



Information Assurance and Auditing

4th Year, 1st Semester

2020

ASSIGNMENT - 01

Student Name - W.A.D.D. Wickramasinghe

Registration Number - IT16092716

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

Specialized in

Computer Systems and Network Engineering

08.05.2020

1. Abstract

Nowadays we are following a pathway which has almost everything online. It is easy to access and use those goods and services around the world. Along with this convenience, we have gained both pros and cons. Now we have to take care of those online available systems. In order to take care of them, we should check whether they are actually secured. That's the moment when "Information Systems Auditing" takes place. We do an audit to check the current situation of the information systems, their exposures to risks, to clarify how to mitigate risks, and to fulfil proper maintenance.

Being protected in the online world is very important for every organization and everyone. Since the risk of sensitive data being revealed is much higher. Therefore, the following best security precautions are a must for any organization. They should be capable of identifying and determining the ways of stealing or making fraud their customer data. Or else they may lose their everything including reputation.

Contents

1. Abstract.....	2
2. Introduction.....	4
3. ZAP	5
4. Qualys SSL Labs.....	8
5. SSL Hopper.....	9
6. Auditing the Department of Examinations website	10
6.1. Auditing with ZAP.....	10
6.2. Auditing with Qualys SSL Labs	14
6.3. Auditing with SSL Hopper	15
7. Auditing the Harvard University website	16
7.1. Auditing with ZAP.....	16
7.2. Auditing with Qualys SSL Labs	17
8. Comprehension	19
9. Conclusion and Recommendation	20
10. References.....	21

2. Introduction

Today, the most popular way of connecting with the world is websites. There are billions of websites on the Internet. Some of them may be audited and performed at a very good level. But, there may be some other websites which are not really taking care of, they are being hacked by unethical parties every day. To stop that behavior, we need to check whether the website is having good performance, whether the tools used are up to date, should be touched with the digital certificate which is obtained. So, auditing should be done to fulfil those requirements.

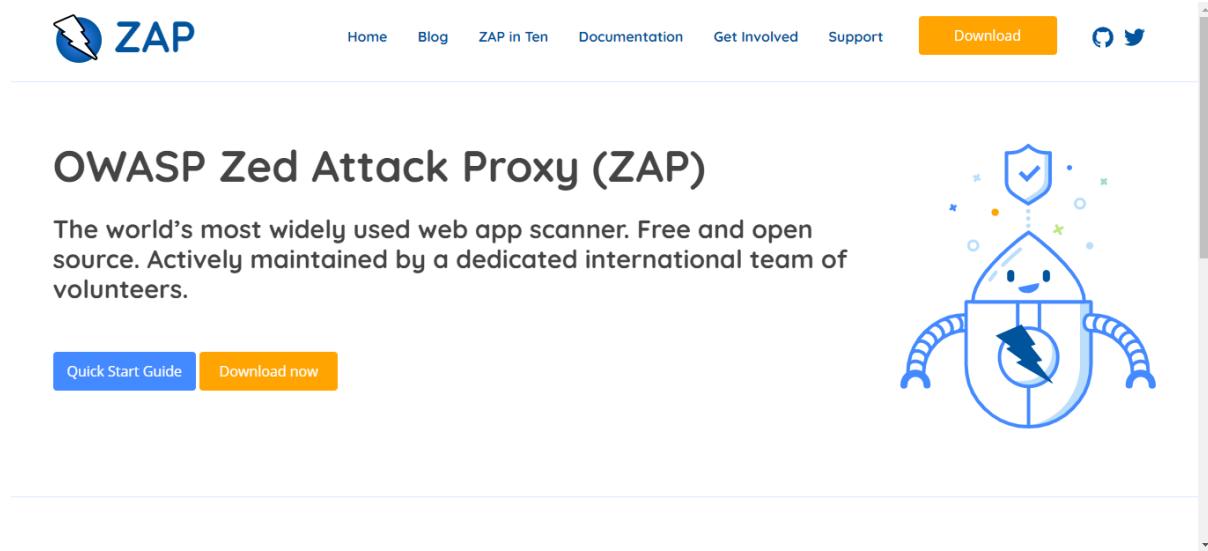
When it comes to business, the owner of it should do audits in a timely manner. It gives them more benefits. The auditing gives an idea about how the user experience with the website. It shows what are the aspects should be improved. It shows, what are the solutions which can be applied to make the website secured and more efficient.

To do so, there should be a checklist, it should follow Advanced Content Audit, User Experience audit, SEO audit, Vulnerability, and security scans. If we properly follow these steps, it will provide a more detailed report regarding the particular website.

3. ZAP

This is the main tool I'm going to use to do this audit. It is a free and open source software which is developed by OWASP.[1]

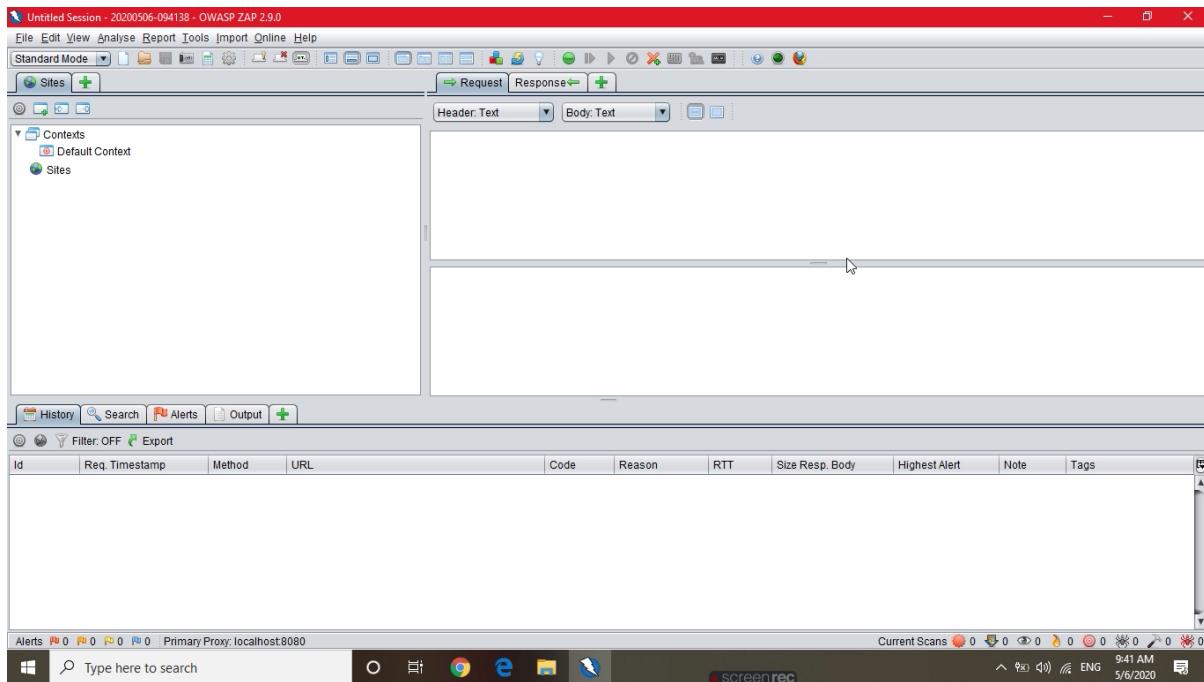
It can be downloaded by this link, <https://owasp.org/www-project-zap/>



