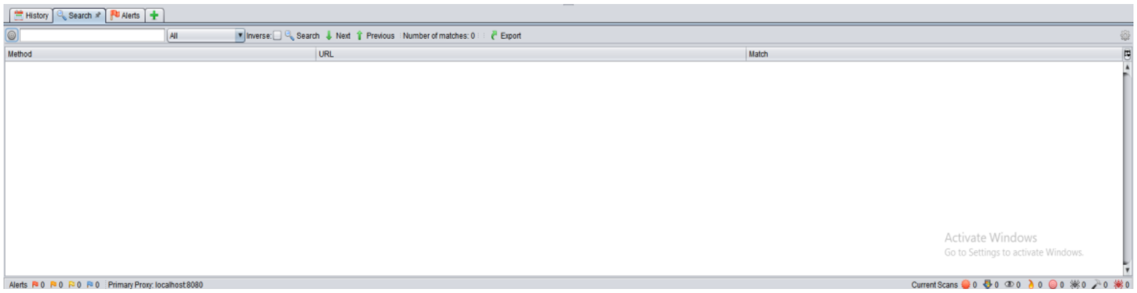
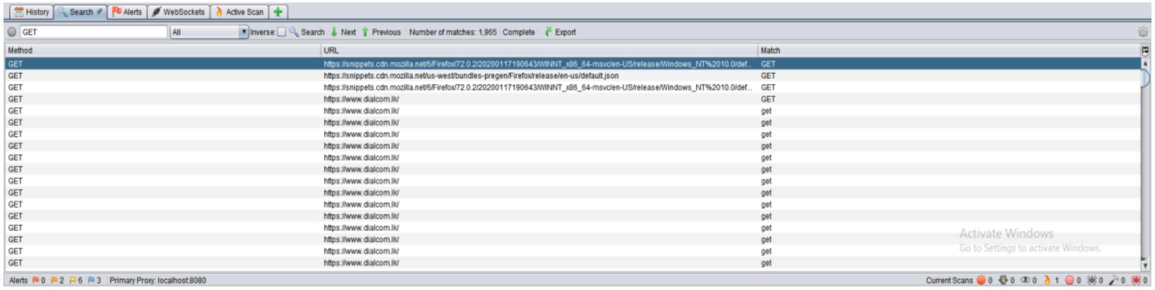

History
Search
Alerts
All
Inverse: □
Search
Next
Previous
Number of matches: 0
Export
Method
URL
Match
Alerts 0 0 0 0 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0
Activate Windows
Go to Settings to activate Windows.

Figure 3. 5

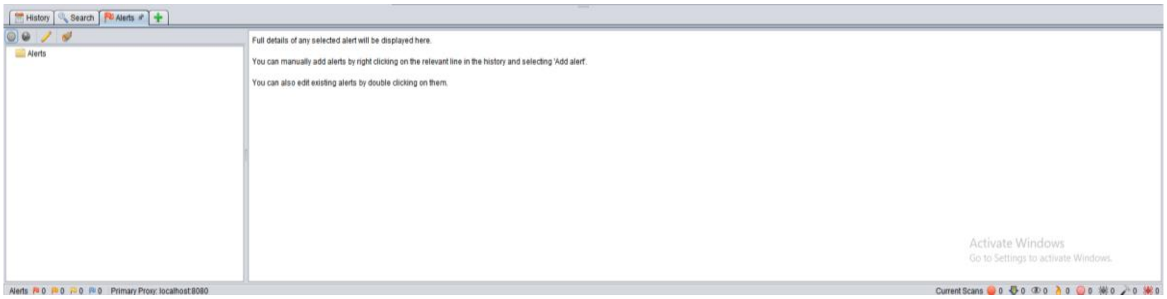


Method	URL	Match
GET	https://snippets.cdn.mozilla.net/6/Firefox/72.0.2/20200117190643/WINNT_x86_64-msvc/en-US/release/Windows_NT%2010.0/def...	GET
GET	https://snippets.cdn.mozilla.net/us-west/bundles-pregen/Firefox/release/en-us/default.json	GET
GET	https://snippets.cdn.mozilla.net/6/Firefox/72.0.2/20200117190643/WINNT_x86_64-msvc/en-US/release/Windows_NT%2010.0/def...	GET
GET	https://www.dialcom.lk/	GET
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get
GET	https://www.dialcom.lk/	get

Activate Windows
Go to Settings to activate Windows.
Alerts 0 2 6 3
Primary Proxy: localhost:8080
Current Scans 0 0 0 1 0 0 0 0

Figure 3. 6

The Alert tab gives you more information about the vulnerabilities that discover within the scan of the website. You can identify the issues according to strength of the issue. If the flag of the issue is Shaded Red that mean it is High risk. If the flag is Shaded Orange that mean the risk is medium. If the flag is Yellow, then is a low risk. Figure 3.5 will show that.



