Information Assurance and Auditing

4th Year, 1st Semester
2020

ASSIGNMENT - 01

Student Name - H.S.I. Madhusanka

Registration Number - IT16000568

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

Specialized in

Computer Systems and Network Engineering

06.05.2020

Abstract

Along with the human evolution everyone needed easiest ways to do their workload. Then they found the fire, and then the wheel was invented. But, nowadays humans have come a long way. They are in an online world now. With the word online we all automatically remind the Internet, where all of us connect. It makes us to think no-one is alone in the Internet. But, the worst case is we also may have been watched without knowing by us. That is the point we need security. In order to fulfil the security, we need best practices and most up to date tools and certificates.

To maintain those needs, to make sure they are functioning properly, to check whether there are any risk and vulnerabilities, we need to do audit. Some website, system or a network runs without auditing in a timely manner then it may cause for a bigger problem in near future. A proper audit makes the organization more profitable and efficient than current rate.

Contents

1. Introduction

Auditing can be done for Websites, Systems or Networks. Websites are the most popular platform for every business, service or any other kind of requirements. For the best usage and user experience, we should do audits in a timely manner. I'm going to perform an audit for websites and web applications specially as security audits.

Nowadays unfortunately, most of the companies and organizations are breached because of misguided sense of security. This is the answer for why cyber criminals are successful in their attacks. Now it is a persistent risk. According to the GDPR in Britain, every company must have a role which is responsible for the data protection, who knows what are the security measurements and precautions going on with their data and have the responsibility to conduct security audits. CIO (Chief Information Officer) and CISO (Chief Information Security Officer) roles have come to the stage as a result of this evolution.

With the experience in Information and Data world we know that cyber security risks never can be completely eliminated. We must be evolved one step forward than the evolution of risks. In order to be forward, even the officers who are responsible for security should be updated meanwhile the softwares and services are up to date in the company.[1] To do so, we need to do our auditing properly. An audit focuses on,

- Cyber Security Standards
- Guidelines and Procedures
- Implementation of the Controls

A proper audit will give you the chance to,

- Establish a Set of Security Standards
- To Help Enforce Regulations and Best Practice
- To Determine the State of Your Security
- To have a good idea about user experience with your website

In order to conduct an Audit, we need to have a scope and a checklist.

As the **Audit Scope**, followings are going to be audited.[2]

- Website Security
- Digital Certificates
- Protocol Support

I'm going to use two tools for auditing which considers Open Web Application Security Project (OWASP) top 10 Security risks.[3]

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting XSS
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

2. Checklist

In order to fulfil the auditing, we need a checklist, since we may have forgotten to pay attention to something, may be a big mistake. So here is the Checklist. This is a general Checklist.[4] But, I'm not going to perform all the following tasks. Since I don't have access permissions for the websites. I'm doing this auditing as a trial.

- Changing Content Management System (CMS) Settings to default
  - User Settings
  - Comment Settings
  - General Visibility of Information

- Selecting most suitable ones among the file permissions
  - Read (r), Write (w), Execute (x)
  - Owner, Group, Public

- Checking availability for software updates
  - Check whether the CMS version is up to date and make sure it.

- Using security extensions for CMS
  - Security plugin settings check

- For installed extensions and plugins. check for,
  - Updates
  - Age
  - Number of installations
  - Checking whether their source is Legitimate

- Backup the Data
  - Offsite Backup
  - Automatic Backup
  - Prepare a reliable plan for recovery
  - Integrity checking for backups to check whether they are not unusable

- Check the server configuration files
  - Being familiar with web server configuration files
  - Prevent Directory browsing
  - Prevent Image hot linking
  - Protect Sensitive files

- Secure Socket Layers (SSL) Certificate Installation
  - Making sure the data of the website in transit is encrypted
  - Setup Secure Shell (SSH) Protocol of File Transferring

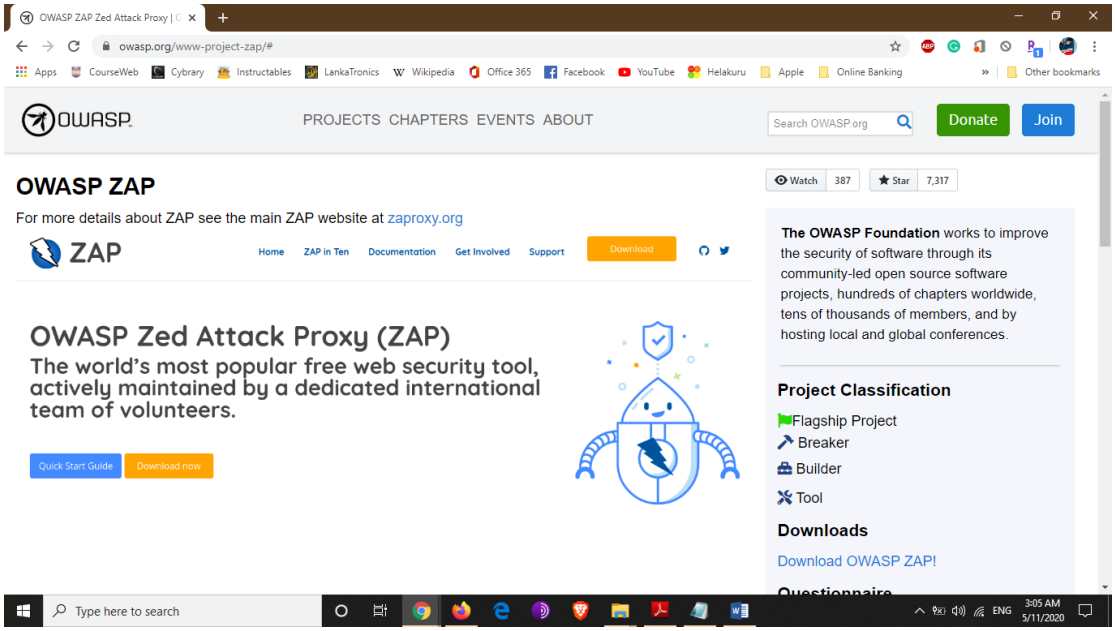
- Set automatic scans for malware detection
- Configuring strong unique passwords
- Making sure the website is not blacklisted

3. Tools

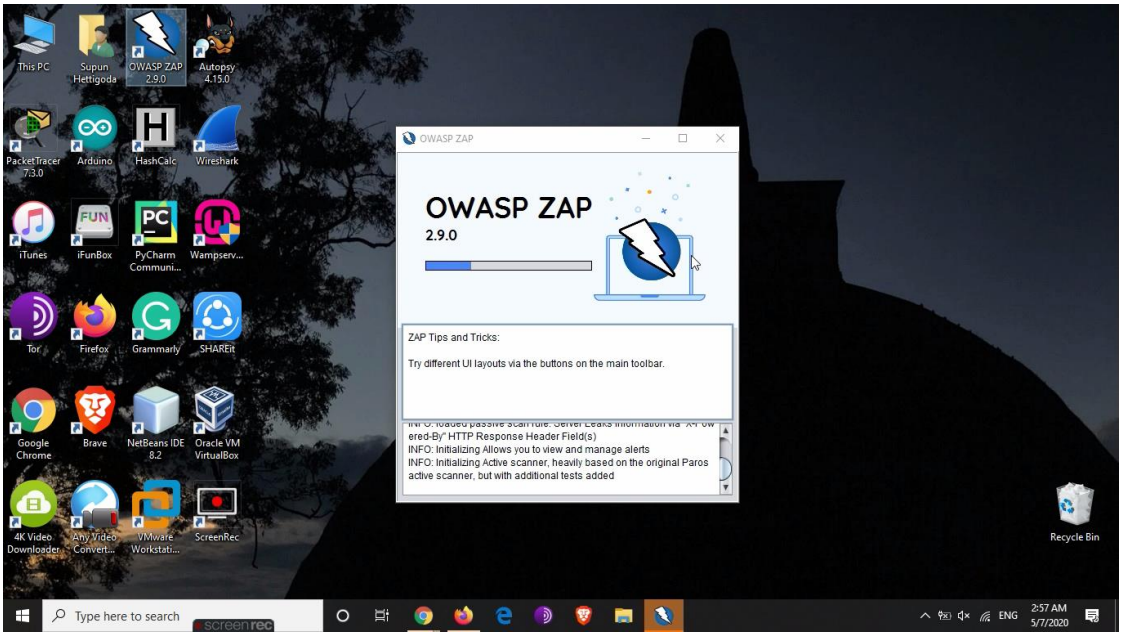
I'm going to use three tools for this audit. Two of them are open source and commercial web scanning tools. The other one is a SSL and Certificate testing tool.

3.1.Zed Attack Proxy (ZAP)

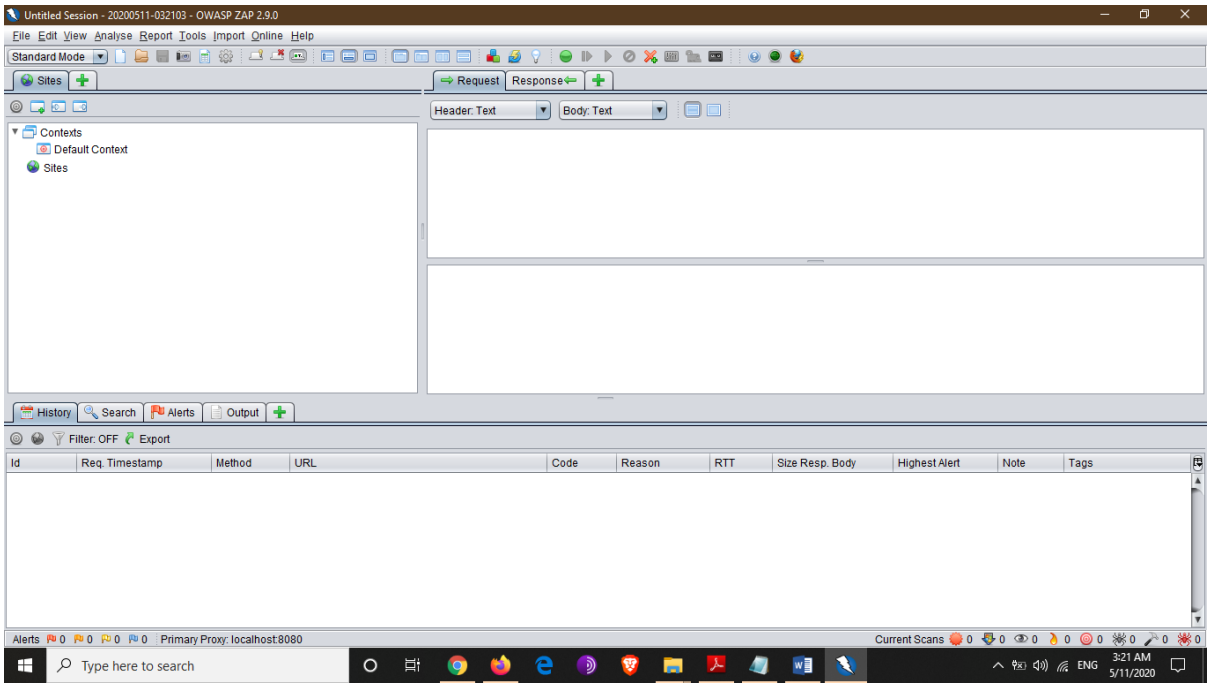
This is going to be the first tool that I'm using to perform this auditing. This is a free and open source tool which can be downloaded from the OWASP website.[5]



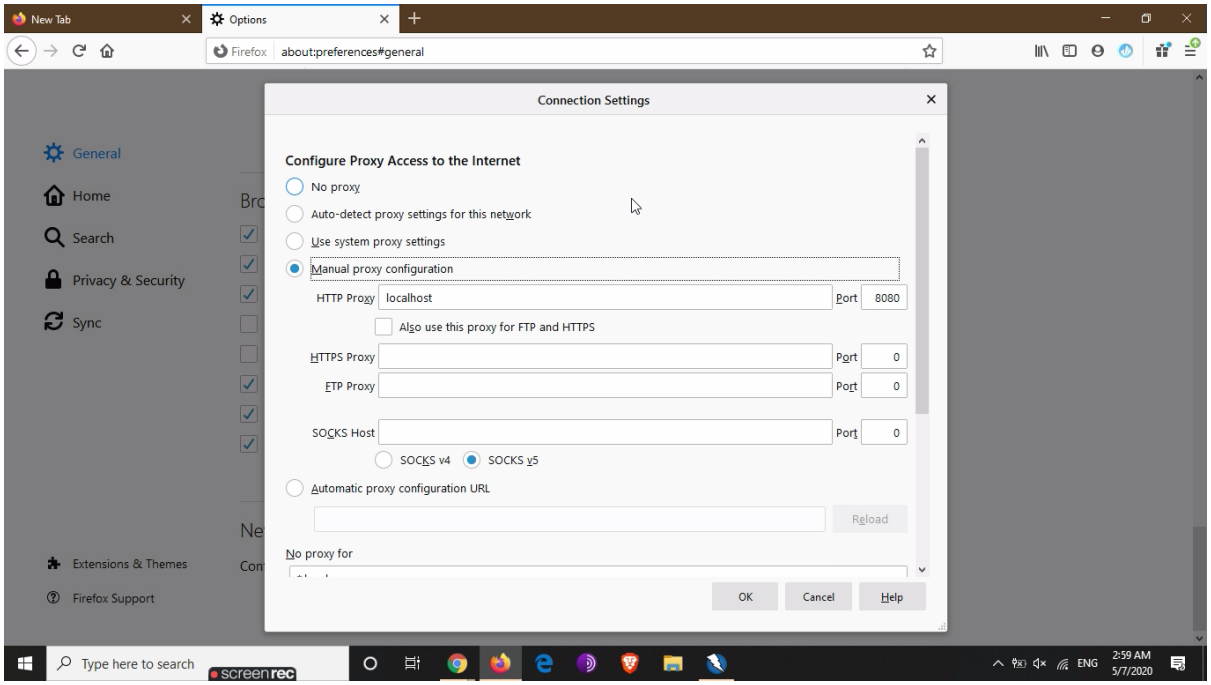
Simply install it using default settings same as the installation of a normal software. Then launch it. This is the up to date version available for now, OWASP ZAP 2.9.0



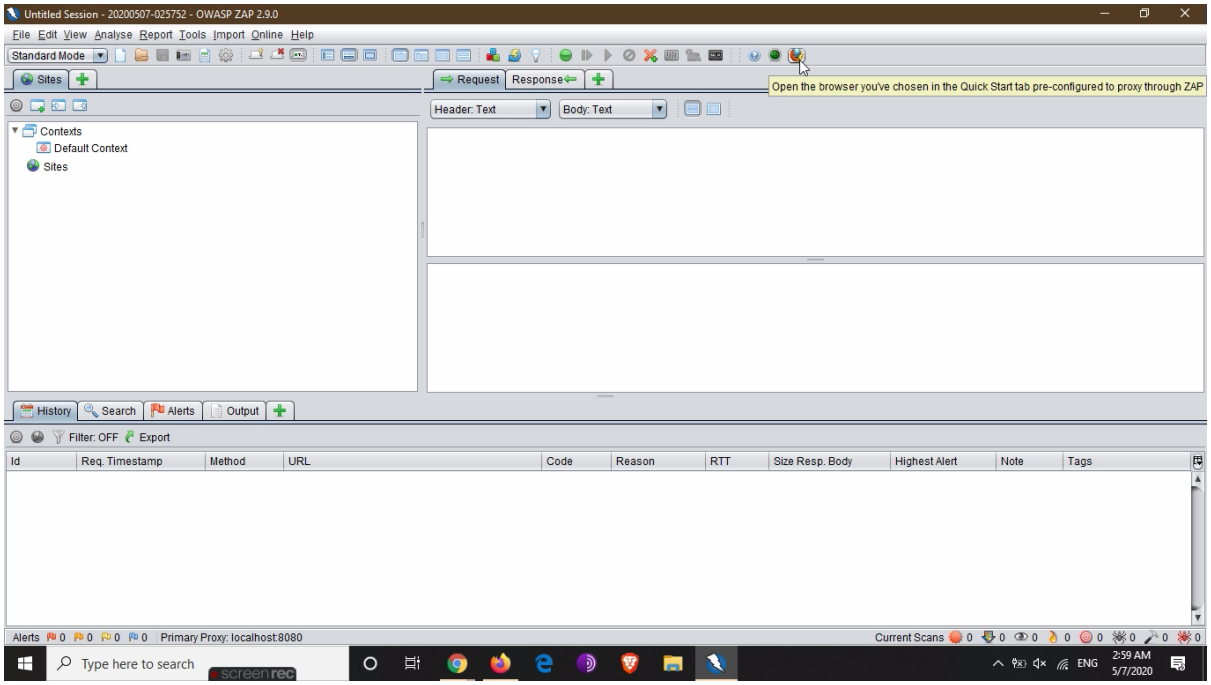
This is how the ZAP home screen looks like.