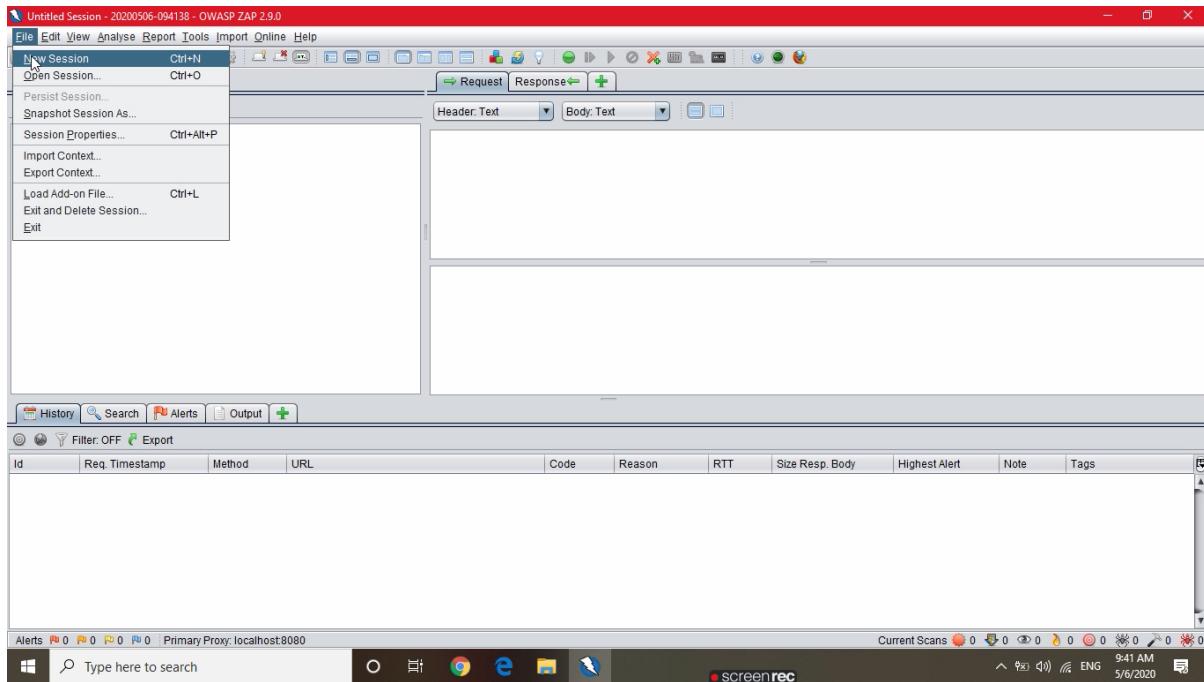
Open the tool.



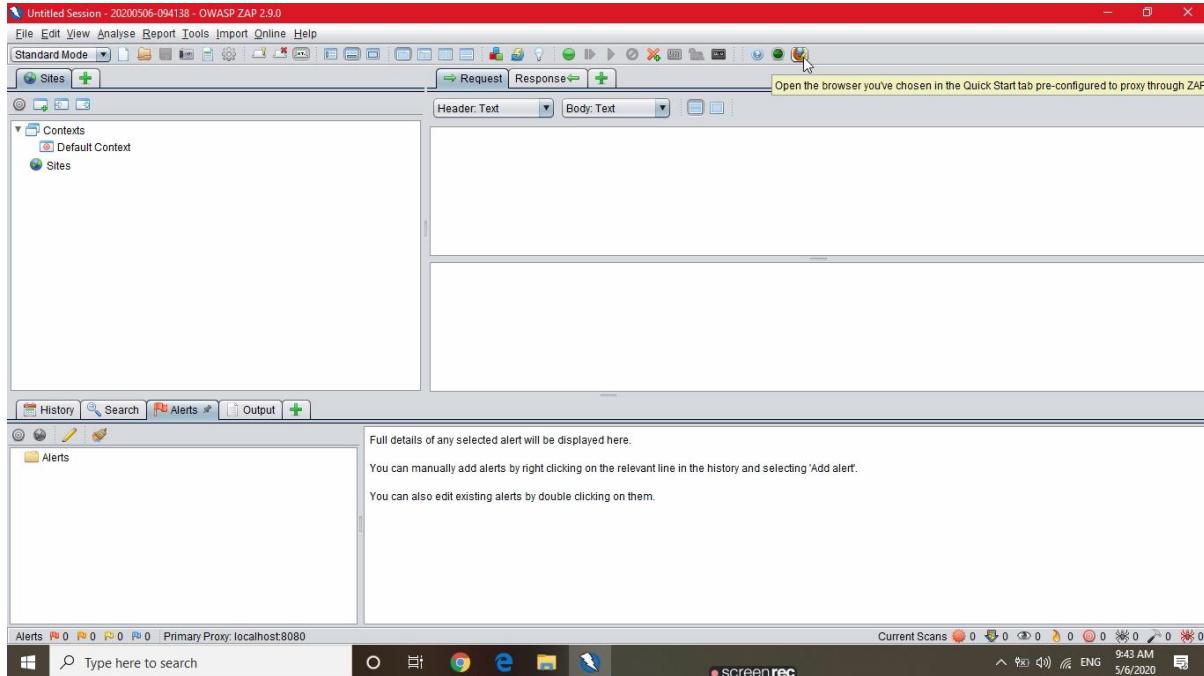
Home screen of ZAP.



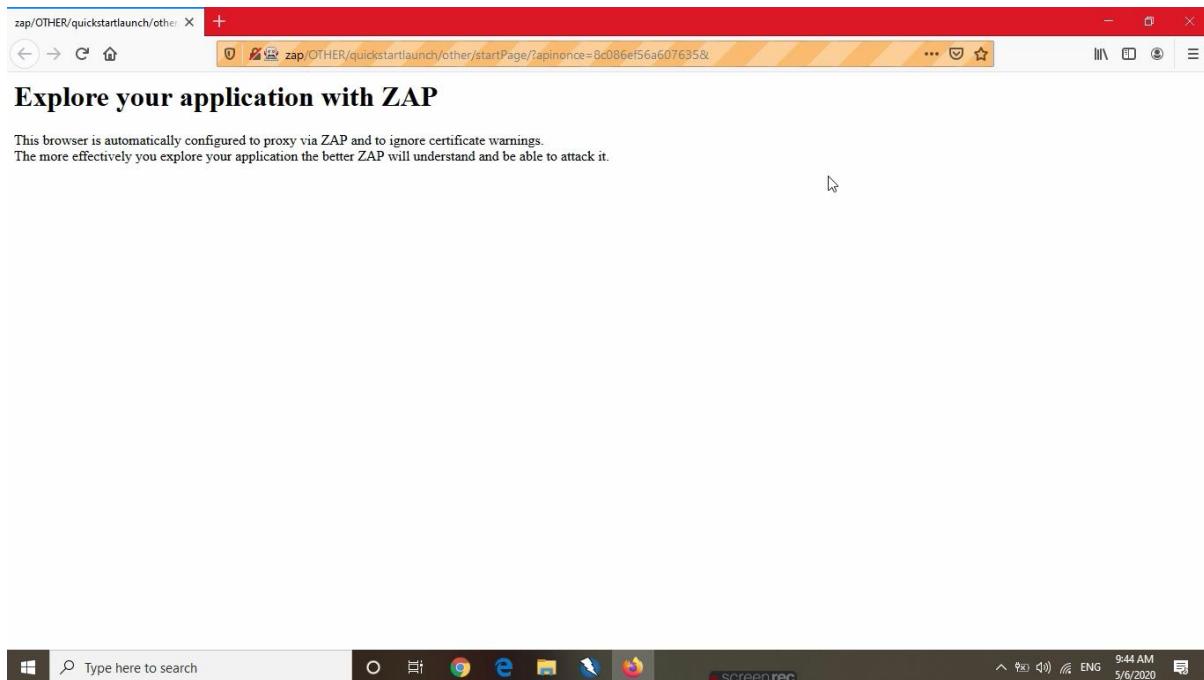
We should start a new session to scan a website.