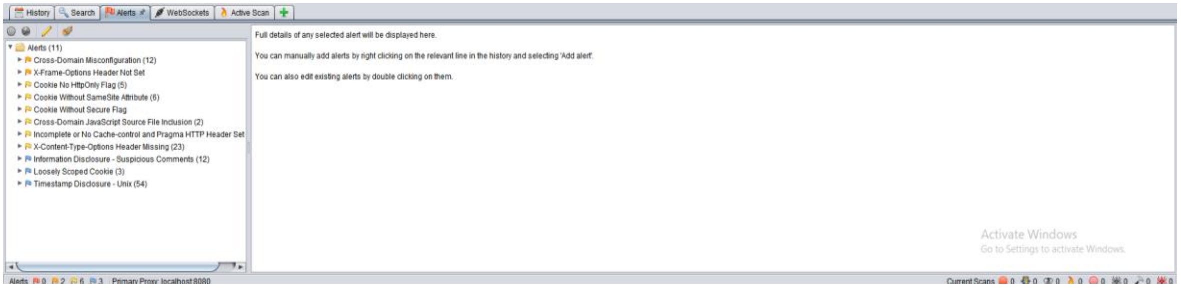
History
Search
Alerts
Alerts
Activate Windows
Go to Settings to activate Windows.
Alerts 0 0 0 0
Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Figure 3. 7



History
Search
Alerts
WebSockets
Active Scan
Activate Windows
Go to Settings to activate Windows.
Alerts 0 2 6 3
Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

- Alerts (11)
  - Cross-Domain Misconfiguration (12)
  - X-Frame-Options Header Not Set
  - Cookie No HttpOnly Flag (5)
  - Cookie Without SameSite Attribute (6)
  - Cookie Without Secure Flag
  - Cross-Domain JavaScript Source File Inclusion (2)
  - Incomplete or No Cache-control and Pragma HTTP Header Set
  - X-Content-Type-Options Header Missing (23)
  - Information Disclosure - Suspicious Comments (12)
  - Loosely Scoped Cookie (3)
  - Timestamp Disclosure - Unix (54)

Full details of any selected alert will be displayed here.

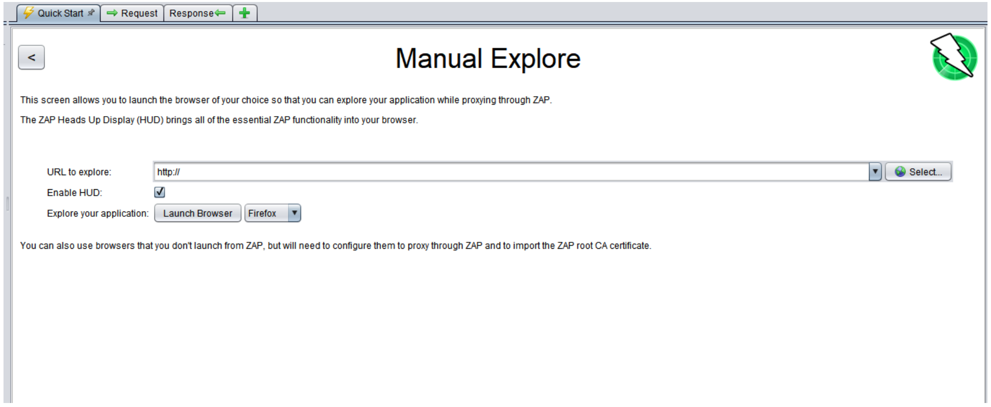
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Figure 3. 8

4. Step to do the Scan of the website

After we start the OWASP ZAP, we have to select whether we are doing automate explore or manual explore. In this case I am doing manual explore. So we click the manual explore button to start the website scan. Then you will prompt a window as figure 4.1.



Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: http://

Enable HUD: ☑

Explore your application: Launch Browser | Firefox

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

Figure 4. 1

In this window, you have to enter the URL of the website that you are going to audit in **URL to explore** dropbox. It will save all the URL that you audited. Then you can select the browser that your website willing to open in the scanning process. You can choose any web browser that install in your system. After that just click the **Launch Browser** button to start the audit.