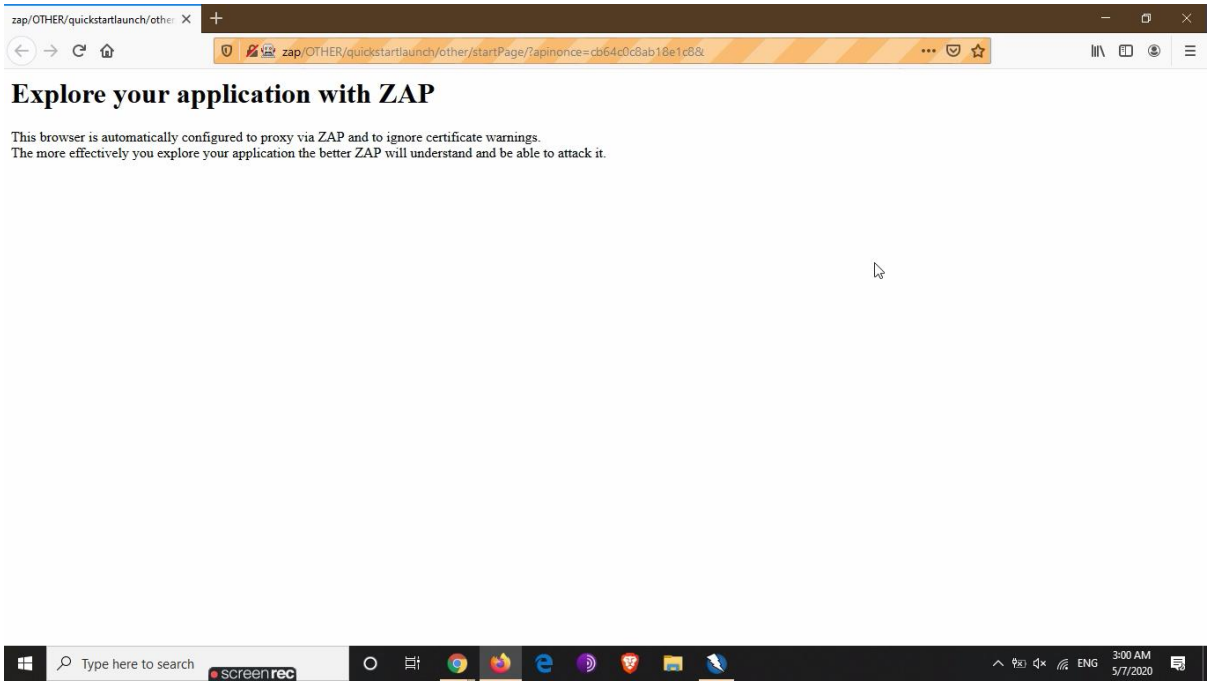
In order to do a scan, a supporting browser should be configured. In this case I use “Firefox” A manual proxy is configured in the web browser as “localhost” and port number as “8080”



Clicking the browser button, The supporting browser tab can be opened.

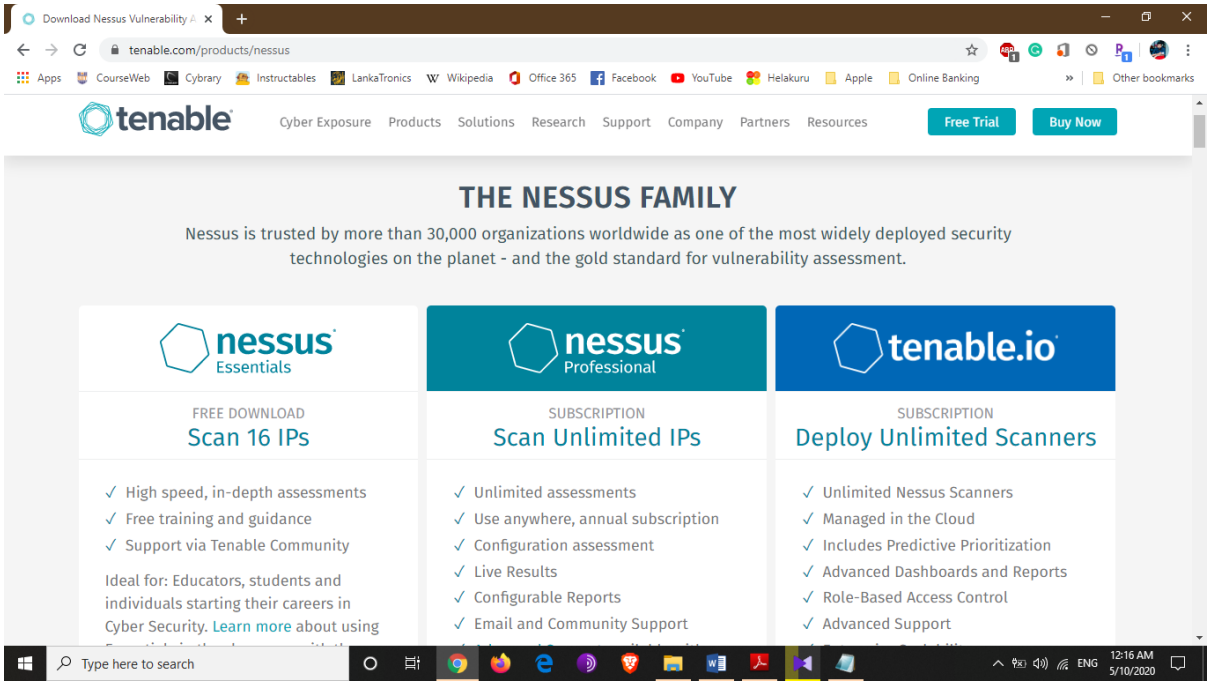


There is a visible difference in supporting browser tab, the address bar is having a different design than in a normal browser tab.

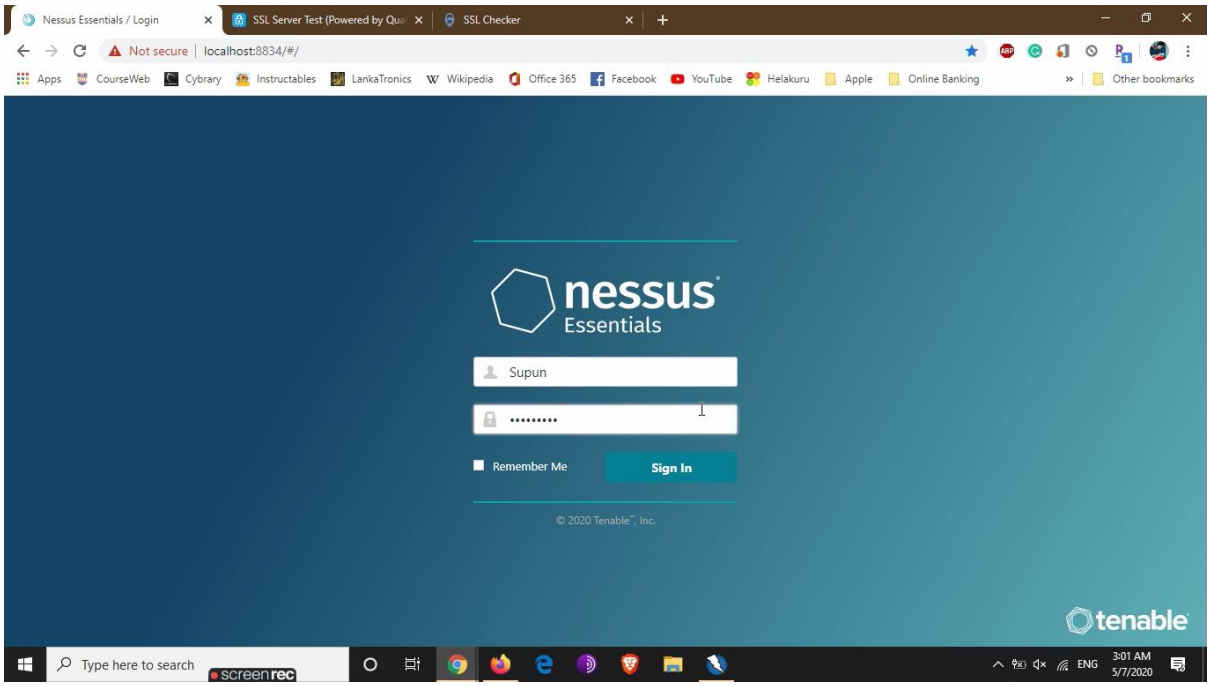


3.2. Nessus

This is going to be the second tool that I'm using to perform this auditing. This is a commercial tool which can be downloaded from the Tenable website.[6]. A free version named "Essential" is available with full privileges for 16 scans.

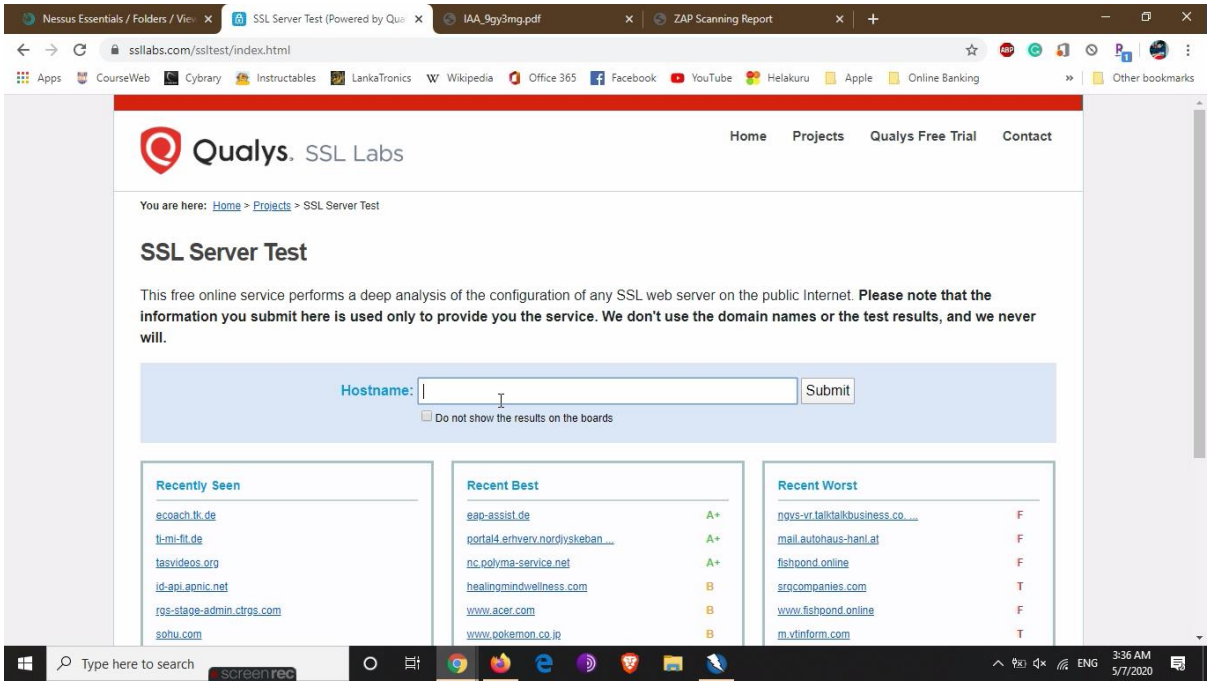


This is how the Nessus home screen looks like. Nessus doesn't need to manually configure a supporting browser it automatically opens with default web browser. Then signed in using credentials.



3.3. Qualys SSL Labs

This is the third tool that I'm using to perform this auditing. This is a website which is doing SSL and Certificate tests for websites. It gives a grading for websites which are scanned. Simply, the URL should be typed in the "Hostname" bar and Submit.[7]

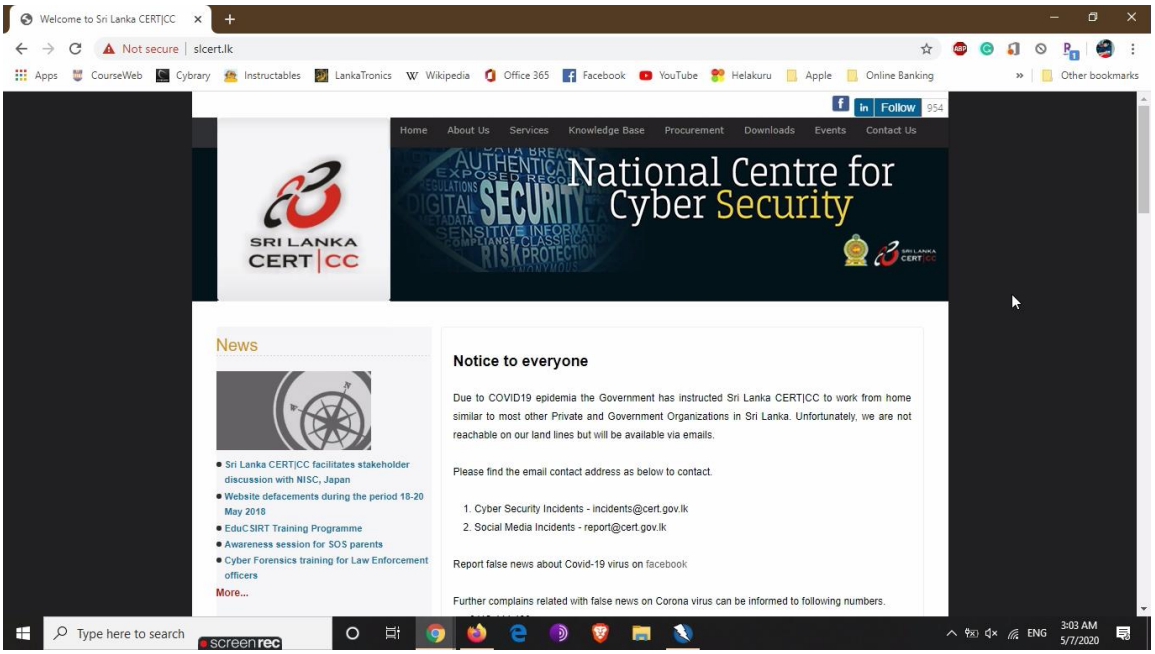


4. Sample Websites

I'm using two websites owned by Sri Lankan and Foreign organizations for auditing and have a clear idea of them by comparing.