The supporting web browser should be opened by the ZAP. I have configured firefox as the supporting browser. To do so, we should configure a manual HTTP proxy as “localhost” for port “8080”.



You can see the difference of address bar in regular firefox page and a page which is supporting to this tool.



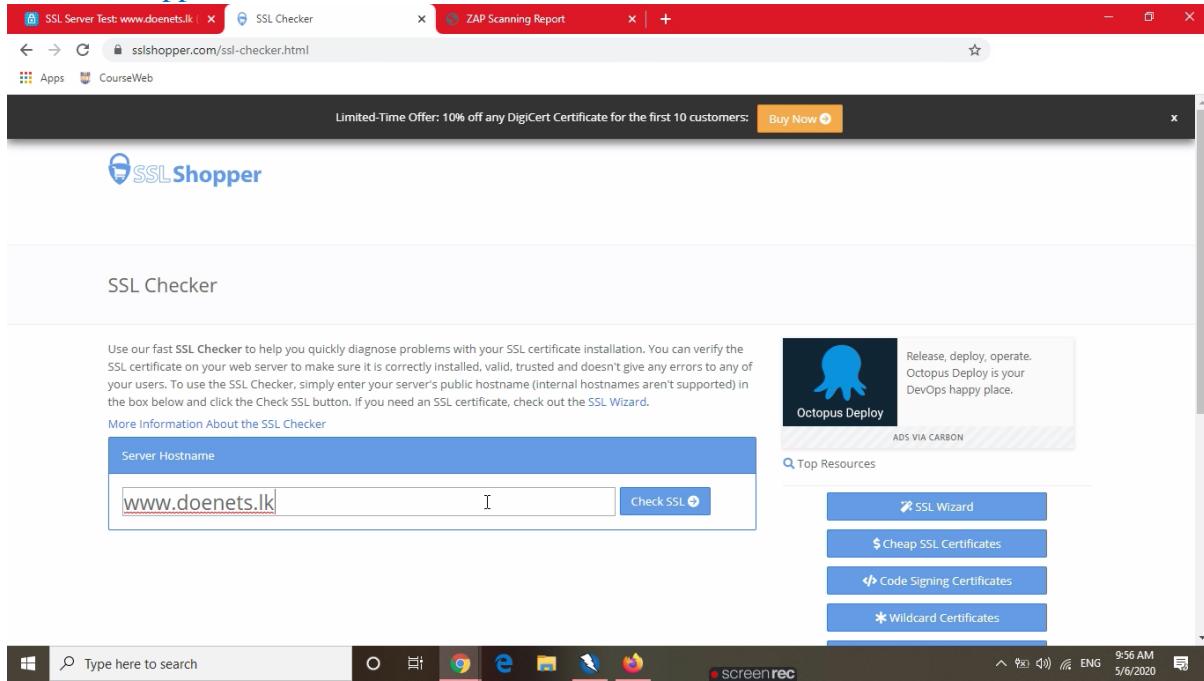
4. Qualys SSL Labs

For the scoring of websites, I'm using SSL Labs website. It provides website scoring for free.[4] <https://www.ssllabs.com/ssltest/>

The screenshot shows the Qualys SSL Labs website interface. At the top, there are tabs for 'SSL Checker' and 'ZAP Scanning Report'. The main navigation menu includes 'Home', 'Projects', 'Qualys Free Trial', and 'Contact'. Below the menu, it says 'You are here: Home > Projects > SSL Server Test'. The main content area is titled 'SSL Server Test' and contains a note about the service's purpose: 'This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.' A form allows users to enter a 'Hostname' (www.doenets.lk) and a 'Submit' button. There is also a checkbox for 'Do not show the results on the boards'. Below the form, there are three sections: 'Recently Seen' (listing sites like ute49cik.ultiprotime.com, goi.valueai.com, www.velocitypayment.com, wenance.lightning.force.com, and comskills-ukraine.co.uk), 'Recent Best' (listing sites like www.kotaksecurities.com, www.velocitypayment.com, comskills-ukraine.co.uk, 3dsecure2.ocbcnisp.com, and account.mrbillie.nl), and 'Recent Worst' (listing sites like mahades.maharashtra.gov.in, onlineapps.anz.com, my.eir.ie, eta-teams.transport.mil, file.mps.or.kr, and dfx.com.ar). The status bar at the bottom shows 'screenrec', the date '5/6/2020', and the time '9:55 AM'.

5. SSL Hopper

I'm using SSL Hopper for testing the situations regarding the Certificate of the website.[5]
www.sslshopper.com/ssl-checker.html