Then web browser gets started and you will see popup window display in the web browser as Figure 4.2. In that, window select **continue on your target** to start the audit.

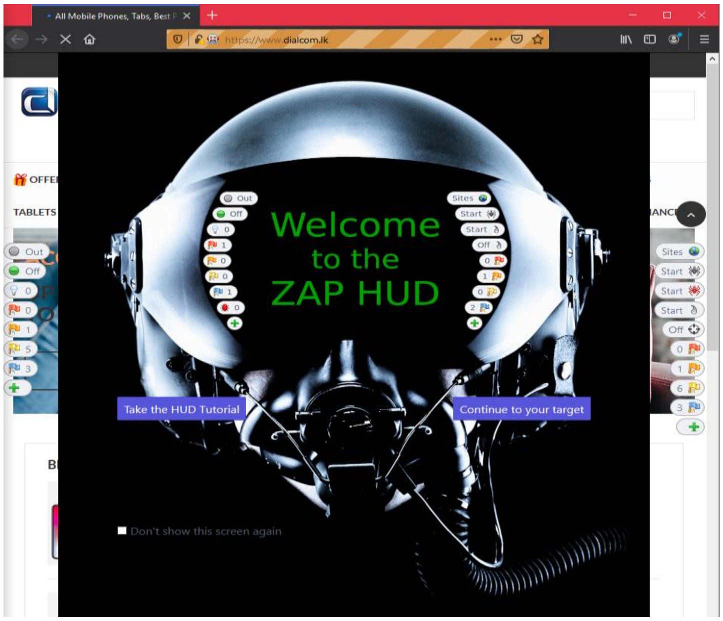


Figure 4. 2

After that, you will see the relevant website that we scan and audit. In the web page, you will notice some labels are popup. They indicate the some issues in the webpage and website as well as option of scans that can do to the website.

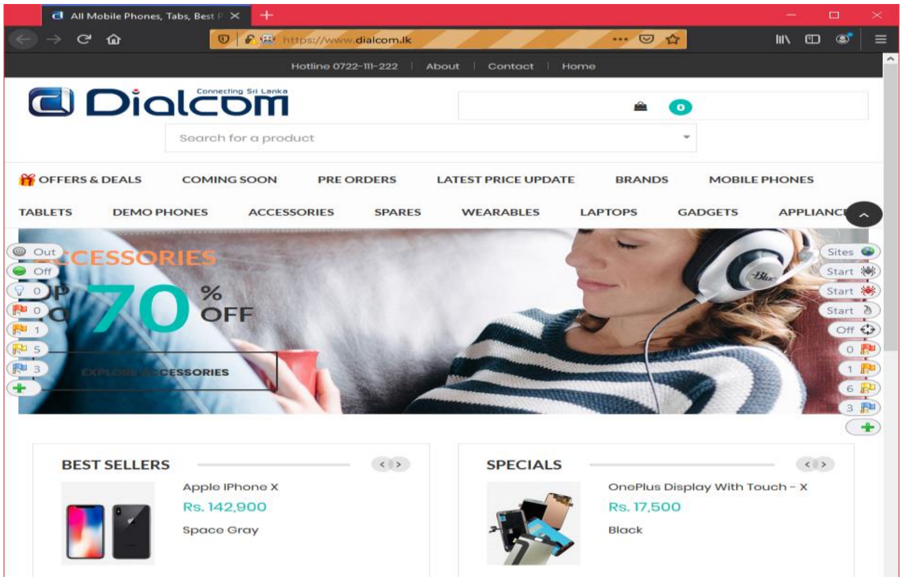
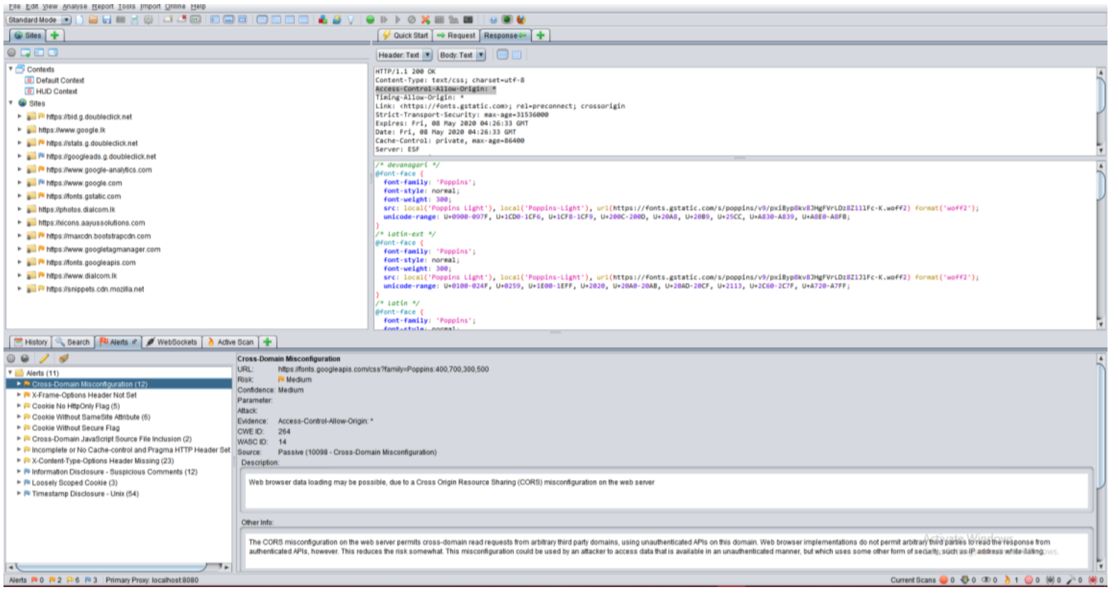