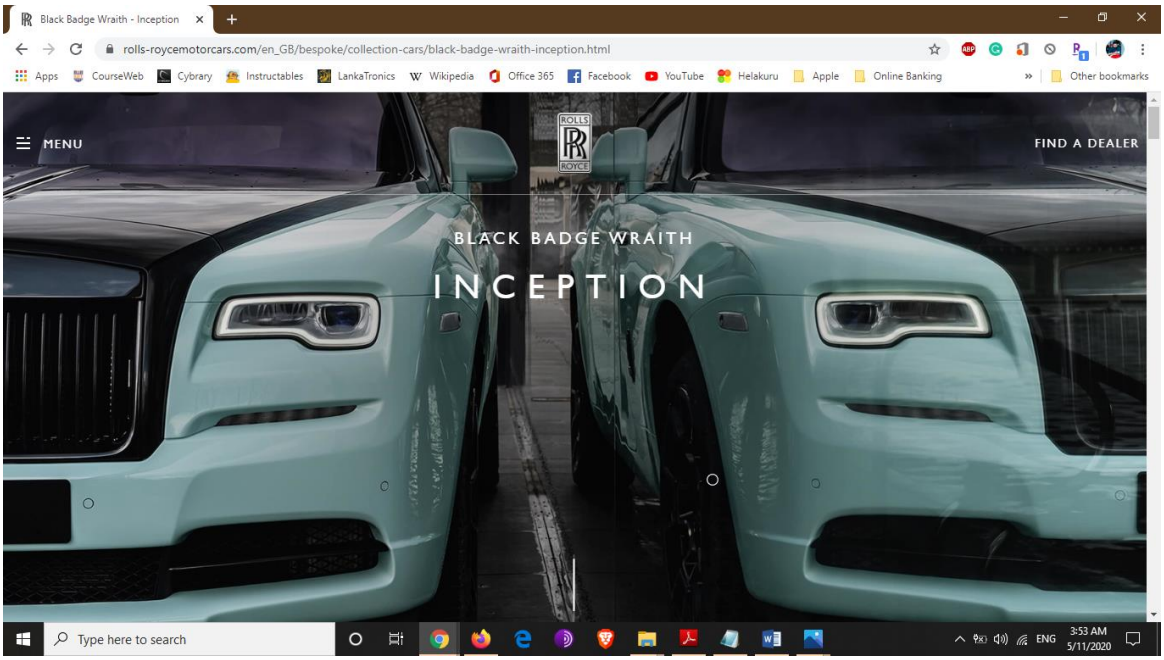
4.1. Sri Lanka Computer Emergency Response Team (SLCERT)

First website is SLCERT. It is the major organization regarding Cyber Security in Sri Lanka which is the "National Centre for Cyber Security". Headquarters located in Bandaranaike Memorial International Conference Hall, Colombo 07.[8]



4.2. Rolls-Royce Motor Cars

Second website is owned by the car manufacturer who produces the most expensive and luxurious cars, the Rolls-Royce. Headquarters located in Goodwood, England.[9]

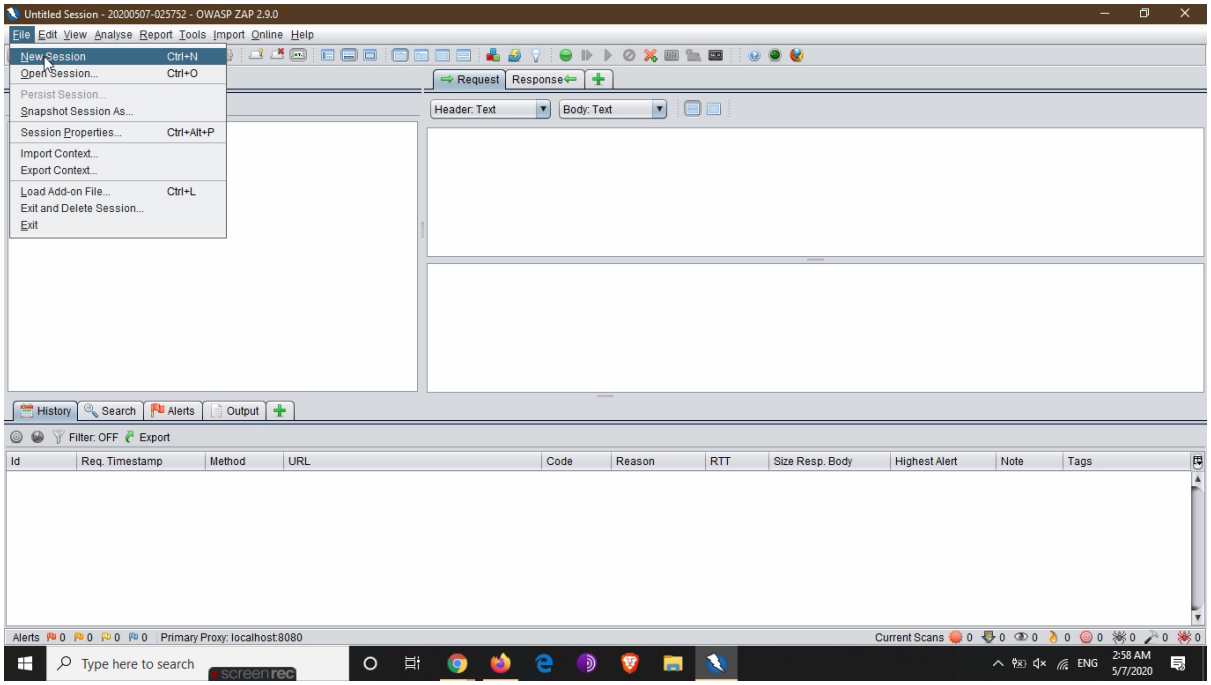


5. Audit - Website Scanning

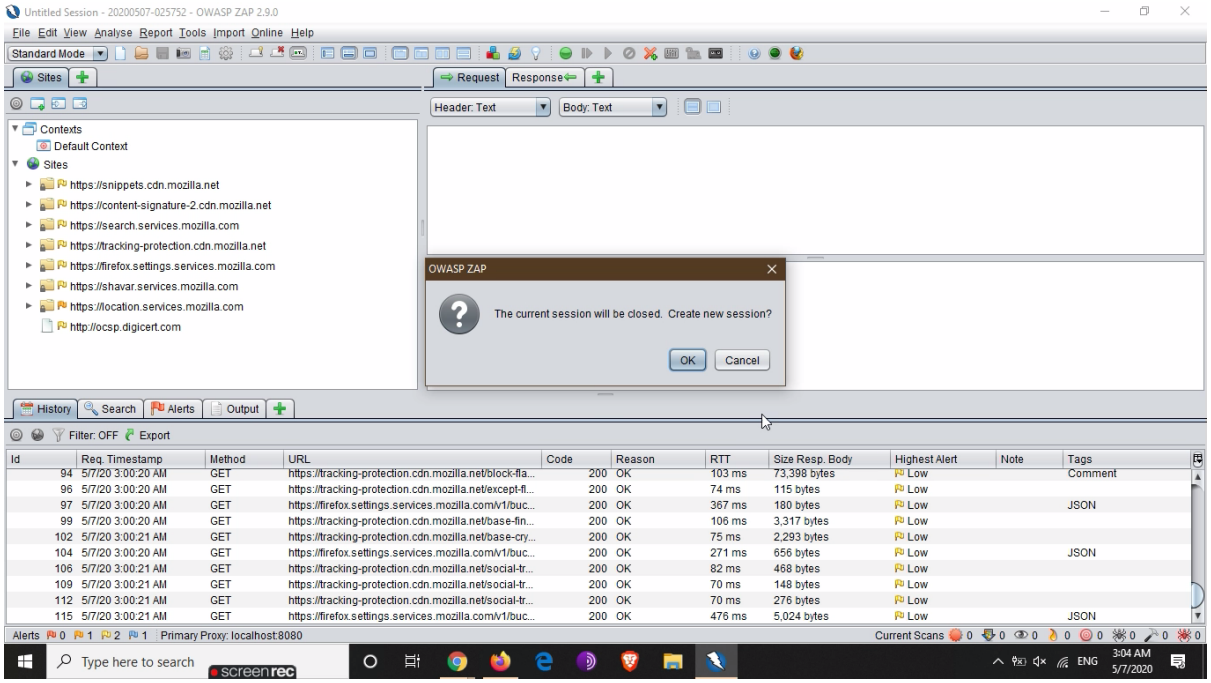
The aim is to find vulnerabilities and misconfigurations of these sample websites. On the other hand, we can have a comparison between websites.

5.1. SLCERT Website Scan - ZAP

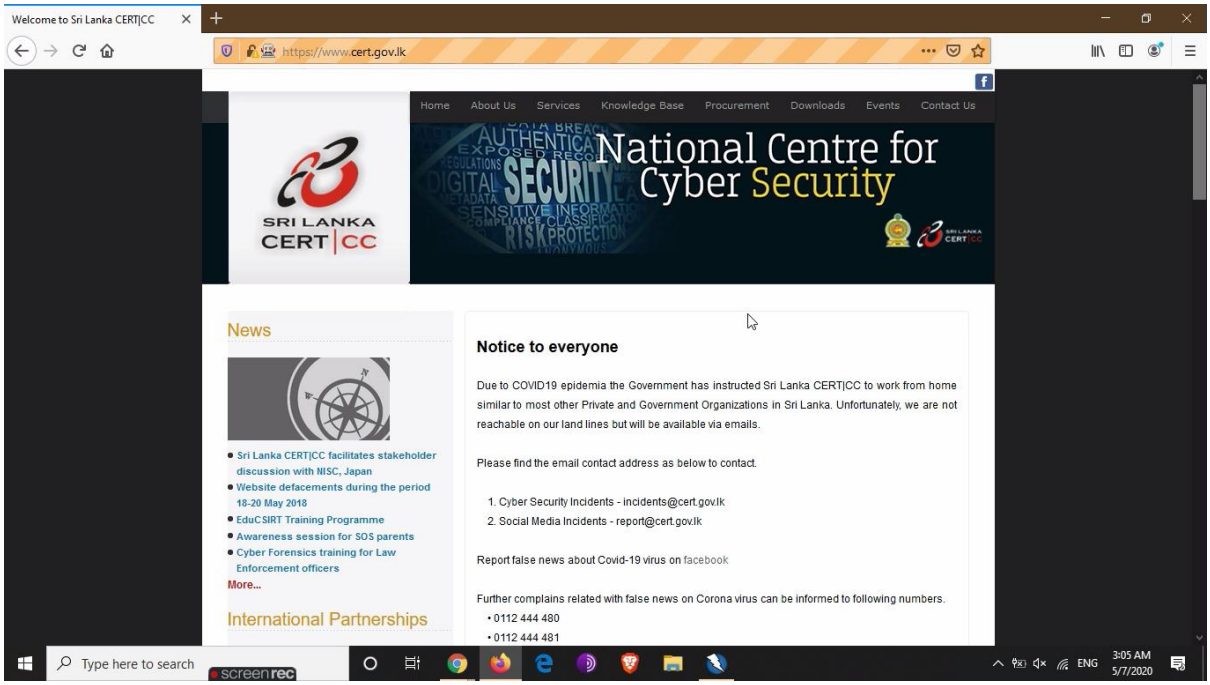
A new session should be started in order to scan the website.



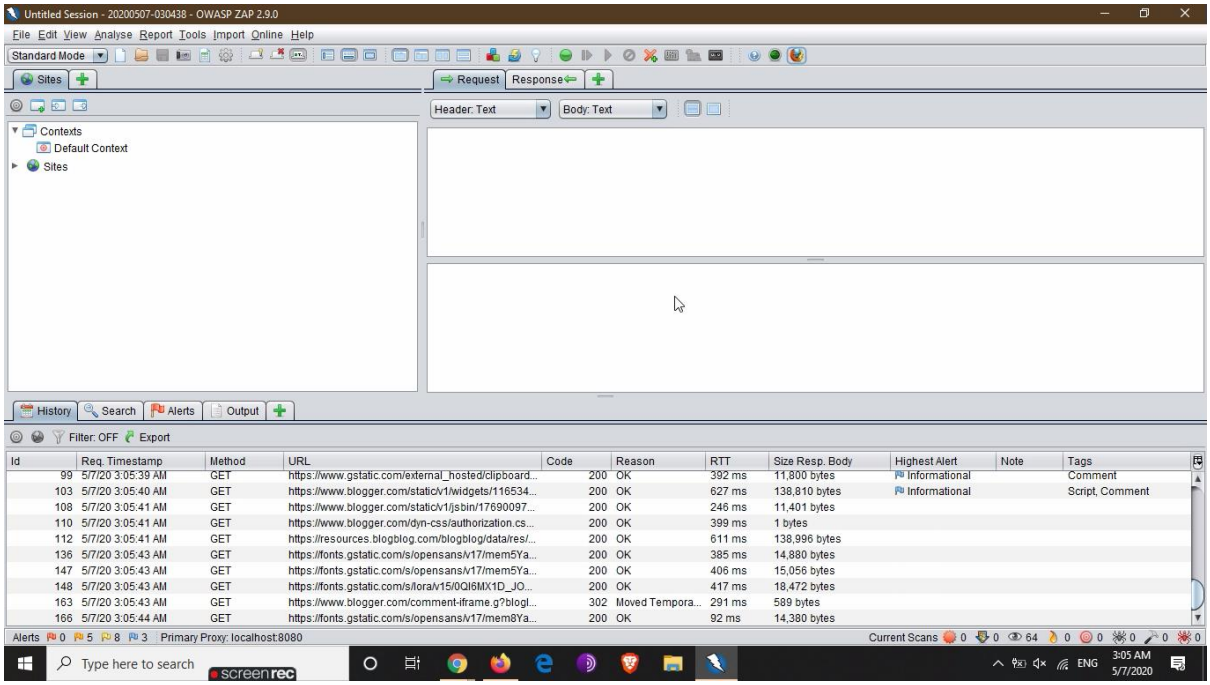
If there is a previous session, it will be closed before starting a new one.



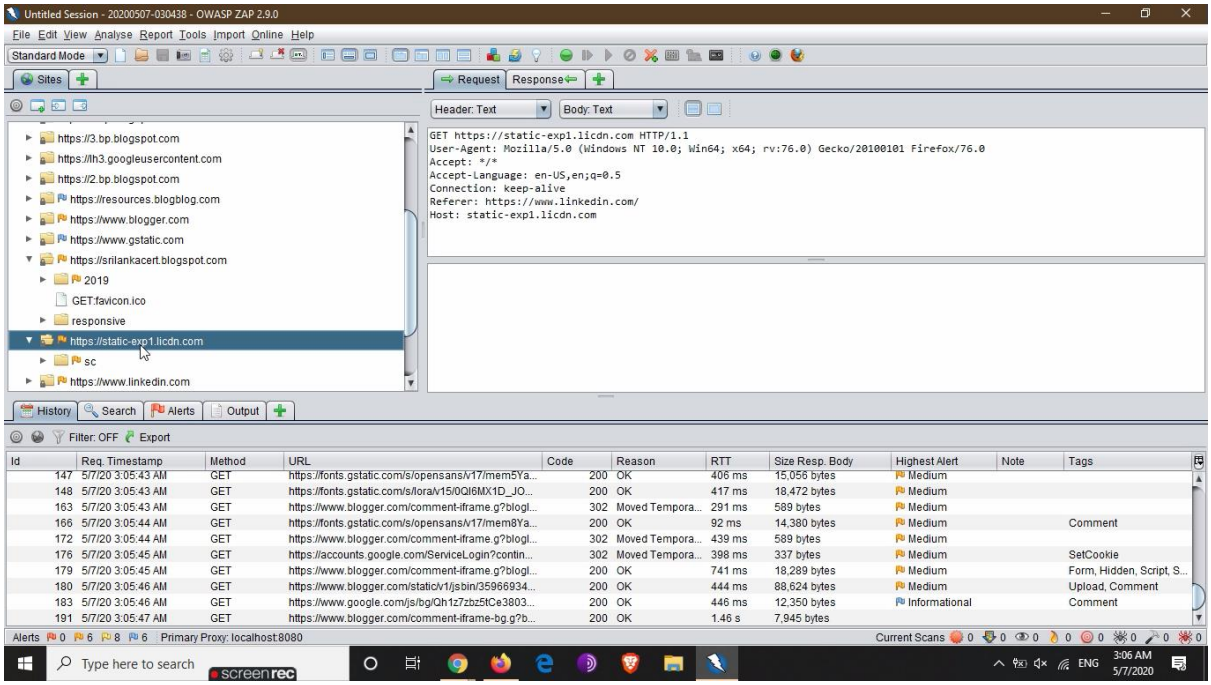
Go to the supporting web browser by clicking the web browser icon on the tool. Then give the URL, “www.cert.gov.lk”