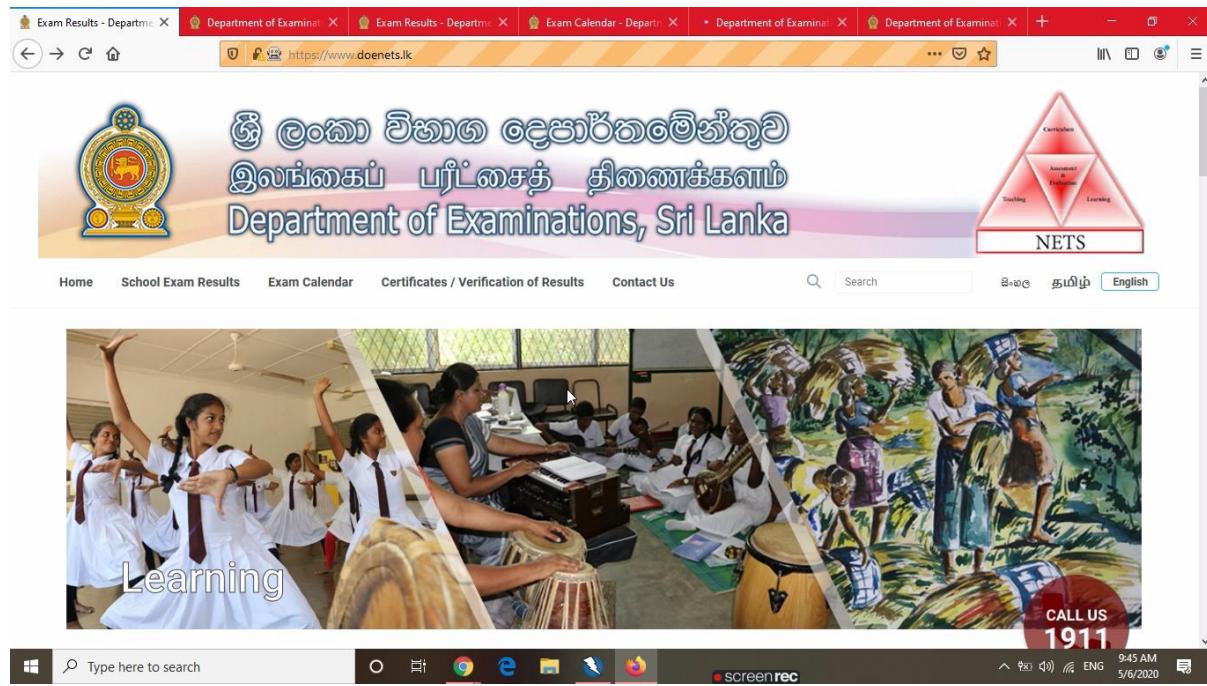


The screenshot shows a Windows desktop environment. A browser window is open to the SSL Shopper SSL Checker page. The URL in the address bar is www.sslshopper.com/ssl-checker.html. The page content includes a heading 'SSL Checker', a brief description of the tool, and a form where the server hostname 'www.doenets.lk' has been entered. Below the form is a 'Check SSL' button. To the right of the main content, there is an advertisement for 'Octopus Deploy' with the text 'Release, deploy, operate. Octopus Deploy is your DevOps happy place.' and 'ADS VIA CARBON'. Further down, there is a sidebar titled 'Top Resources' with four items: 'SSL Wizard', 'Cheap SSL Certificates', 'Code Signing Certificates', and 'Wildcard Certificates'. At the bottom of the screen, the Windows taskbar is visible, showing the Start button, a search bar with the text 'Type here to search', and icons for various applications like File Explorer, Google Chrome, Microsoft Edge, and Mozilla Firefox. The system tray shows the date and time as '5/6/2020 9:56 AM'.

6. Auditing the Department of Examinations website

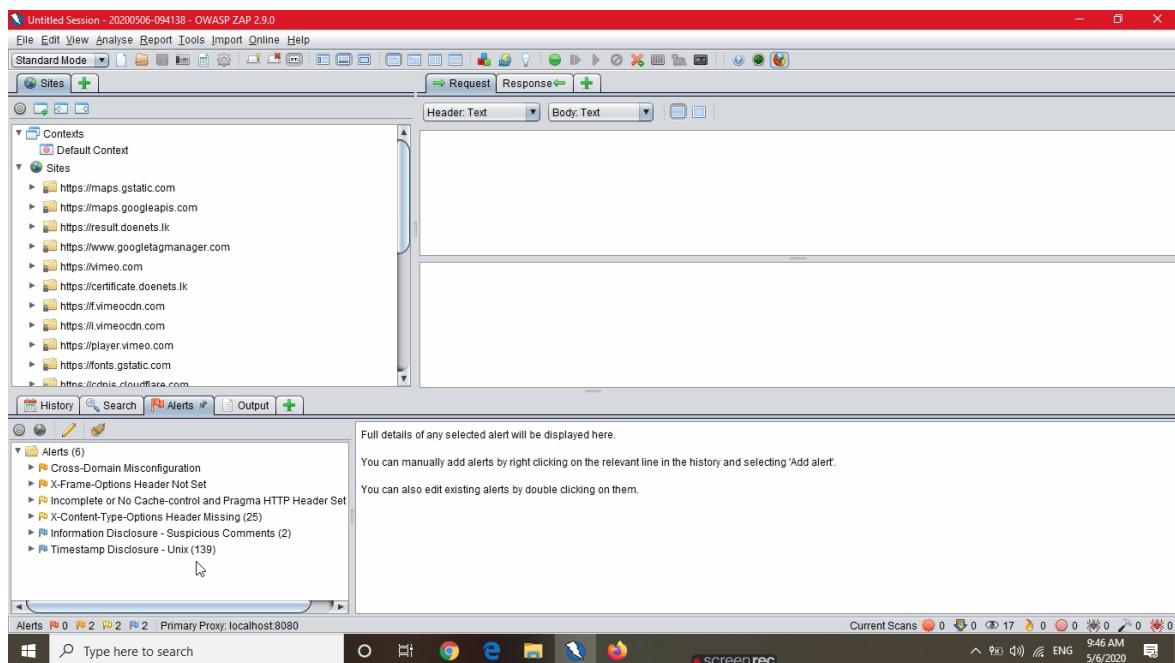
I'm going to audit the website of Examination Department, Sri Lanka.[2] Which is a popular website among everyone when the GCE O/L and A/L exam result releasing time.