Figure 4. 3

While loading this website, you can notice ZAP tool will run the audit in GUI. You can notice History tab, Alerts tab running while this process running. In figure 3.4 and figure 3.8, you will see those tabs are running.

After all issues shows in the alert tab, we can examine those issues one by one. When you just click on one of those alerts, you will get the details of that issue, even the source codes of that context.


File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
HUD Context
Sites
https://bid.g.doubleclick.net
https://www.google.lk
https://stats.g.doubleclick.net
https://googleads.g.doubleclick.net
https://www.google-analytics.com
https://www.google.com
https://fonts.gstatic.com
https://photos.dialcom.lk
https://icons.aayussolutions.com
https://maxcdn.bootstrapcdn.com
https://www.googletagmanager.com
https://fonts.googleapis.com
https://www.dialcom.lk
https://snippets.cdn.mozilla.net
History
Search
Alerts
WebSockets
Active Scan
Alerts (11)
Cross-Domain Misconfiguration (12)
X-Frame-Options Header Not Set
Cookie No HttpOnly Flag (5)
Cookie Without SameSite Attribute (6)
Cookie Without Secure Flag
Cross-Domain JavaScript Source File Inclusion (2)
Incomplete or No Cache-control and Pragma HTTP Header Set
X-Content-Type-Options Header Missing (23)
Information Disclosure - Suspicious Comments (12)
Loosely Scoped Cookie (3)
Timestamp Disclosure - Unix (54)
Alerts 0 2 6 3 Primary Proxy: localhost:8080
Current Scans 0 0 0 1 0 0 0 0

```
HTTP/1.1 200 OK
Content-Type: text/css; charset=utf-8
Access-Control-Allow-Origin: *
Timing-Allow-Origin: *
Link: <https://fonts.gstatic.com>; rel=preconnect; crossorigin
Strict-Transport-Security: max-age=31536000
Expires: Fri, 08 May 2020 04:26:33 GMT
Date: Fri, 08 May 2020 04:26:33 GMT
Cache-Control: private, max-age=86400
Server: ESF
```

```
/* devanagari */
@font-face {
  font-family: 'Poppins';
  font-style: normal;
  font-weight: 300;
  src: local('Poppins Light'), local('Poppins-Light'), url(https://fonts.gstatic.com/s/poppins/v9/pxiByp8kv8JHgFVrLDz8Z11lFc-K.woff2) format('woff2');
  unicode-range: U+0900-097F, U+1CD0-1CF6, U+1CF8-1CF9, U+200C-200D, U+20A8, U+20B9, U+25CC, U+A830-A839, U+A8E0-A8FB;
}
/* latin-ext */
@font-face {
  font-family: 'Poppins';
  font-style: normal;
  font-weight: 300;
  src: local('Poppins Light'), local('Poppins-Light'), url(https://fonts.gstatic.com/s/poppins/v9/pxiByp8kv8JHgFVrLDz8Z1JlFc-K.woff2) format('woff2');
  unicode-range: U+0100-024F, U+0259, U+1E00-1EFF, U+2020, U+20A0-20AB, U+20AD-20CF, U+2113, U+2C60-2C7F, U+A720-A7FF;
}
/* latin */
@font-face {
  font-family: 'Poppins';
  font-style: normal;
```