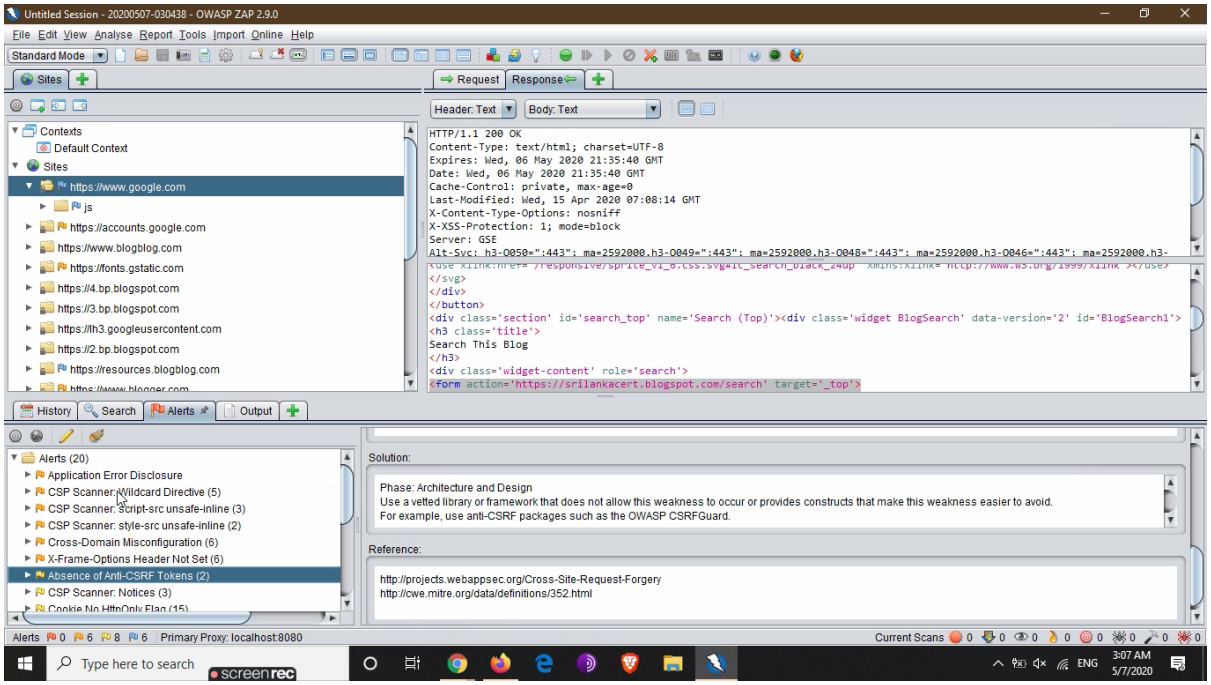
The scanning is started automatically in the application side.



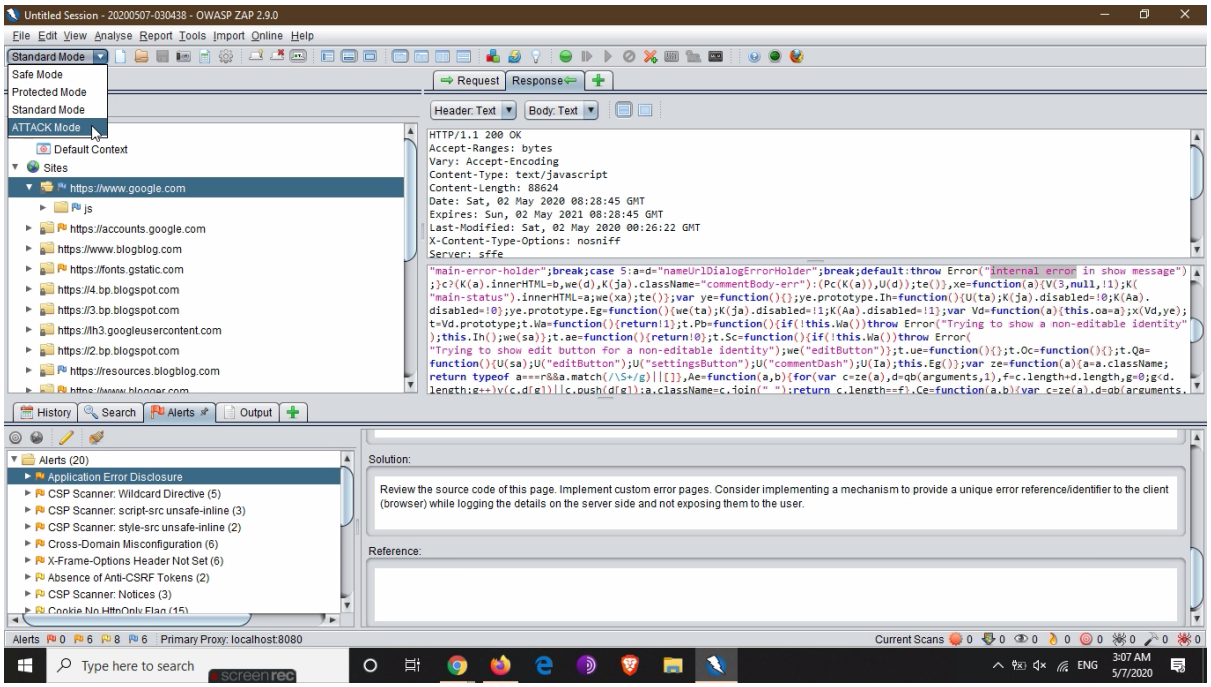
Number of found vulnerabilities are appeared Alerts bar below the application.

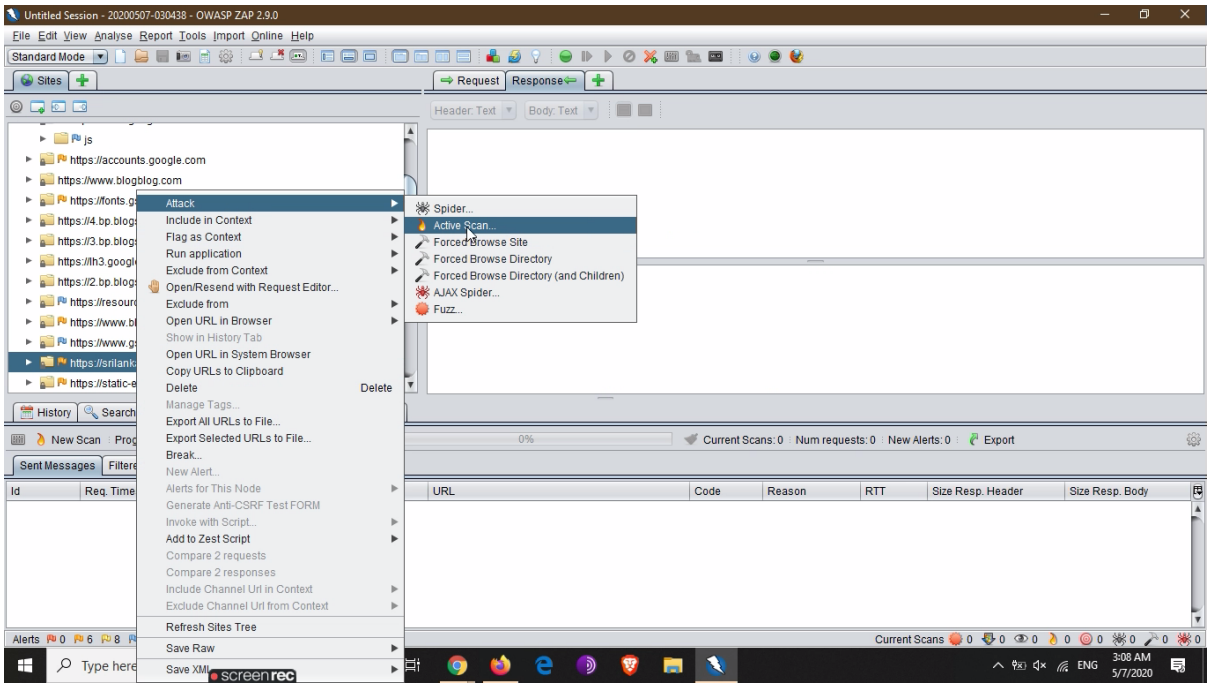


Click on a particular flag and then the part of the code is shown which the vulnerability is included along with the solution.

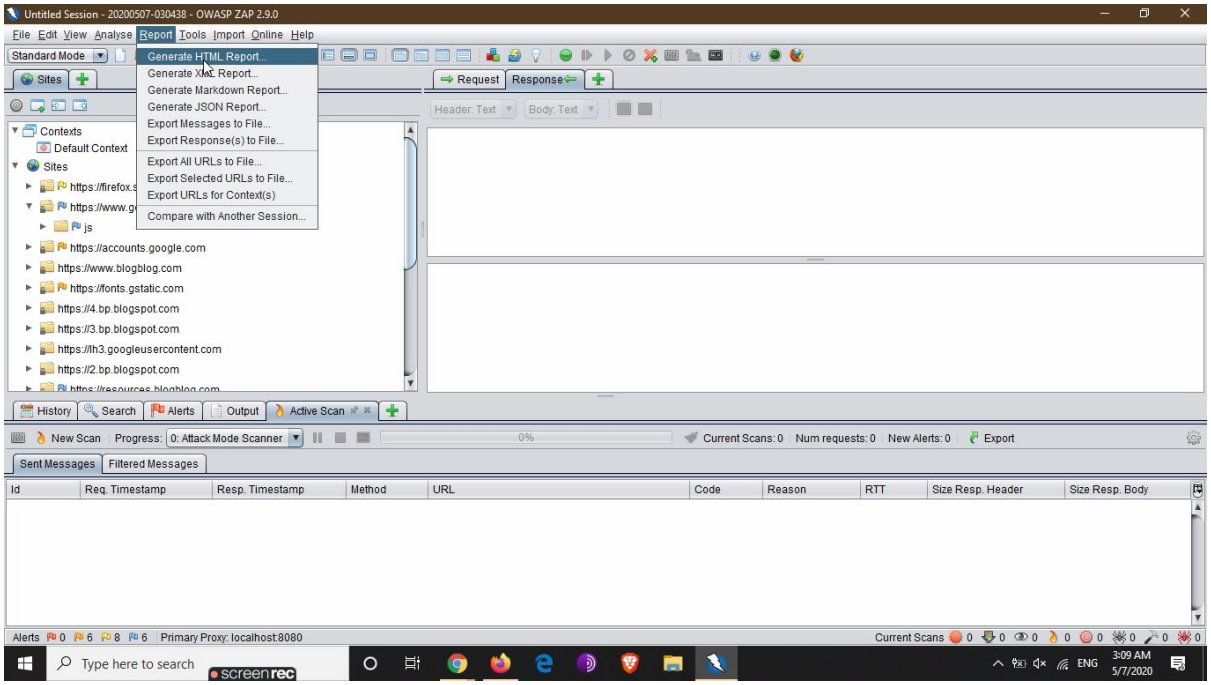


For now, only a “Passive Scan” was done. If a deeper scanning is needed, “ATTACK Mode” and “Active Scan” can be used. But, for now it is not allowed. Since, I’m doing this without the permission of the SLCERT.

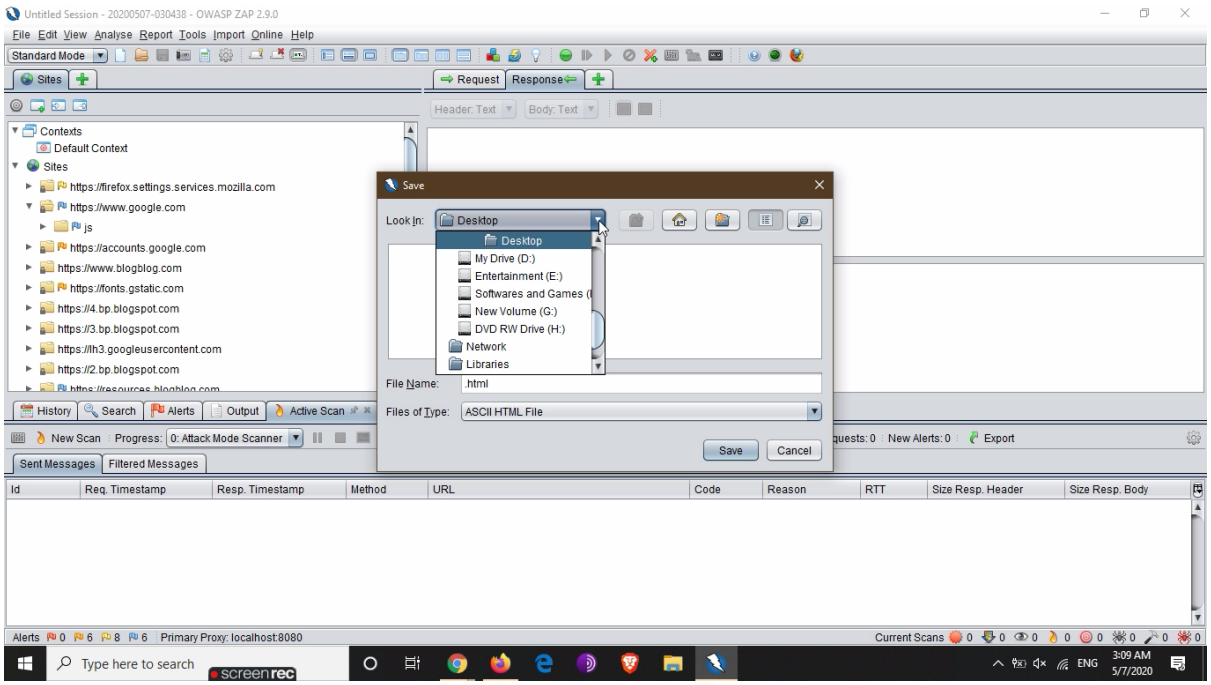




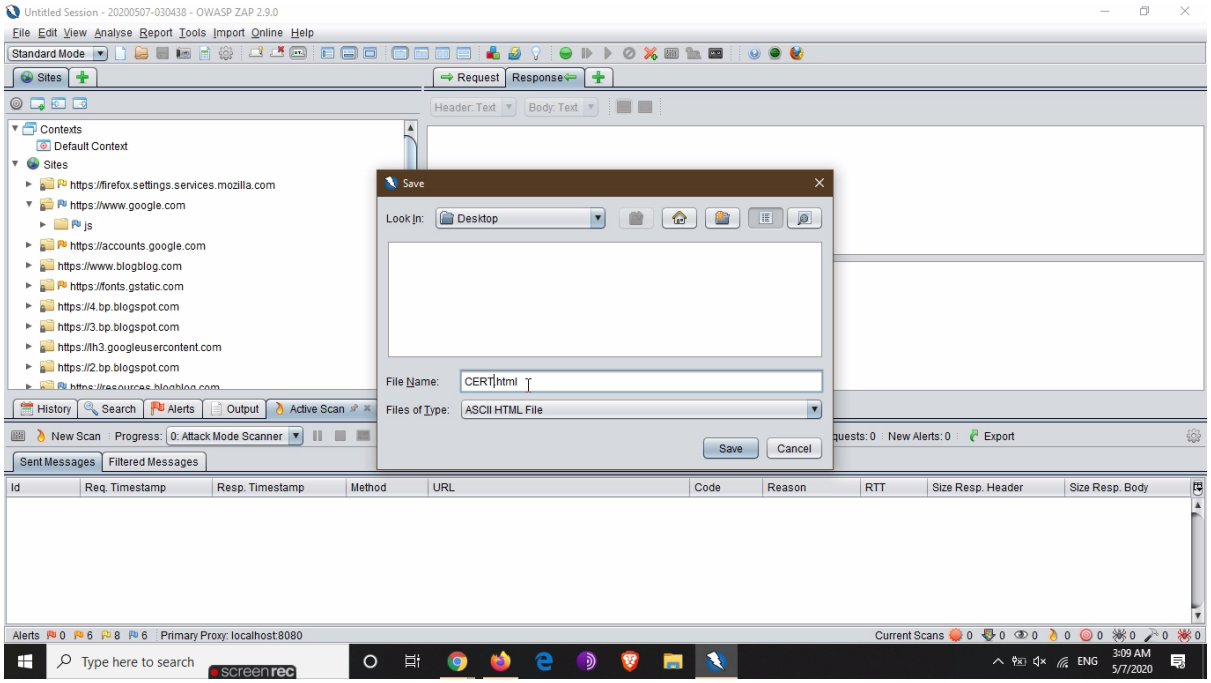
A Detailed Report can be generated using the Report tab.