<https://doenets.lk/>

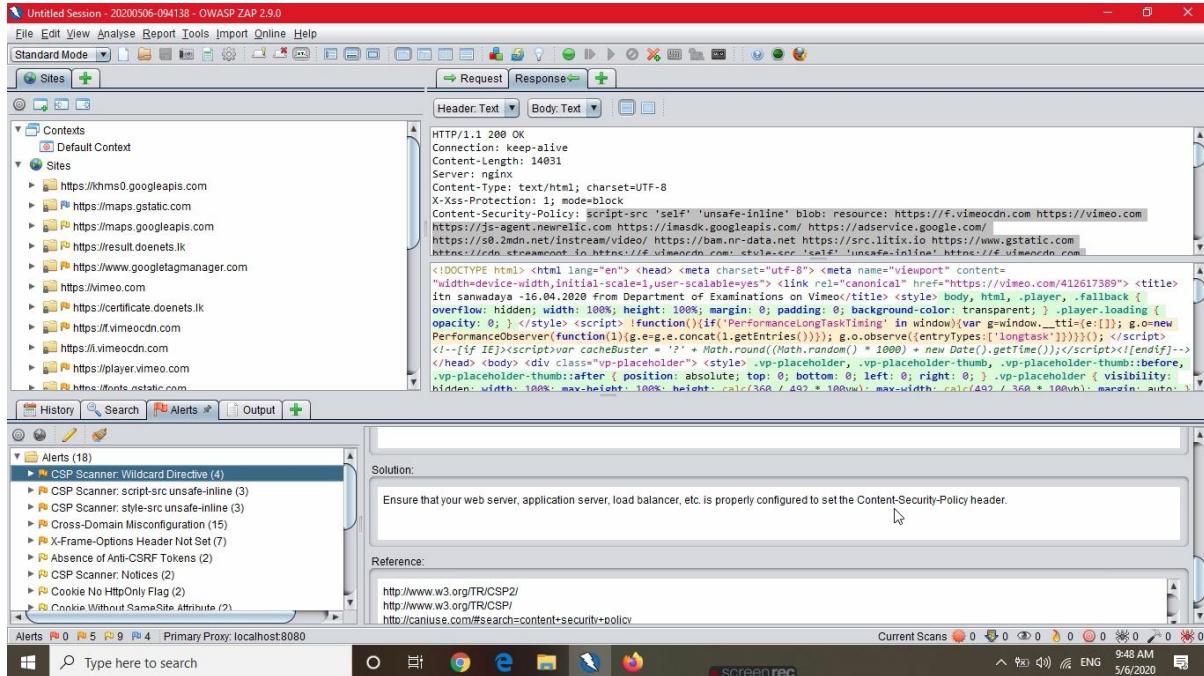


6.1. Auditing with ZAP

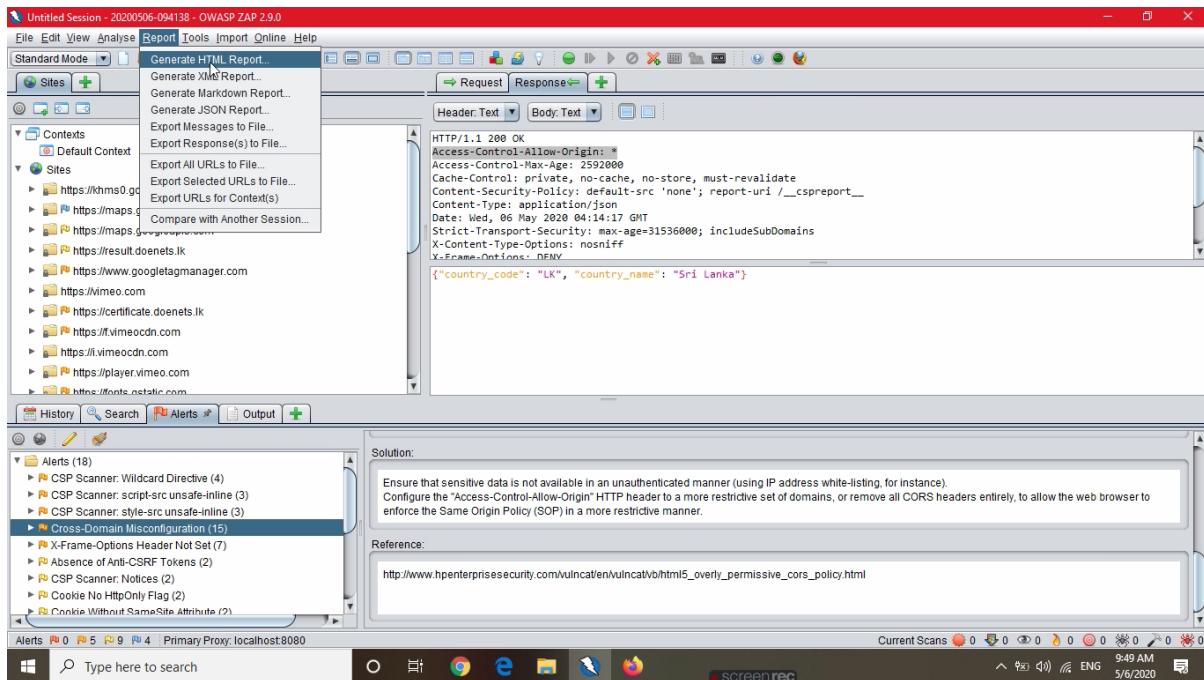
After browsing using the supporting browser the tool will automatically start the scanning.



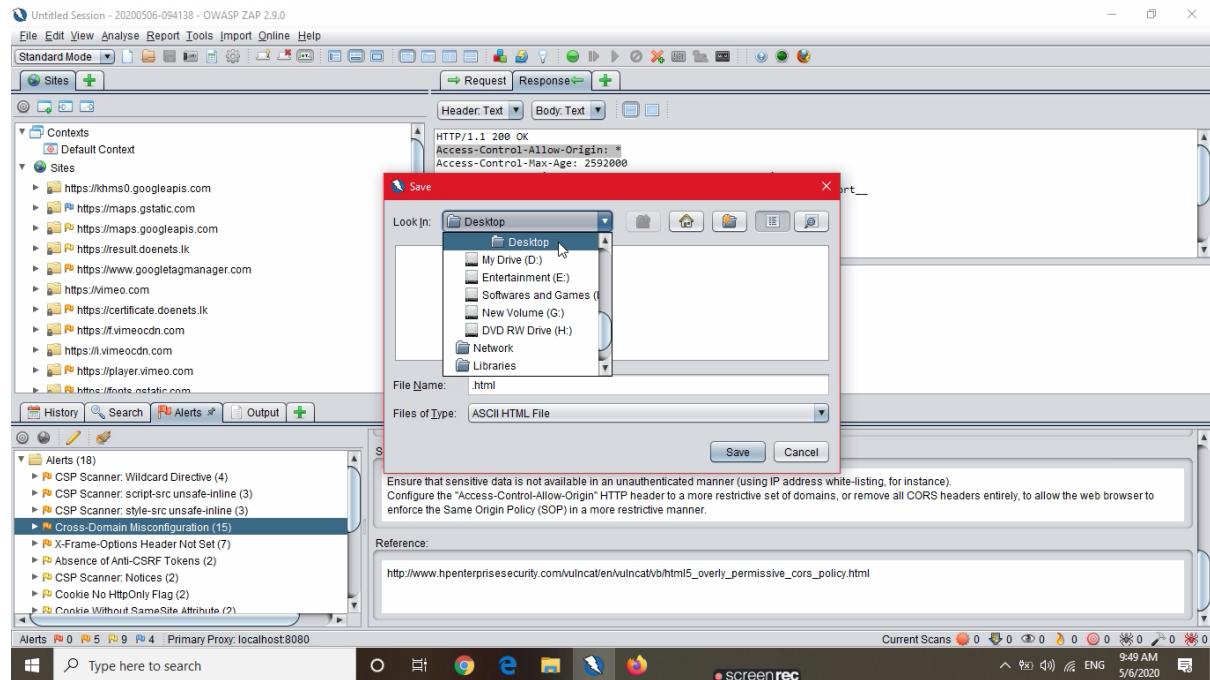
The amount of alerts regarding vulnerabilities can be seen in the alerts tab at the bottom of the tool. By clicking in the generated alerts we can find the place which the vulnerability exists, reason for that and the solution proposed.