Cross-Domain Misconfiguration

URL: https://fonts.googleapis.com/css?family=Poppins:400,700,300,500
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)

Description:

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server

Other Info:

The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Figure 4. 4

Finally, you can get clear report about all these issue by clicking report button in tool bar and select any kind of report generates. There are four type of reports that you can generate by the ZAP. Normally HTML report is very common and easy report we used.

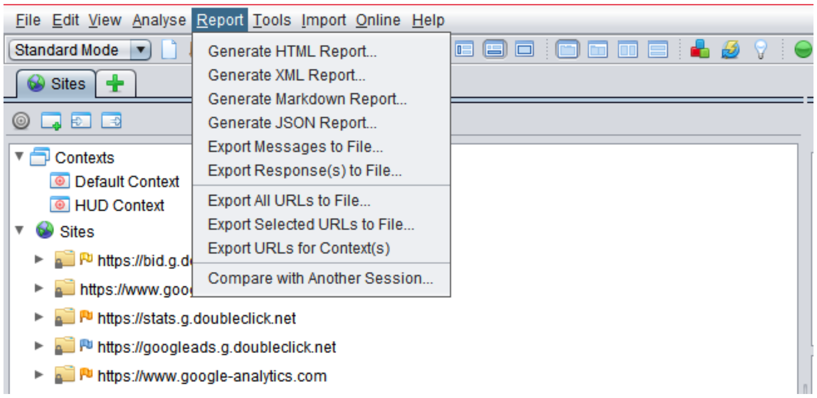
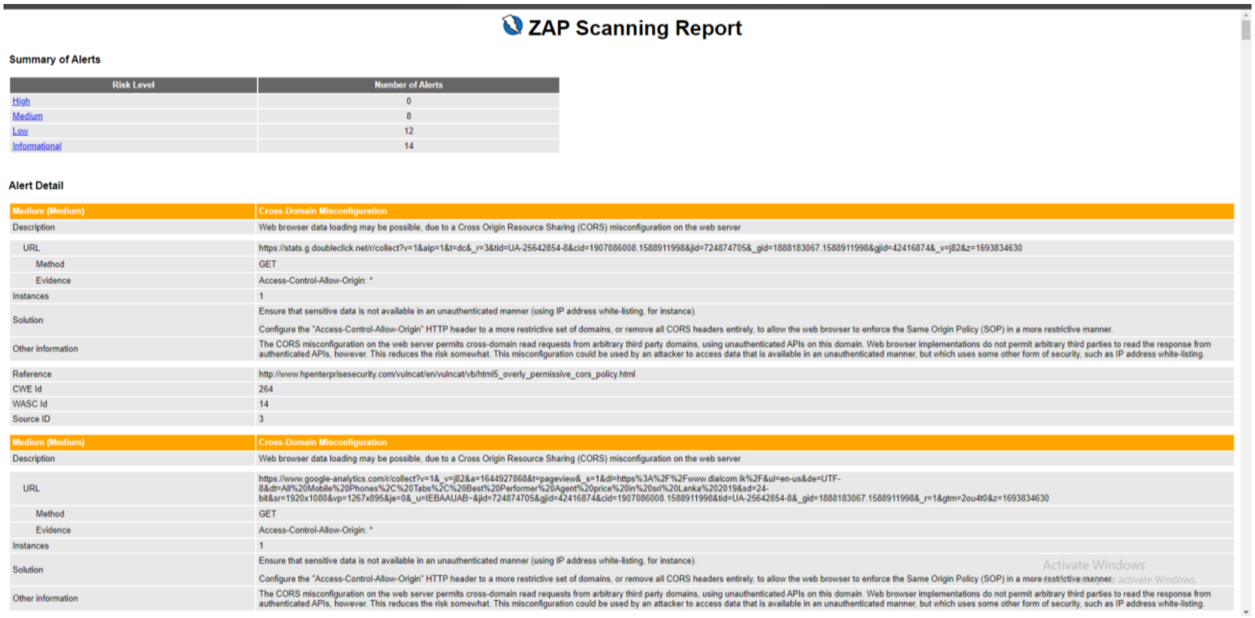