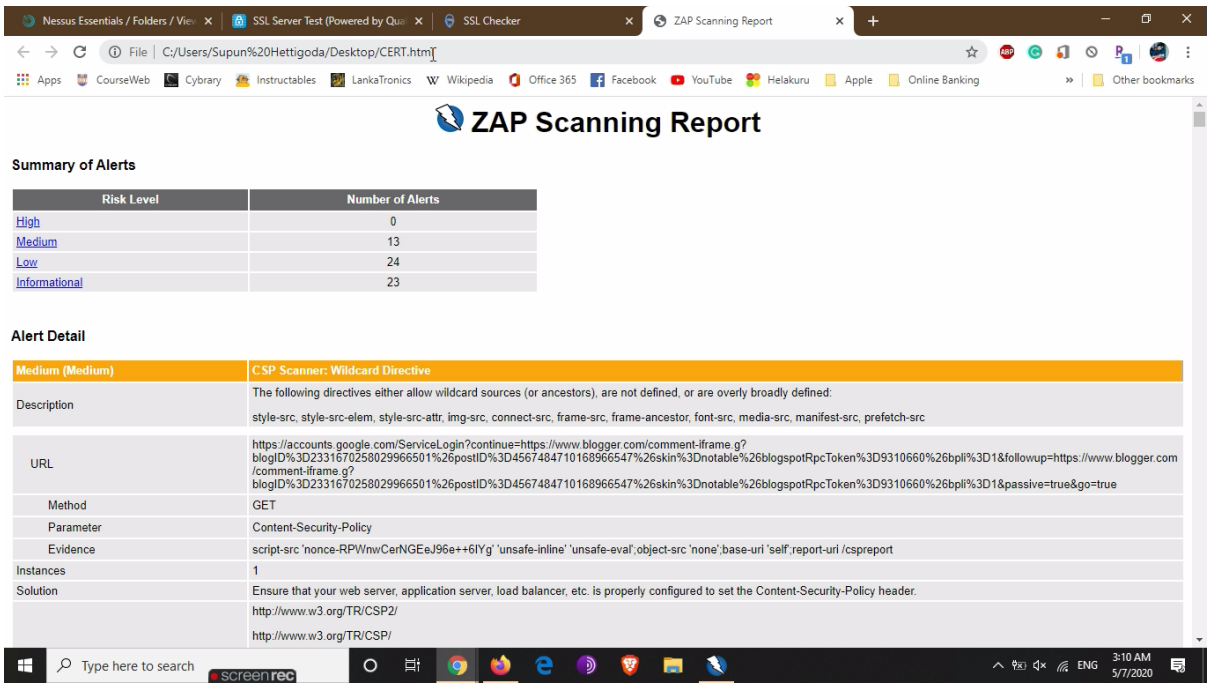
File location should be selected.



A file name should be given. Then click “Save”.

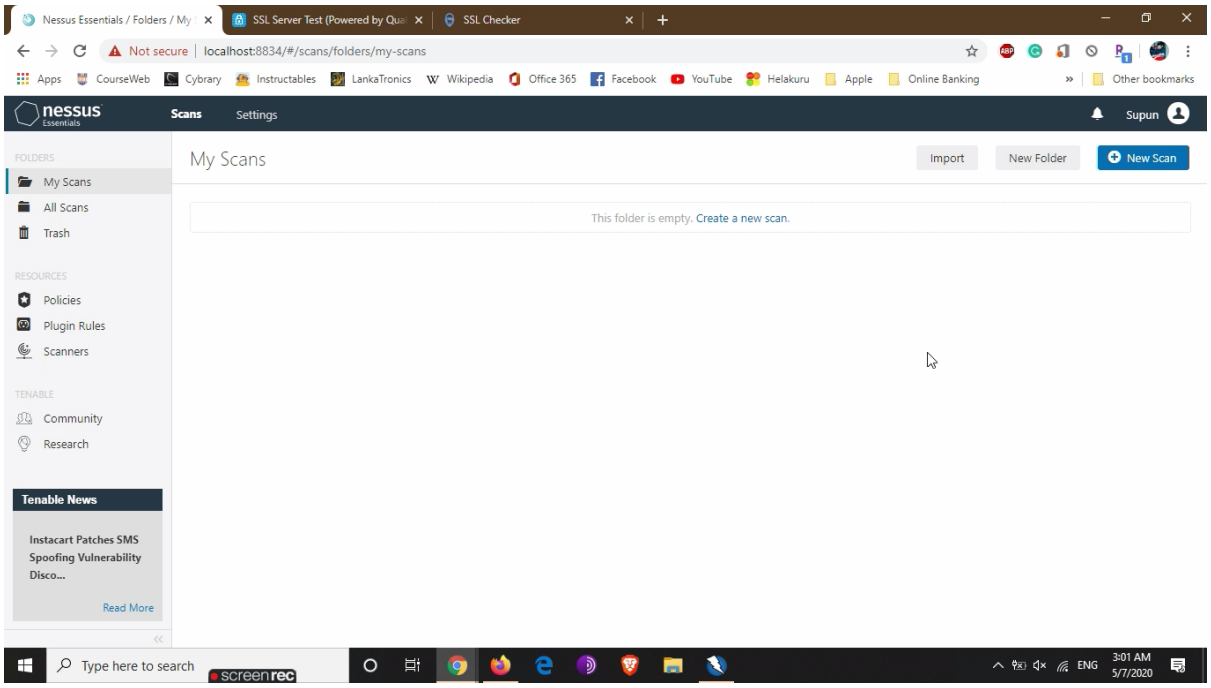


Then the report which is having .html format will be opened using the default web browser. Report shows there are 13 of Medium level security alerts, 24 of Low level security alerts and 23 of Informational level security alerts were generated according to those vulnerabilities. The description of the vulnerability and solution is also given by the report.

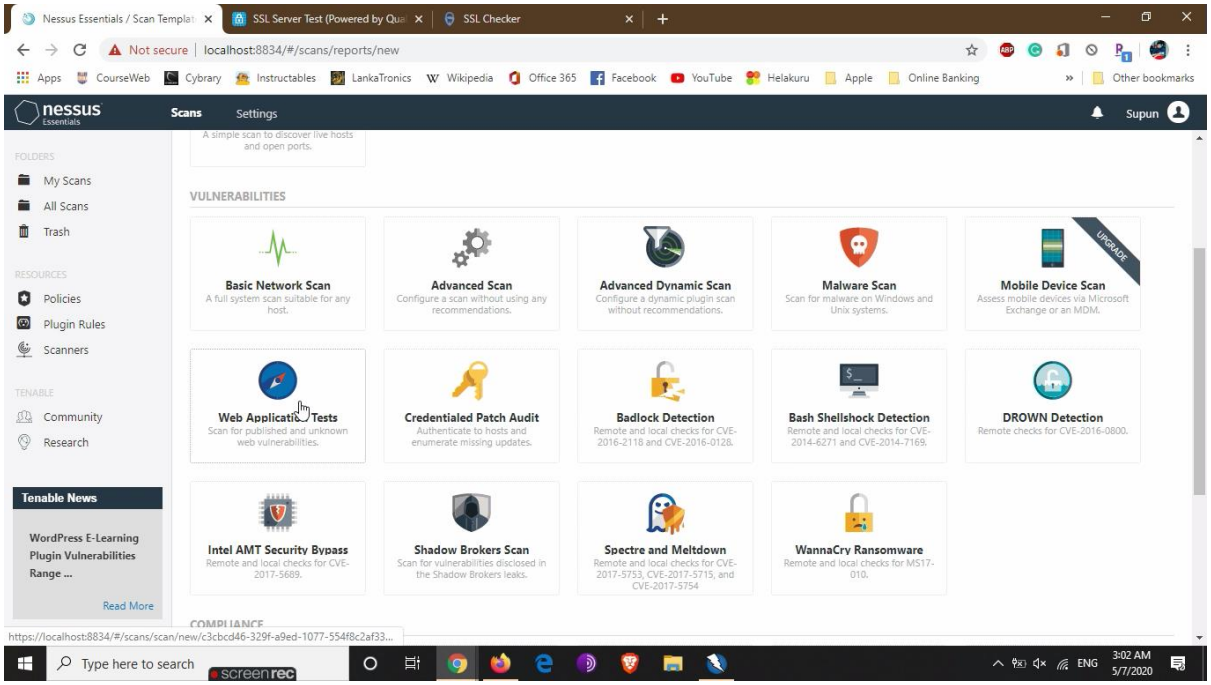


5.2. SLCERT Website Scan - Nessus

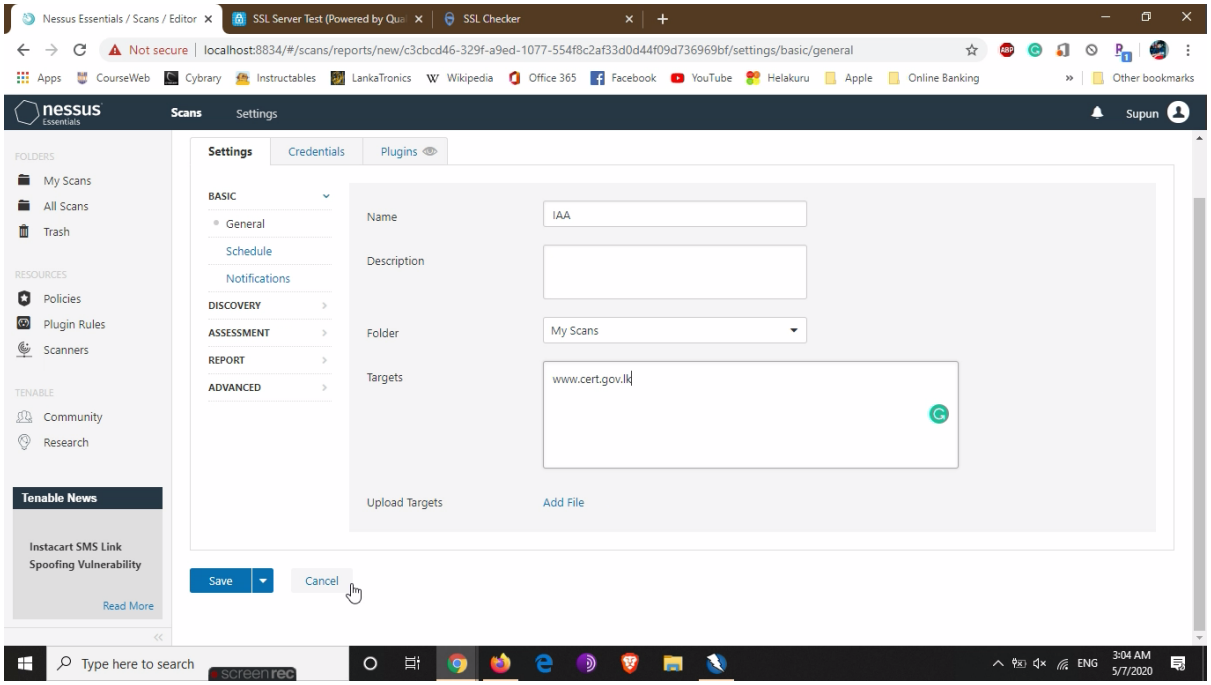
A new scan should be configured by clicking the “New Scan” button.



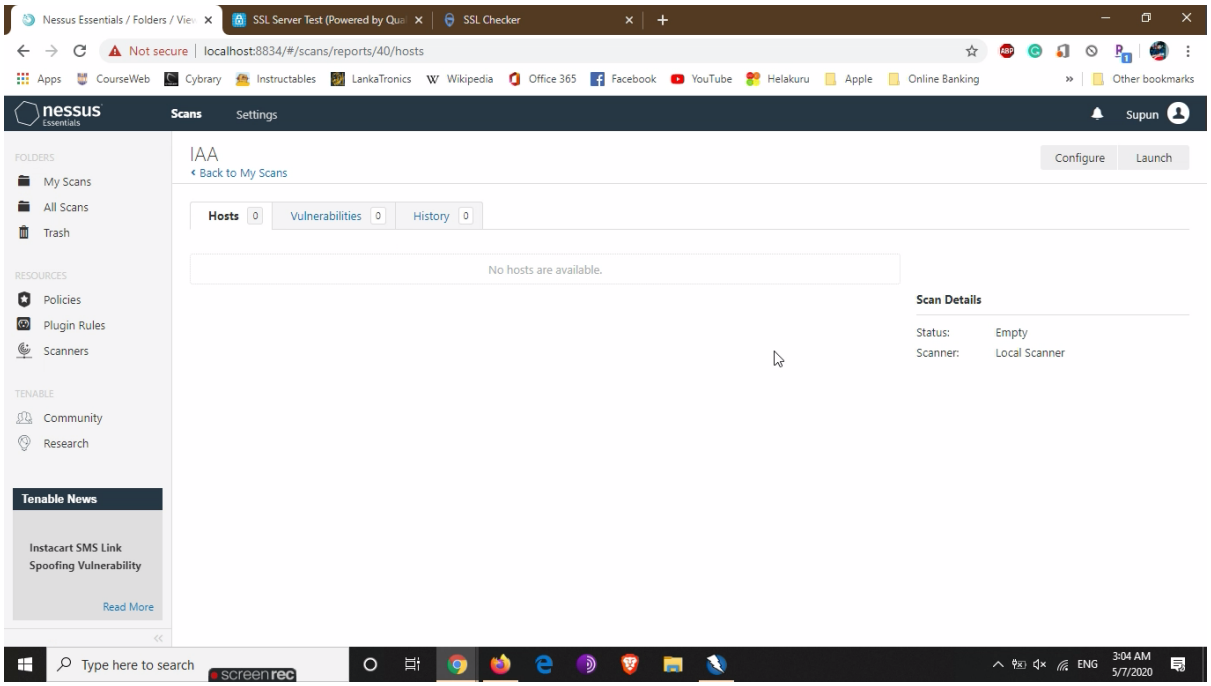
Since we are doing a website scan, “Web Application Tests” should be selected.



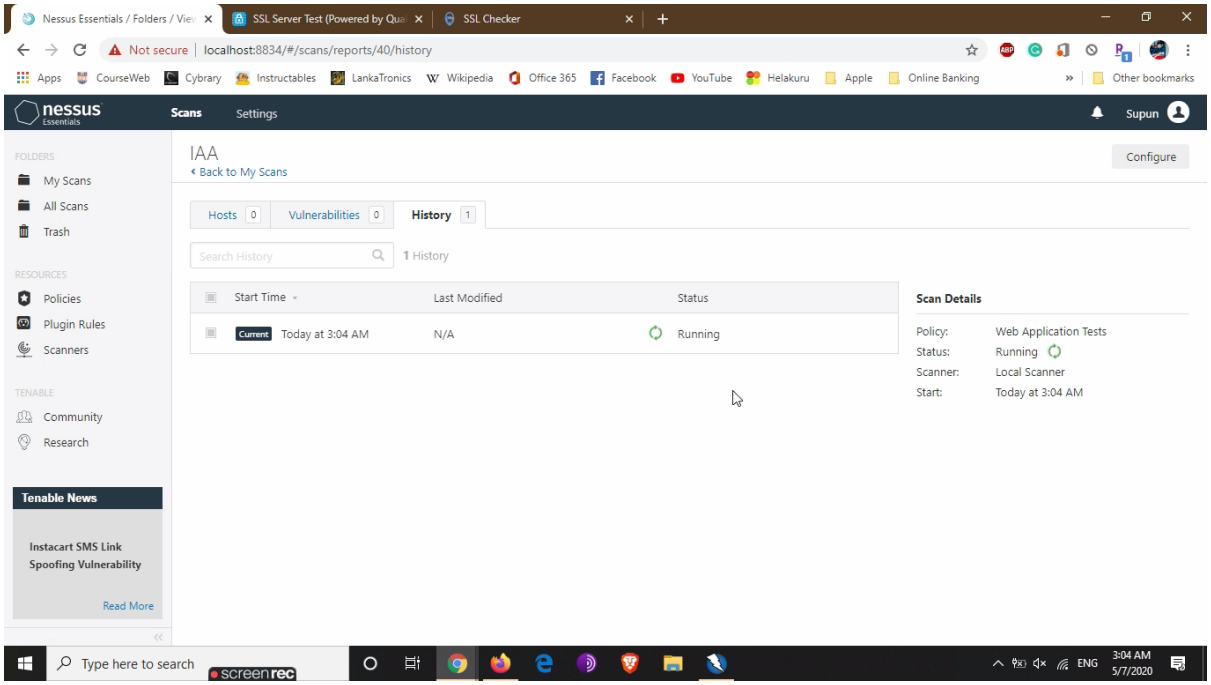
A Name and the URL should be given for the scan as the “Name” and “Target” respectively.