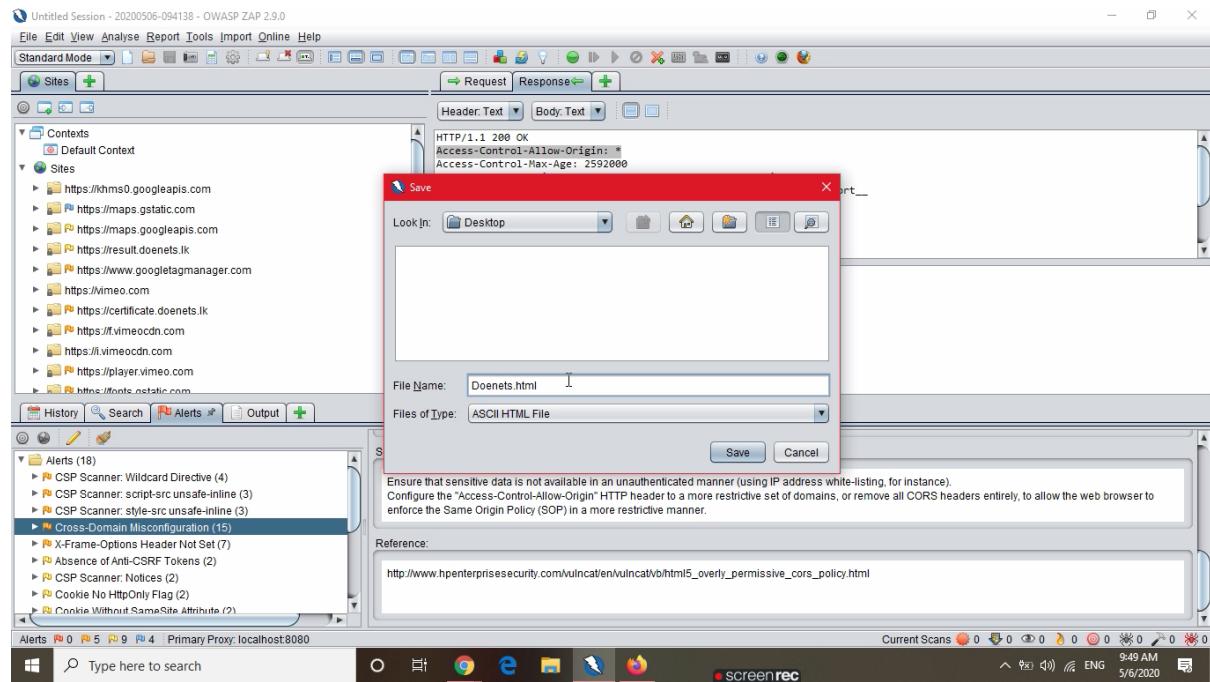
Then we can generate a report regarding the detected vulnerabilities. It gives further more clear idea about things we found.



A file location should be selected.



A name should be given.



This is the report generated.

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	16
Low	32
Informational	23

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://www.googletagmanager.com/gtag/js?id=UA-132651734-2
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

Windows taskbar: Type here to search, File, Start, Task View, Edge, File Explorer, Task Manager, Firefox, screenrec, ENG, 9:49 AM, 5/6/2020

Alert Detail

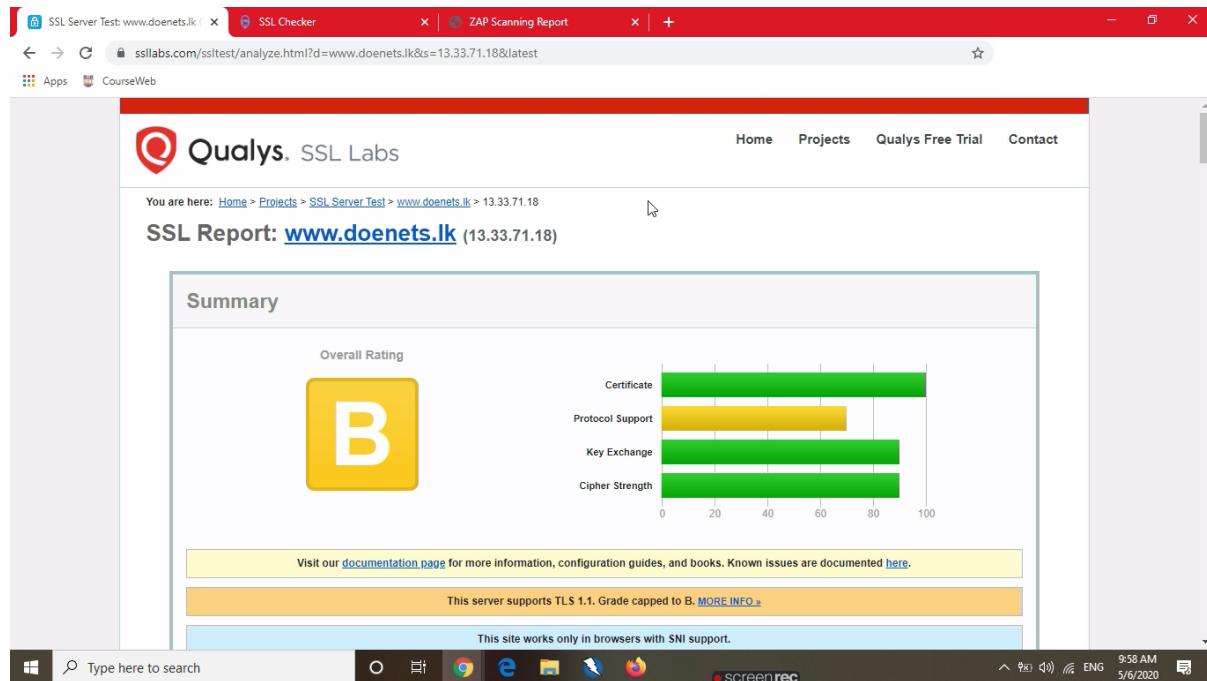
Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://www.googletagmanager.com/gtag/js?id=UA-132651734-2
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	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)	CSP Scanner: script-src unsafe inline
Description	script-src includes unsafe-inline.
URL	https://certificate.doenets.lk/
Method	GET
Parameter	Content-Security-Policy
Content-Security-Policy	default-src *, script-src 'self' 'unsafe-inline' https://www.google-analytics.com https://www.googletagmanager.com www.google.com https://www.gstatic.com

Windows taskbar: Type here to search, File, Start, Task View, Edge, File Explorer, Task Manager, Firefox, screenrec, ENG, 9:50 AM, 5/6/2020