File
Edit
View
Analyse
Report
Tools
Import
Online
Help
Standard Mode
Sites
Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...
Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)
Compare with Another Session...
Contexts
Default Context
HUD Context
Sites
https://bid.g.d
https://www.goo
https://stats.g.doubleclick.net
https://googleads.g.doubleclick.net
https://www.google-analytics.com

Figure 4. 5

This is report that generate from the ZAP



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	8
Low	12
Informational	14

Alert Detail

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://stats.g.doubleclick.net/r/collect?v=1&aip=1&t=dc&_r=3&tid=UA-25642854-8&cid=1907086008.1588911998&jid=724874705&_gid=1888183067.1588911998&gjid=42416874&_v=j82&z=1693834630
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html
CWE Id	264
WASC Id	14
Source ID	3

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://www.google-analytics.com/r/collect?v=1&_v=j82&a=1644927868&t=pageview&_s=1&dl=https%3A%2F%2Fwww.dialcom.lk%2F&ul=en-us&de=UTF-8&dt=All%20Mobile%20Phones%2C%20Tabs%2C%20Best%20Performer%20Agent%20price%20in%20sri%20Lanka%202019&sd=24-bit&sr=1920x1080&vp=1267x895&je=0&_u=IEBAAUAB~&jid=724874705&gjid=42416874&cid=1907086008.1588911998&tid=UA-25642854-8&_gid=1888183067.1588911998&_r=1&gtm=2ou4t0&z=1693834630
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Figure 4. 6

5. Problem Identification

In this scan, we see there are number of issues identify by the ZAP. One medium issue and five low issues in page alerts. As well as there are one medium issue and six low issues identify in the site alerts. Those we can see this site is not clearly optimized site. One of the main issue is **X-Frame - Option Header Not Set** and **Cross-Domain Misconfiguration**. As well as, see several informational issues with the blue flag.

Main disadvantage that arose from these issues is loading speed is and browsing speed will get decrease. Therefore, almost the website performance is ok, but have to increase to get better usage from the website.

6. Conclusion

In my audit scenario, I used to audit one of the most used website in Sri Lanka. But, it contain some medium level issues regarding to the performance. So, it is good to have practice to audit the website regularly to keep the site safe and less issue with good performance. Because, by doing such audit you can get clear identification about the issues.

Using a tool like ZAP to such an audit is very useful. Because, these tools make our work easy and do the task accurately. Because, they build an environment that we can focus the work to do at best. In website auditing, there are so many tools that we can try. Therefore, auditing a website is not much difficult if we understand our wants and right tool.

Finally in this audit, we can concern this site is at medium optimization level. But it can improve much better by removing those issues. We have to follow the audit report that we get after scan of the website. By removing those issue we can get the website to good performance that having higher SEO ratings.

7. Reference

- [1]"What is a Website? - Definition from Techopedia", *Techopedia.com*, 2020. [Online]. Available: https://www.techopedia.com/definition/5411/website. [Accessed: 06- May- 2020].
- [2]R. Churt, "How to Audit Your Website for Improved SEO and Conversions", Blog.hubspot.com, 2020. [Online]. Available: https://blog.hubspot.com/marketing/website-audit. [Accessed: 06- May- 2020].
- [3]"TECHNOLOGY RADAR Our thoughts on the technology and trends that are shaping the future" (PDF). Thoughtworks.com. Retrieved 6 May 2015.
- [4]M. Birkner, "Automated Security Testing of web applications using OWASP Zed Attack Proxy - codecentric AG Blog", *codecentric AG Blog*, 2020. [Online]. Available: https://blog.codecentric.de/en/2013/10/automated-security-testing-web-applications-using-owasp-zed-attack-proxy/. [Accessed: 06- May- 2020].
- [5]M. Rouse, "What is IT audit (information technology audit)? - Definition from WhatIs.com", SearchCompliance, 2020. [Online]. Available: https://searchcompliance.techtarget.com/definition/IT-audit-information-technology-audit. [Accessed: 05- May- 2020].
- [6]L. Obbayi, "Introduction to OWASP ZAP for Web Application Security Assessments", *Infosec Resources*, 2020. [Online]. Available: https://resources.infosecinstitute.com/introduction-owasp-zap-web-application-security-assessments/#gref. [Accessed: 07- May- 2020].