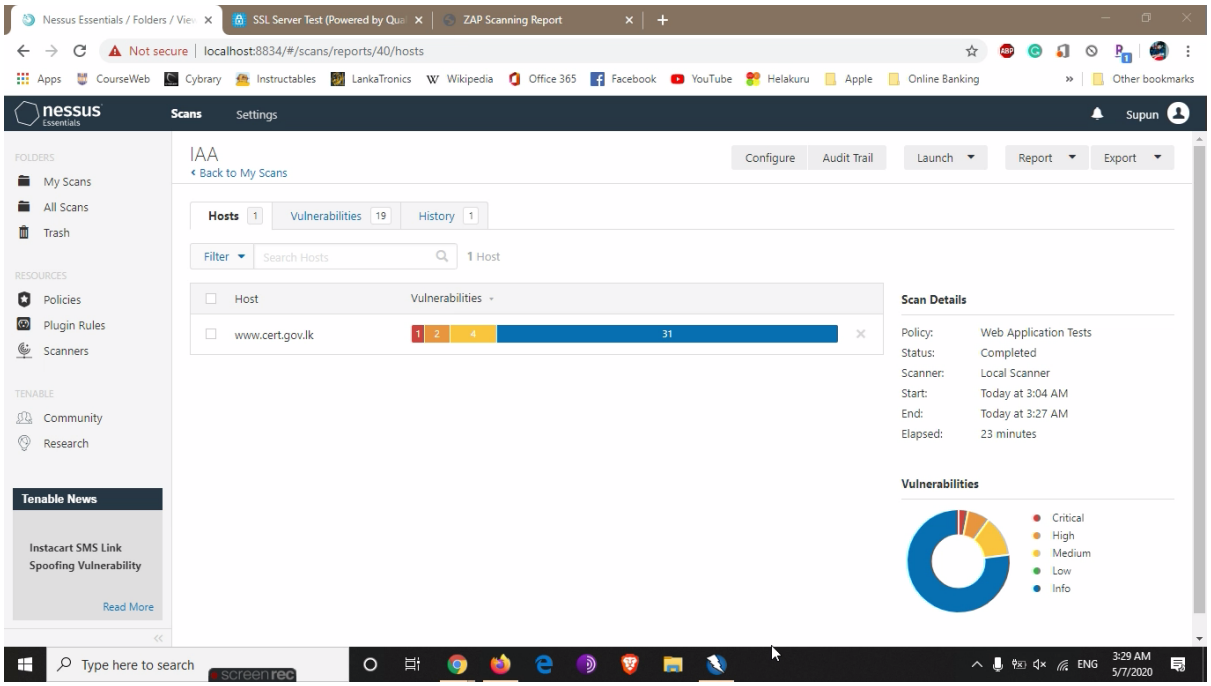
Then the scheduled scan is shown. It can be started by clicking “Launch”



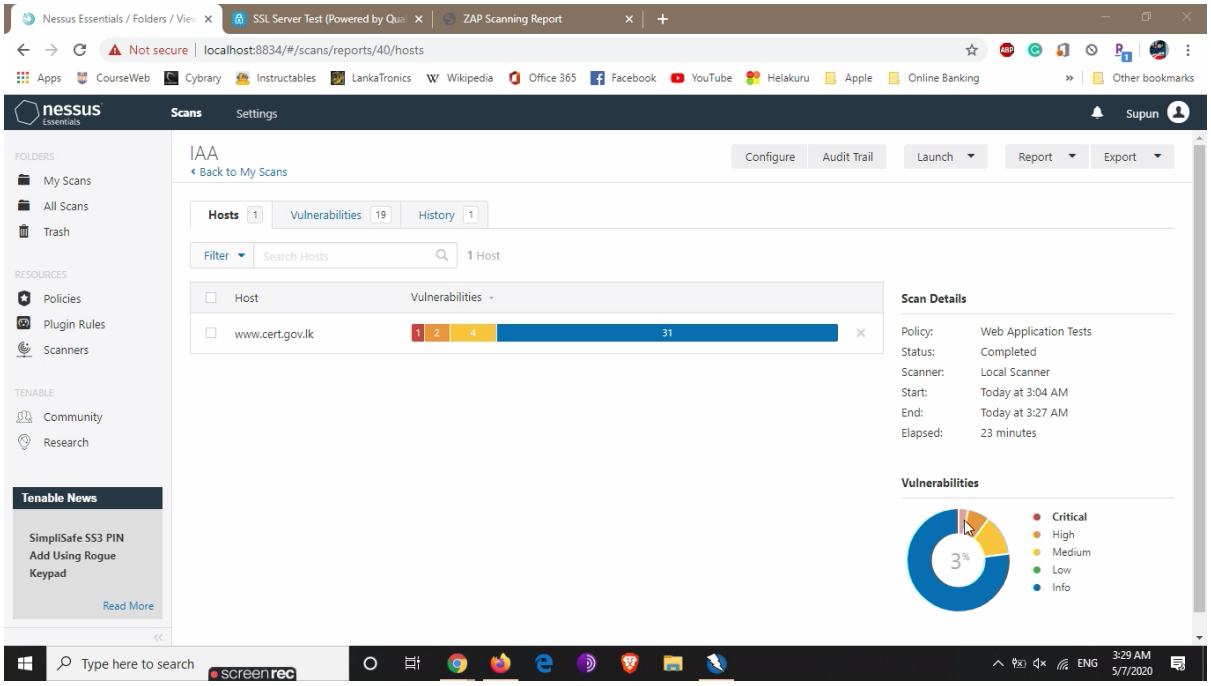
The scan was launched.



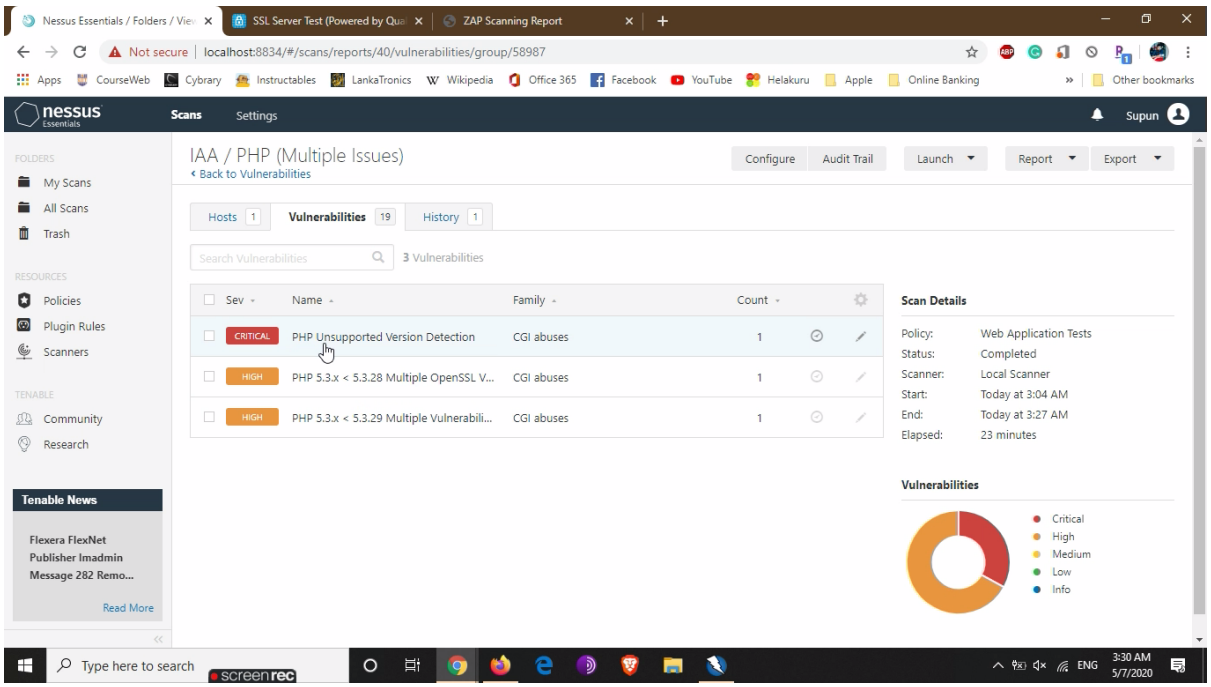
The scan is completed after few minutes. But, sometimes it takes hours.



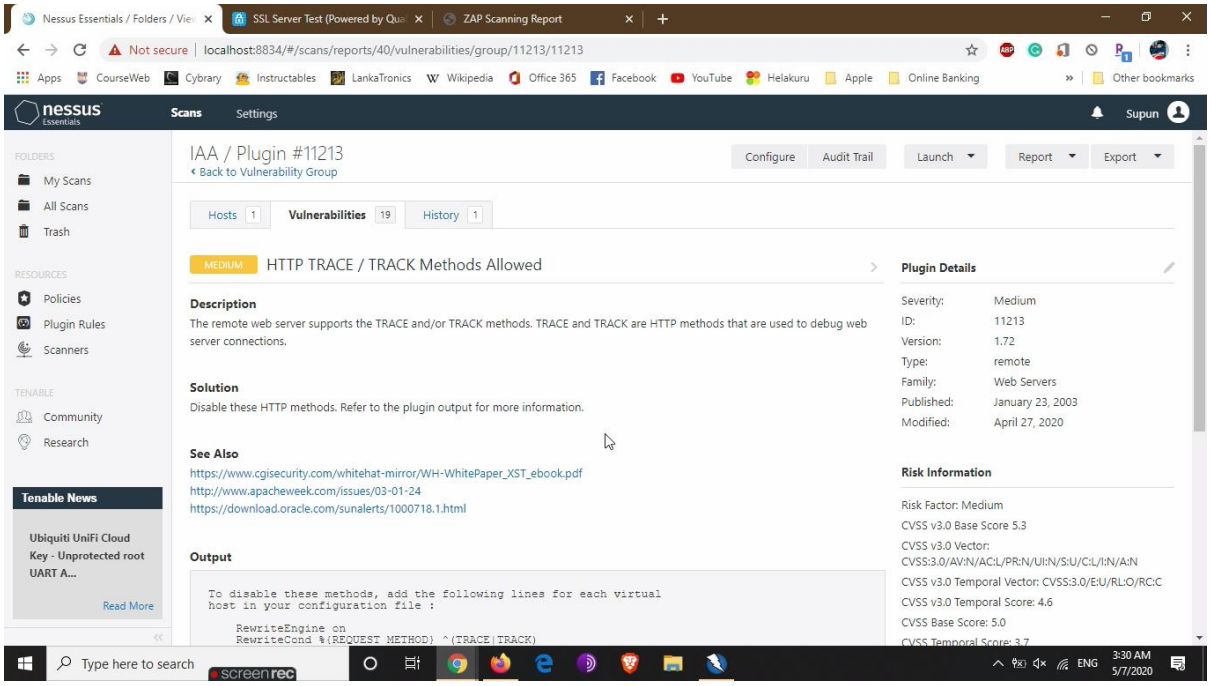
Now, It's a different result. Nessus found a Critical Red Alert vulnerability of the SLCERT website.

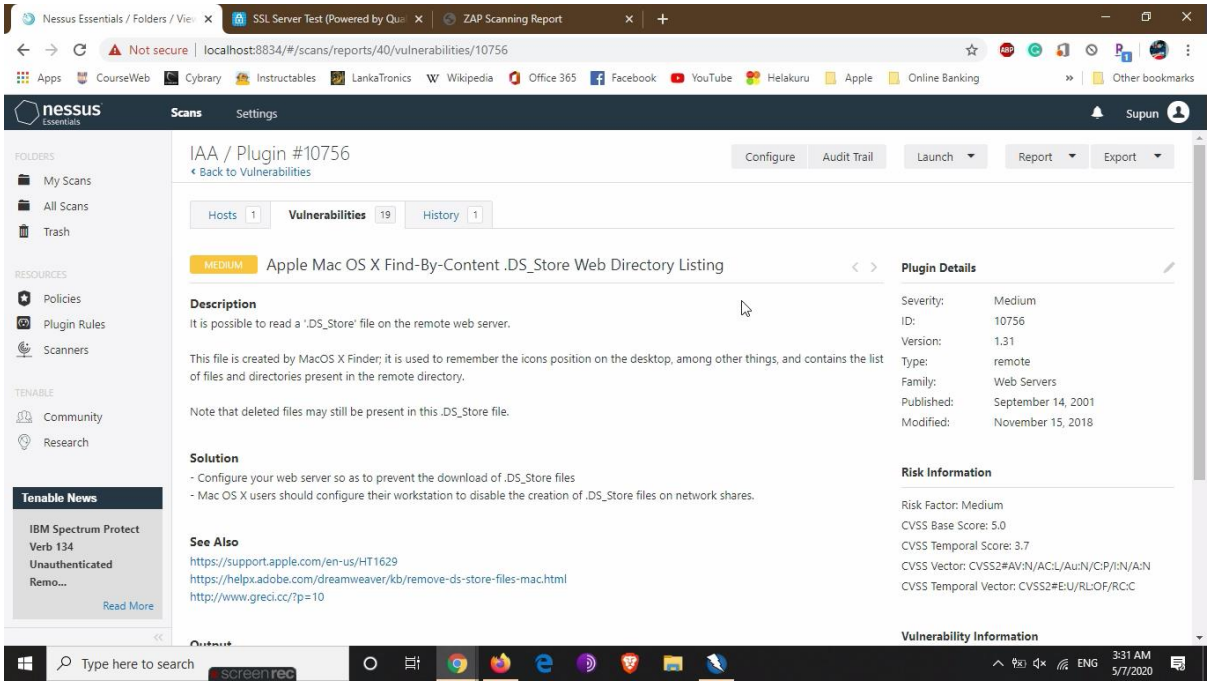


It shows there is an unsupported PHP version is used. It might be outdated. If the version is found by a hacker, the vulnerability will be exploited.