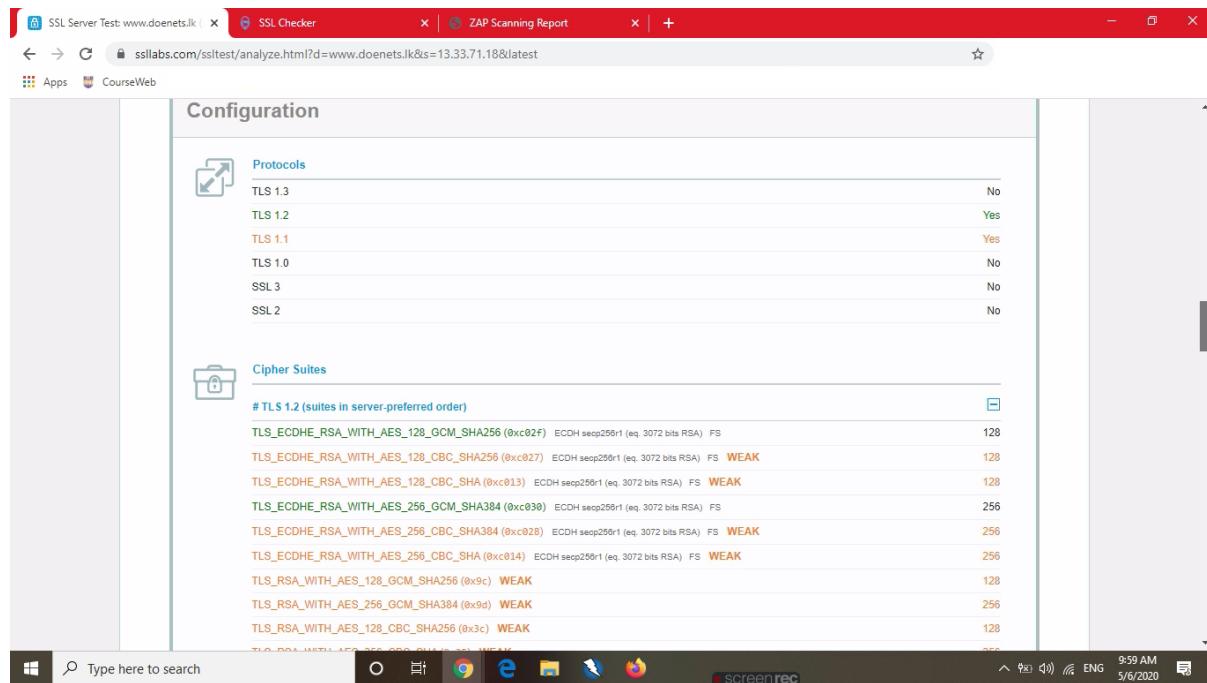
6.2. Auditing with Qualys SSL Labs

Simply copy and paste the URL into the search bar of the SSL Labs web page. Then it will scan and rate it. The website has gained B class rating. You can see the reasons to obtain the particular class.



The screenshot shows the Qualys SSL Labs Summary report for the URL www.doenets.lk. The overall rating is a large yellow 'B'. Below it, four horizontal bars represent different security metrics: Certificate (green, ~95%), Protocol Support (yellow, ~70%), Key Exchange (green, ~85%), and Cipher Strength (green, ~85%). A note at the bottom states: "Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#)". Another note says: "This server supports TLS 1.1. Grade capped to B. [MORE INFO](#)". A third note at the bottom indicates: "This site works only in browsers with SNI support". The browser taskbar at the bottom shows various icons and the time as 9:58 AM on 5/6/2020.

You can see it is supporting some outdated protocols such as TLS 1.1



The screenshot shows the Qualys SSL Labs Configuration report for the URL www.doenets.lk. Under the 'Protocols' section, TLS 1.1 is listed as 'Yes'. Under the 'Cipher Suites' section, several cipher suites are listed with their details and key sizes:

Cipher Suite	Description	Key Size
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x9c)	WEAK	128

6.3. Auditing with SSL Hopper

Again copy and paste the URL into the search bar of the SSL Hopper web page. Then it will show the certificate details.

The screenshot shows a Microsoft Edge browser window with three tabs open:

- SSL Server Test: www.doenets.lk
- SSL Checker
- ZAP Scanning Report

The main content area displays the results of the SSL checker for the server www.doenets.lk. It includes a form to enter a server hostname, a "Check SSL" button, and a list of audit results with green checkmarks:

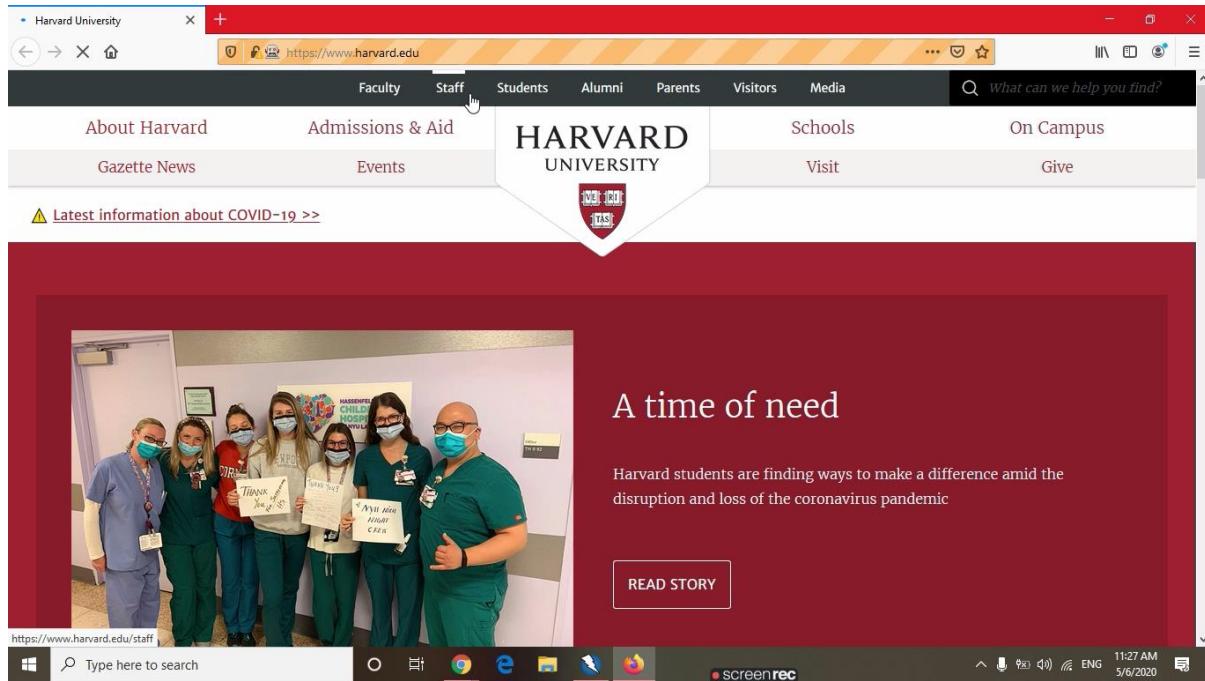
- www.doenets.lk resolves to 99.84.102.17
- Server Type: AmazonS3
- The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).
- The certificate will expire in 385 days. (A "Remind me" button is present.)
- The hostname (www.doenets.lk) is correctly listed in the certificate.

Below this, there is a detailed view of the certificate's common name, SANs, validity period, serial number, and signature algorithm.

On the right side of the page, there is an advertisement for DigiCert SSL certificates, featuring a "Buy Now" button and a "Get Pricing" button.