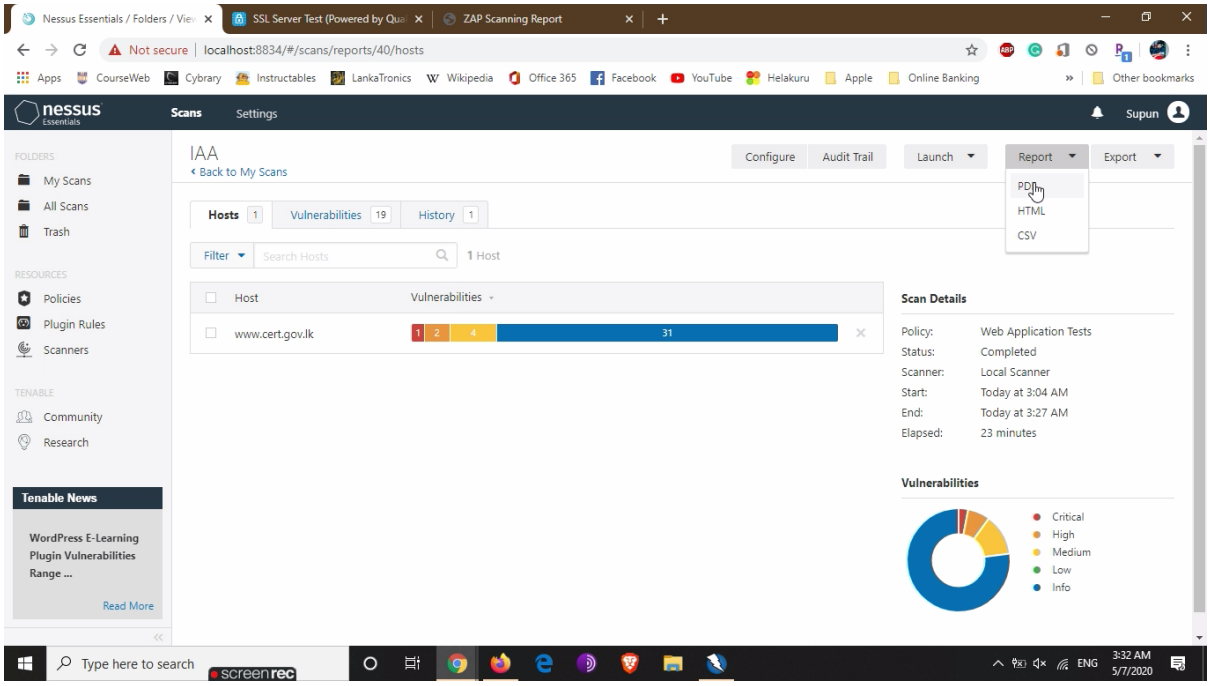


Here are the another two Medium Level security alert for a vulnerability which is having a HTTP issue and a Mac OS regarding issue respectively.

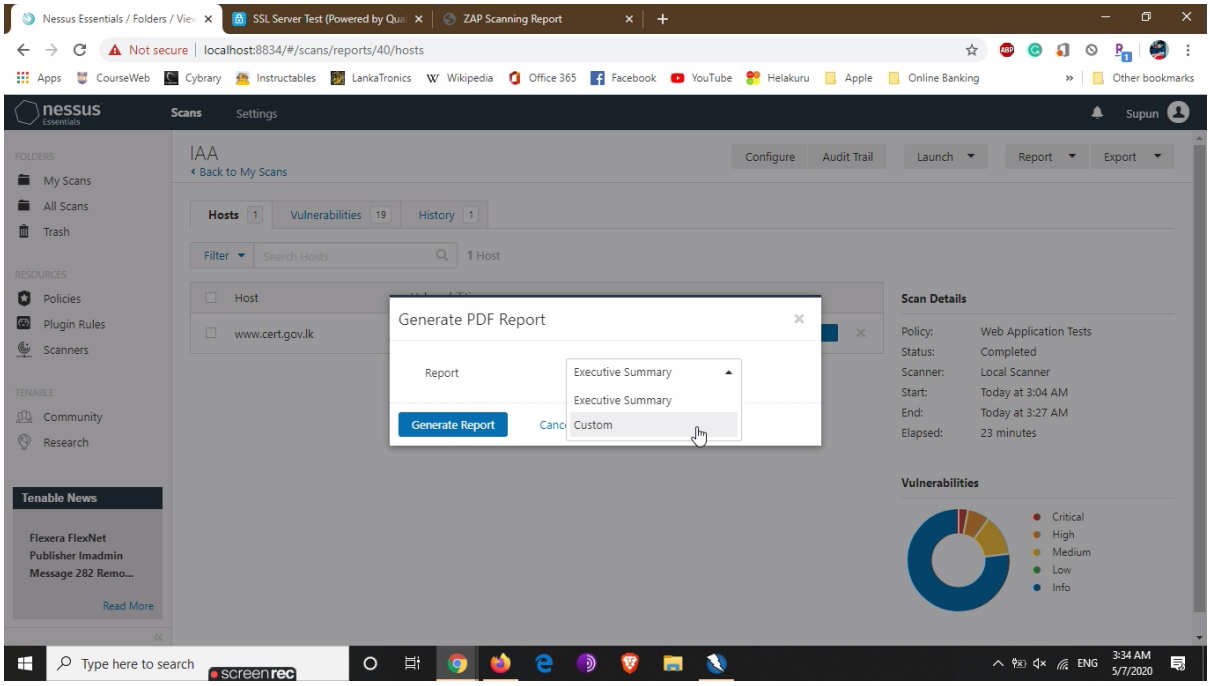




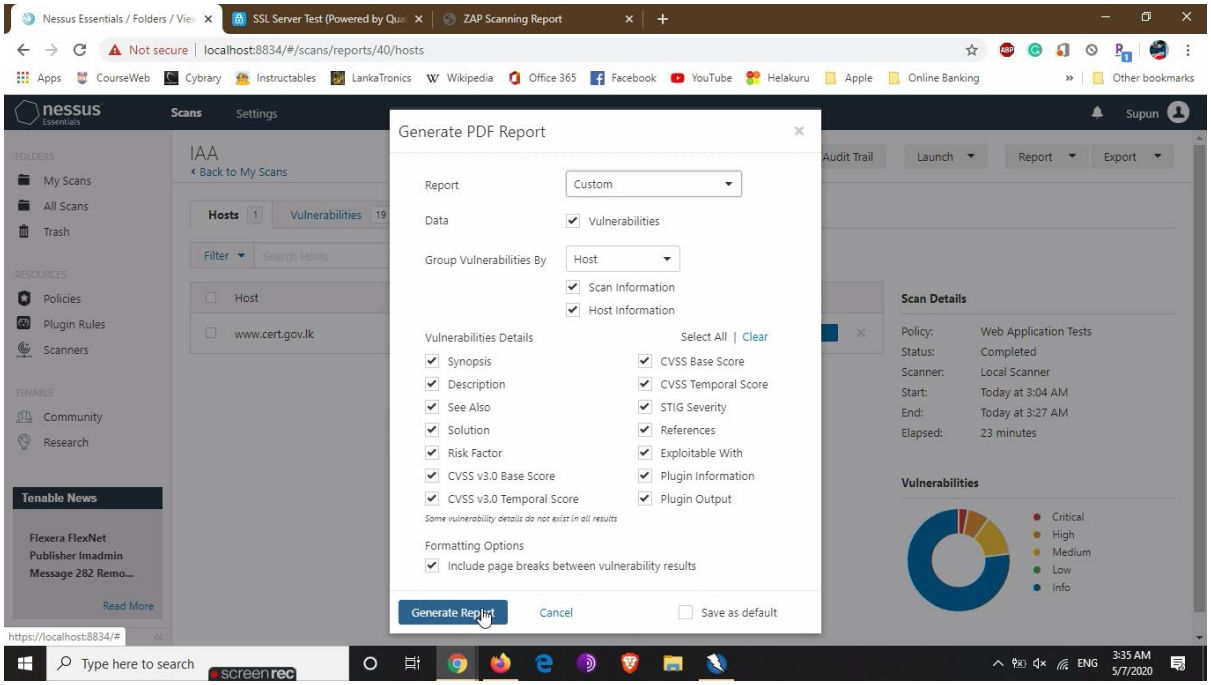
A Report can be generated using the “Report” button which is having PDF format or others. For the ease of use, this time PDF format is selected.



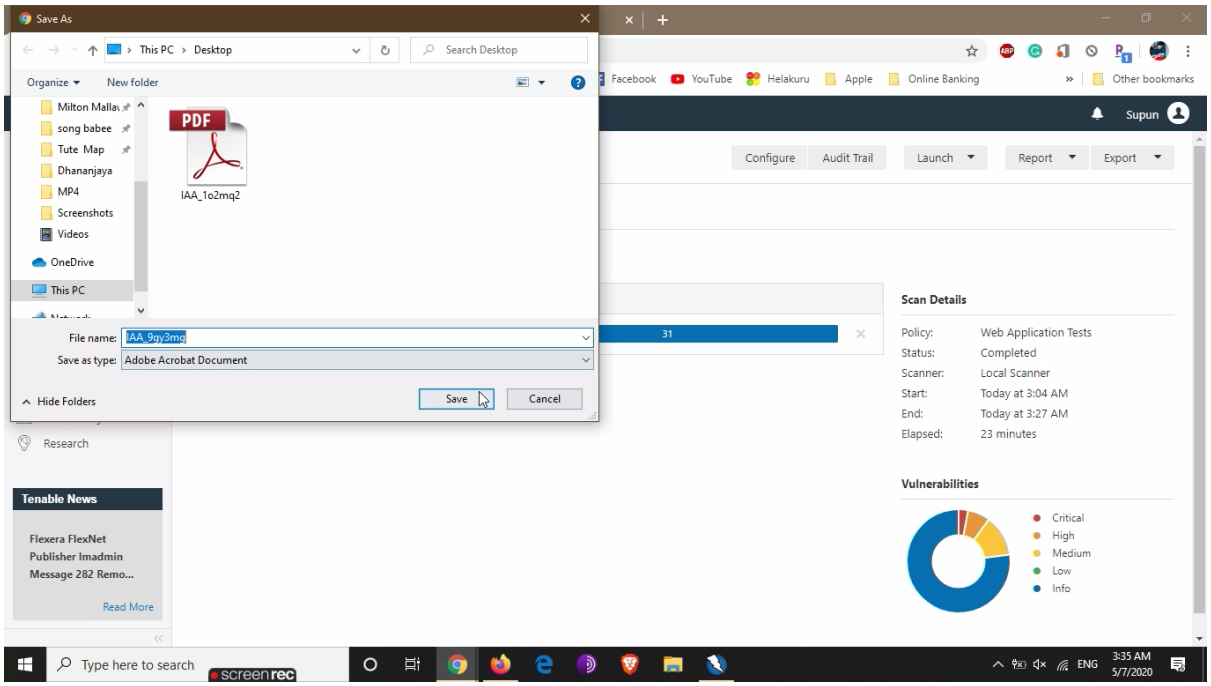
In order to generate a detailed report, “Custom” type should be selected. “Executive Summary” generates only a small summary of the scan which shows plugin details.



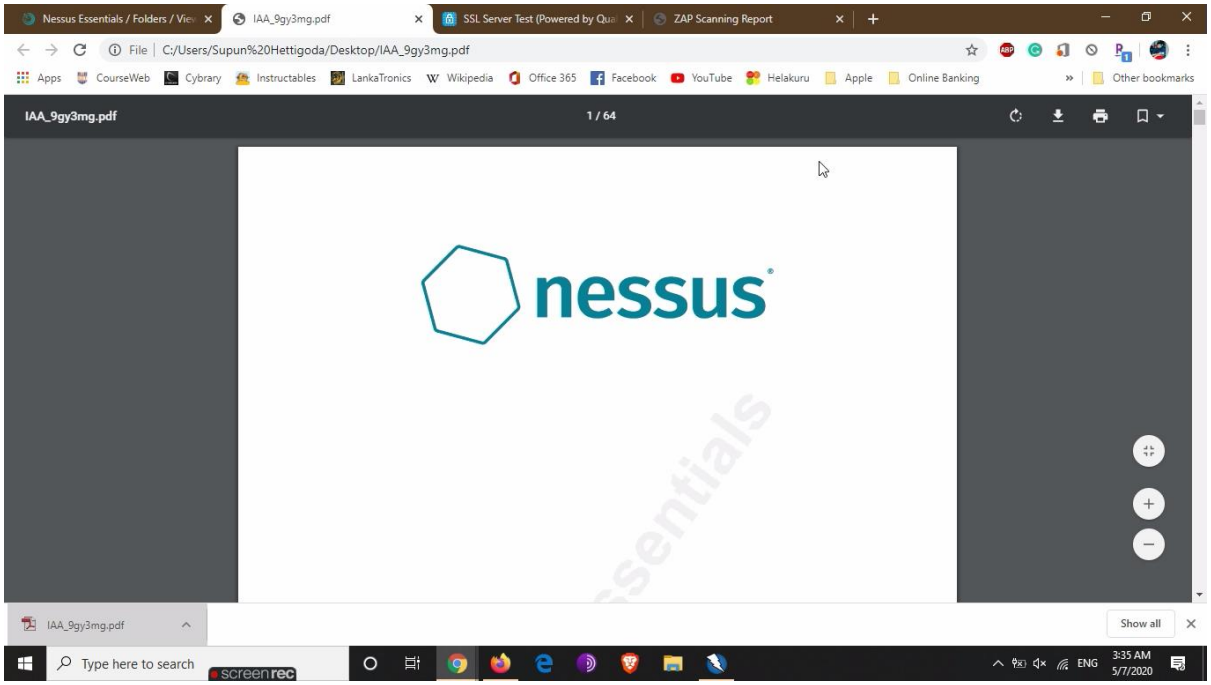
Report can be customized by checking the boxes as the auditor wish.



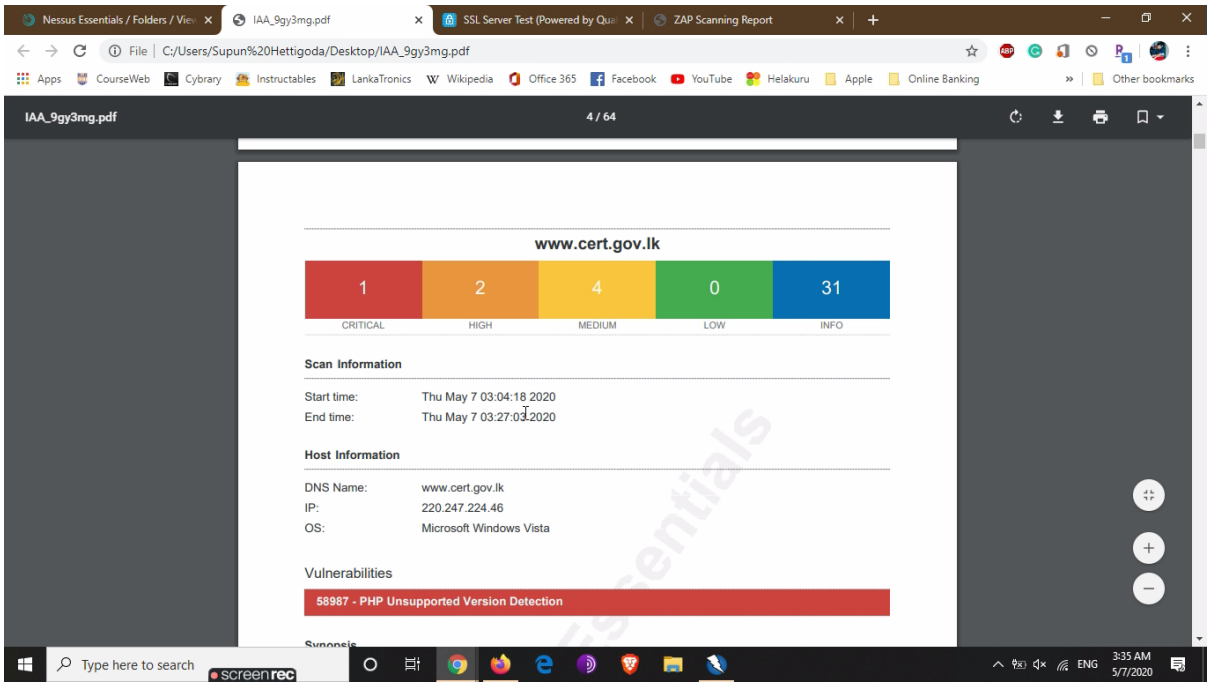
The file location should be selected. A file name also can be given.