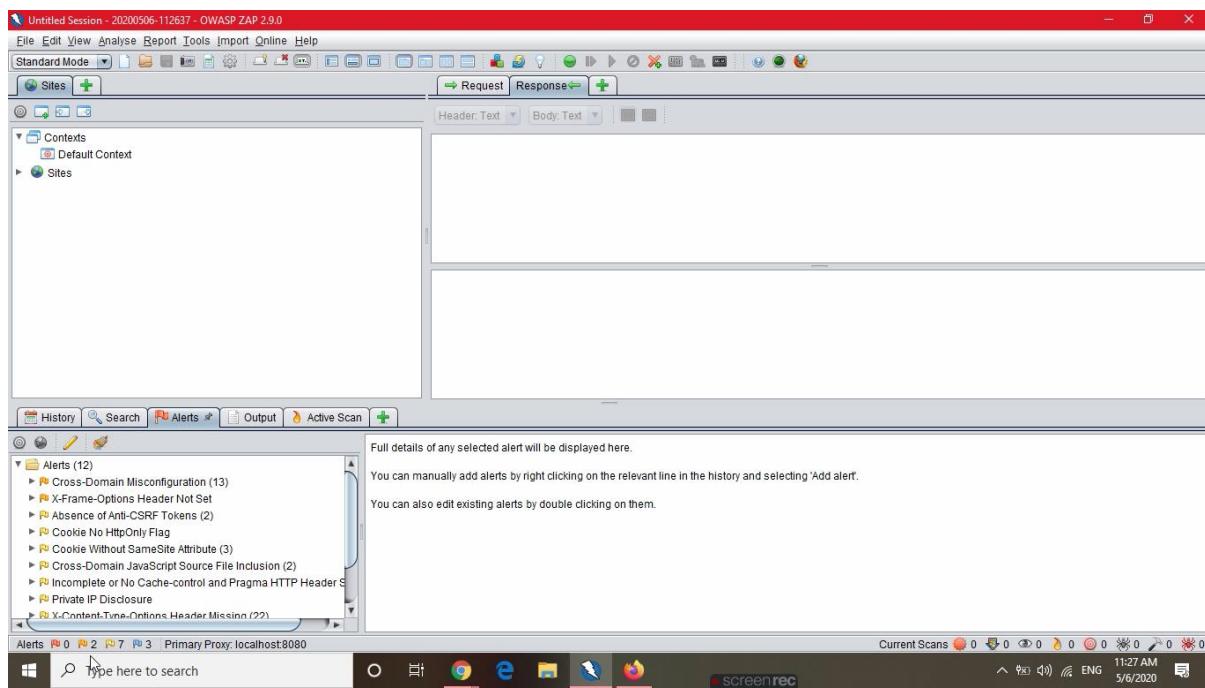
7. Auditing the Harvard University website

As a comparison to have a better idea, I did the auditing with another website. It is the website of the Harvard University.[3] <https://www.harvard.edu/>



7.1. Auditing with ZAP

Again I used ZAP and did the scan.



Here is the report regarding the Harvard University website.

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	8
Low	17
Informational	18

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://static.doubleclick.net/instream/ad_status.js

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

7.2. Auditing with Qualys SSL Labs

Then I used SSL Labs to gain the score.

Qualys. SSL Labs

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.

Hostname: www.harvard.edu | Submit | Do not show the results on the boards

Recently Seen	Recent Best	Recent Worst
www.fordpartsprime.com unaux.com solarreach.com.au www.fishpond.online store.movistar.com www.xn--12c1ck0b6hd9yb9b...	subto1.eu (A+) ftbvistaweb.ngahrhosting.com (A+) testscale05052020.skyfencene... (A) uatmin@popo1.capitalstar.com... (A) www.facebook.com (B) www.1111code.com (B)	m.vtinform.com (T) avx-imt.payoda.com (T) superdepot.net.au (T) anix64.go.ro (T) the-modeling-agency.com (F) meet.shell.com (F)

Here is the result. It is “A+”, So you can see the reasons why it got an A+.

The screenshot shows the Qualys SSL Labs SSL Report for www.harvard.edu. The overall rating is **A+**. The report includes a summary chart showing the following scores:

Category	Score
Certificate	100
Protocol Support	100
Key Exchange	88
Cipher Strength	88

Below the chart, there is a yellow box with a link to the documentation page and a blue box stating "This site works only in browsers with SNI support". At the bottom, a green box indicates "HTTP Strict Transport Security (HSTS) with long duration deployed on this server". The taskbar at the bottom shows various icons and the date/time as 11:31 AM 5/6/2020.

It supports modern TLS versions. No supporting for older versions such as TLS 1.1.

The screenshot shows the configuration section of the Qualys SSL Labs report. Under the "Protocols" heading, the supported versions are listed as follows:

Protocol	Status
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Under the "Cipher Suites" heading, the supported ciphers are listed in server-preferred order:

Cipher Suite	Key Exchange	Hash	Strength
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519	(eq. 3072 bits RSA)	FS 128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519	(eq. 3072 bits RSA)	FS 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519	(eq. 3072 bits RSA)	FS WEAK 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519	(eq. 3072 bits RSA)	FS WEAK 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519	(eq. 3072 bits RSA)	FS WEAK 128

The taskbar at the bottom shows various icons and the date/time as 11:32 AM 5/6/2020.

8. Comprehension

Examination Department's website is having some issues and lower grading compared to the Harvard University website.

In the report of the Doenets, CORS Misconfiguration was mentioned. It will be a big deal for unethical parties. One of the most common CORS misconfigurations is incorrectly using wildcards such as (*) under which domains are allowed to request resources. It is the default behavior. But, it can be configured with safeguarding the website.

9. Conclusion and Recommendation

There are some issues to be addressed with good configuration and updates. Updating the Doenets website to support only TLS 1.2 or higher is a major update to be done. Because it is the technique of encrypting sensitive data.[7] Older TLS versions may be vulnerable. So, it must be up to date.

The other thing is X-frame header was not set. It defines whether a browser is allowed or not to render a page. If it is not set it is a reason for the “ClickJacking” attack. Which means, hijacking the click making a fraud button click by the victim. So, the X-frame header should be set.[8]

10. References

- [1]"OWASP ZAP", Zaproxy.org, 2020. [Online]. Available: <https://www.zaproxy.org/>. [Accessed: 06- May- 2020].
- [2]"Department of Examinations - Sri Lanka", Doenets.lk, 2020. [Online]. Available: <https://doenets.lk/>. [Accessed: 06- May- 2020].
- [3]H. University, "Harvard University", Harvard University, 2020. [Online]. Available: <https://www.harvard.edu/>. [Accessed: 06- May- 2020].
- [4]"SSL Server Test (Powered by Qualys SSL Labs)", Ssllabs.com, 2020. [Online]. Available: <https://www.ssllabs.com/ssltest/index.html>. [Accessed: 06- May- 2020].
- [5]"SSL Checker", Sslshopper.com, 2020. [Online]. Available: <https://www.sslshopper.com/ssl-checker.html>. [Accessed: 06- May- 2020].
- [6]P. J, "3 Ways to Exploit Misconfigured Cross-Origin Resource Sharing (CORS)", We45.com, 2020. [Online]. Available: <https://www.we45.com/blog/3-ways-to-exploit-misconfigured-cross-origin-resource-sharing-cors>. [Accessed: 06- May- 2020].
- [7]"What is TLS & How Does it Work? | ISOC Internet Society", Internet Society, 2020. [Online]. Available: https://www.internetsociety.org/deploy360/tls/basics/?gclid=Cj0KCQjwhtT1BRCiARIsAGlY51LRwFqL_49HAMNZn82t5UqJtIeb-s4CIauccbYJCEkofcrCGs2mh_8aApajEALw_wcB. [Accessed: 06- May- 2020].
- [8]"Clickjacking | OWASP", Owasp.org, 2020. [Online]. Available: <https://owasp.org/www-community/attacks/Clickjacking>. [Accessed: 06- May- 2020].