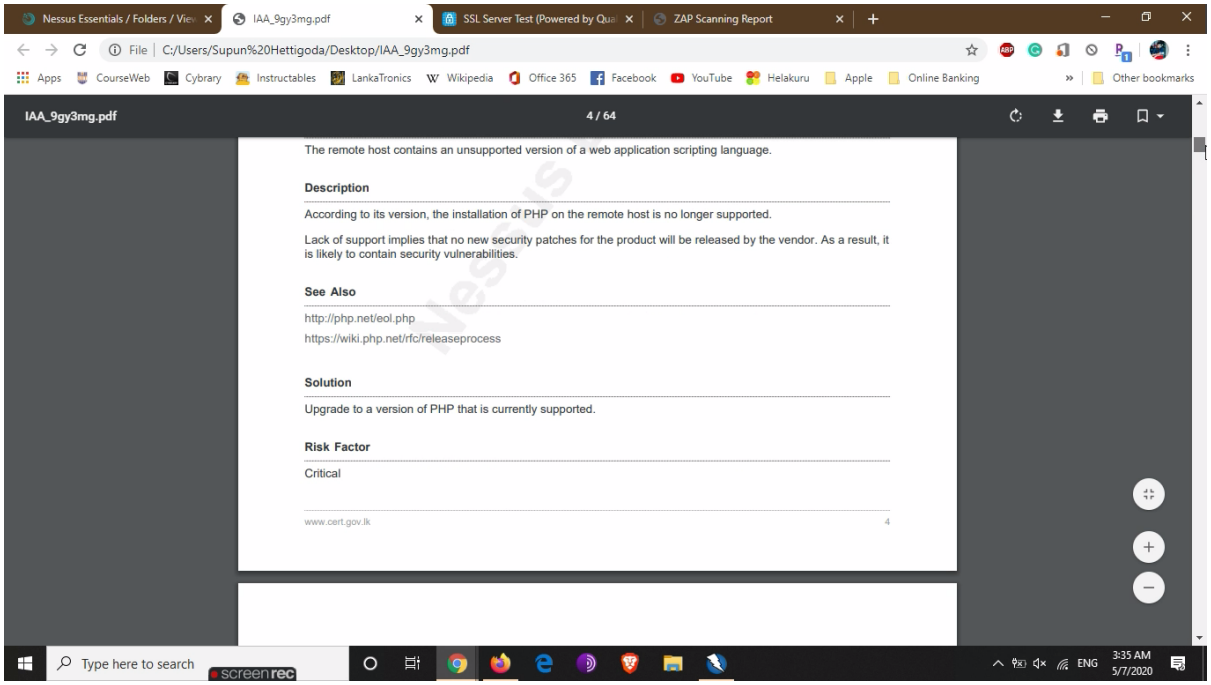
Here is the opening page of the scan report.



Vulnerabilities according to the threat levels are clearly shown here.

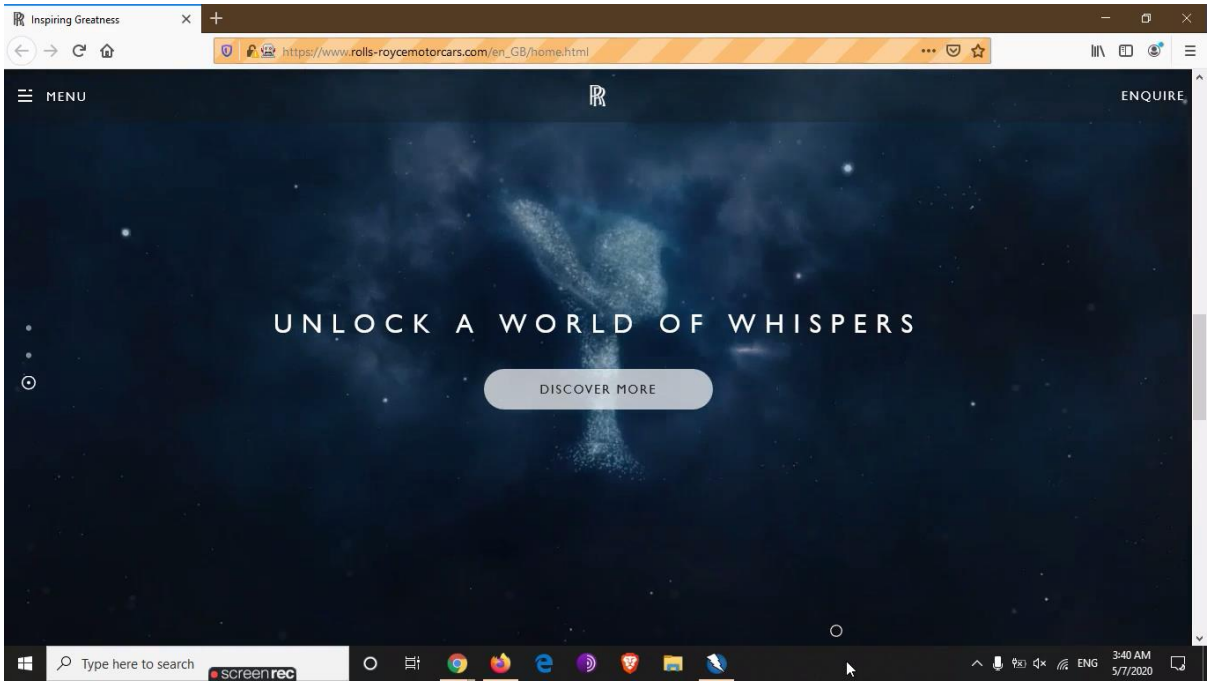


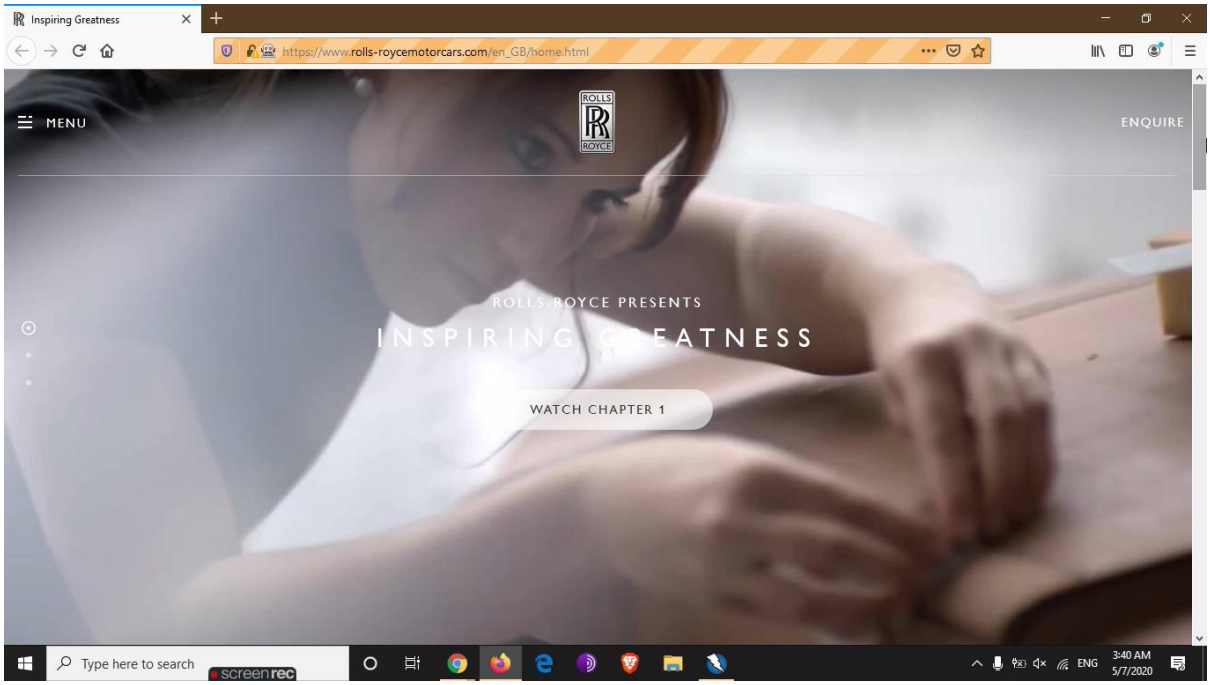
Description and the solution is also given.



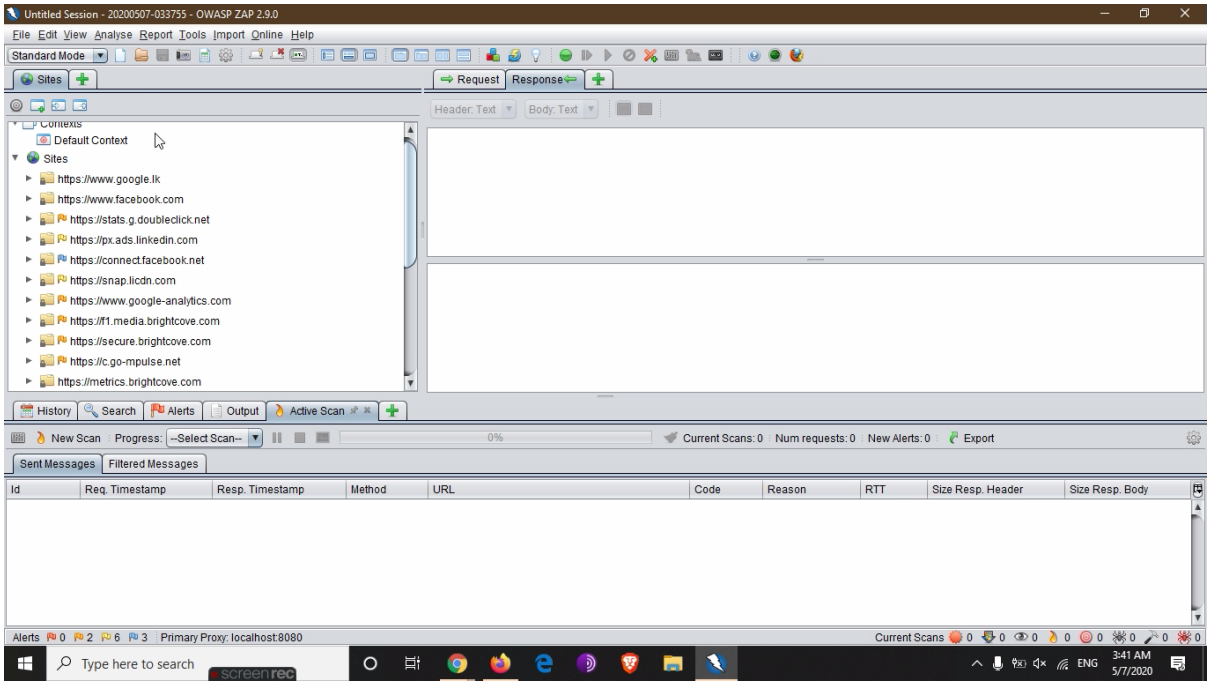
5.3. Rolls-Royce Website Scan - ZAP

Browse the URL “www.rolls-roycemotorcars.com” using the supporting web browser.

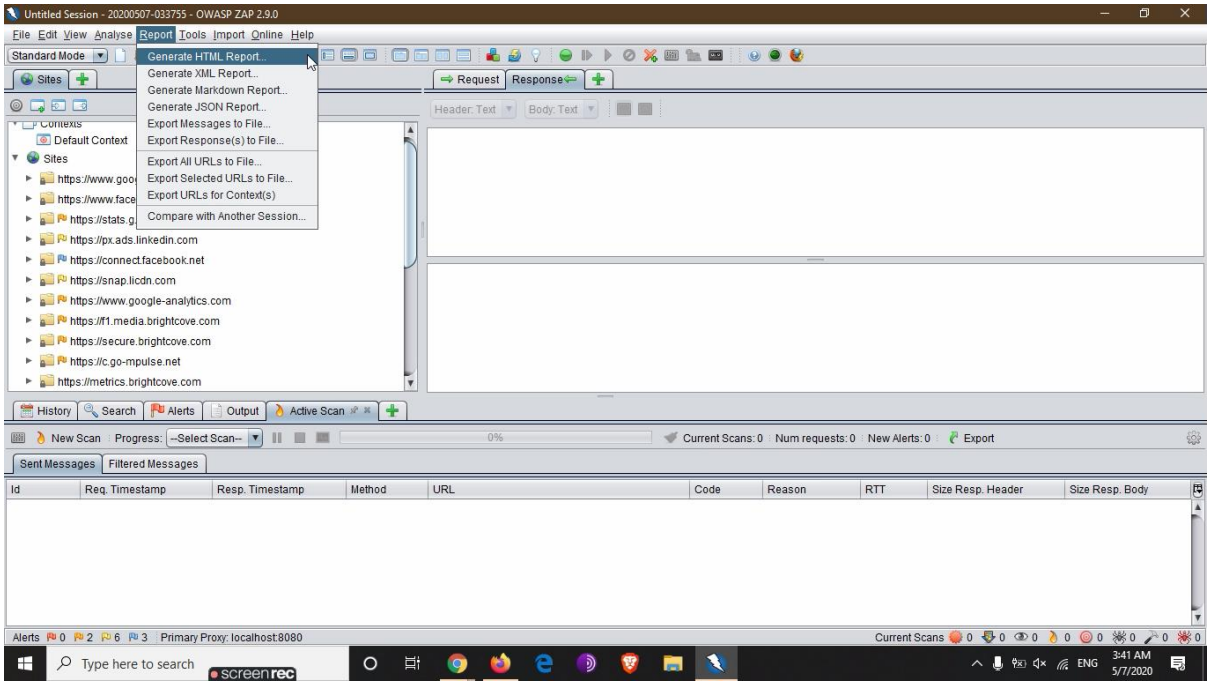




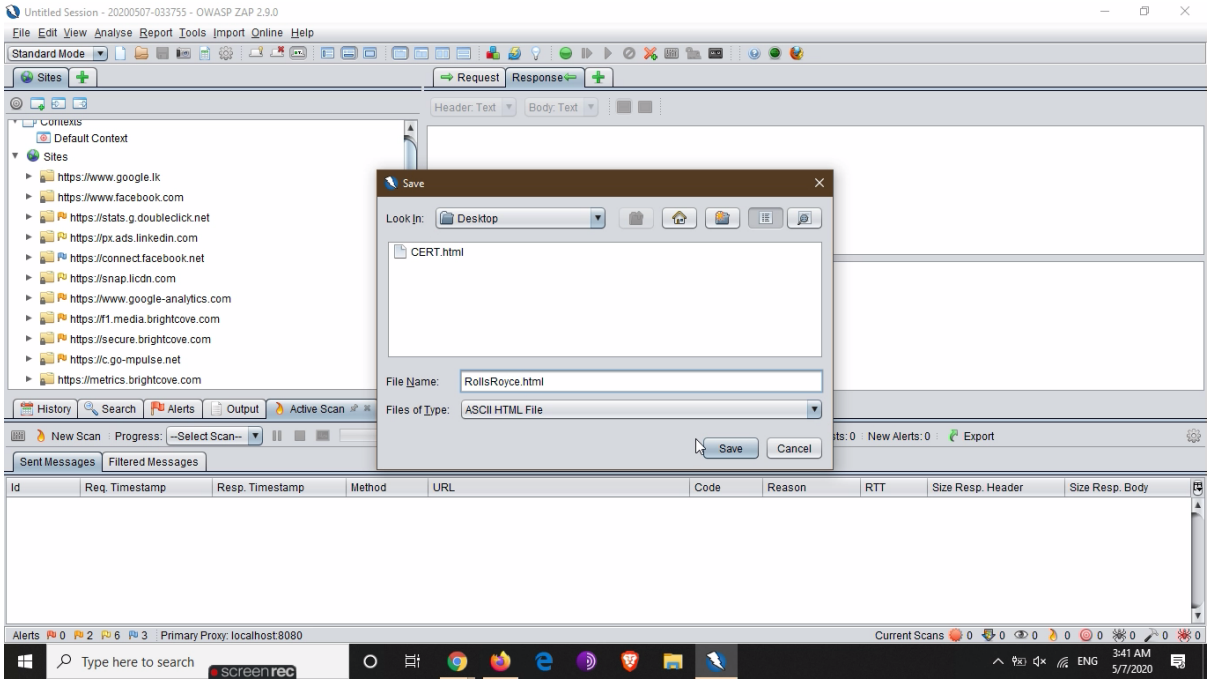
The scan is automatically started. Number of alerts can be seen.



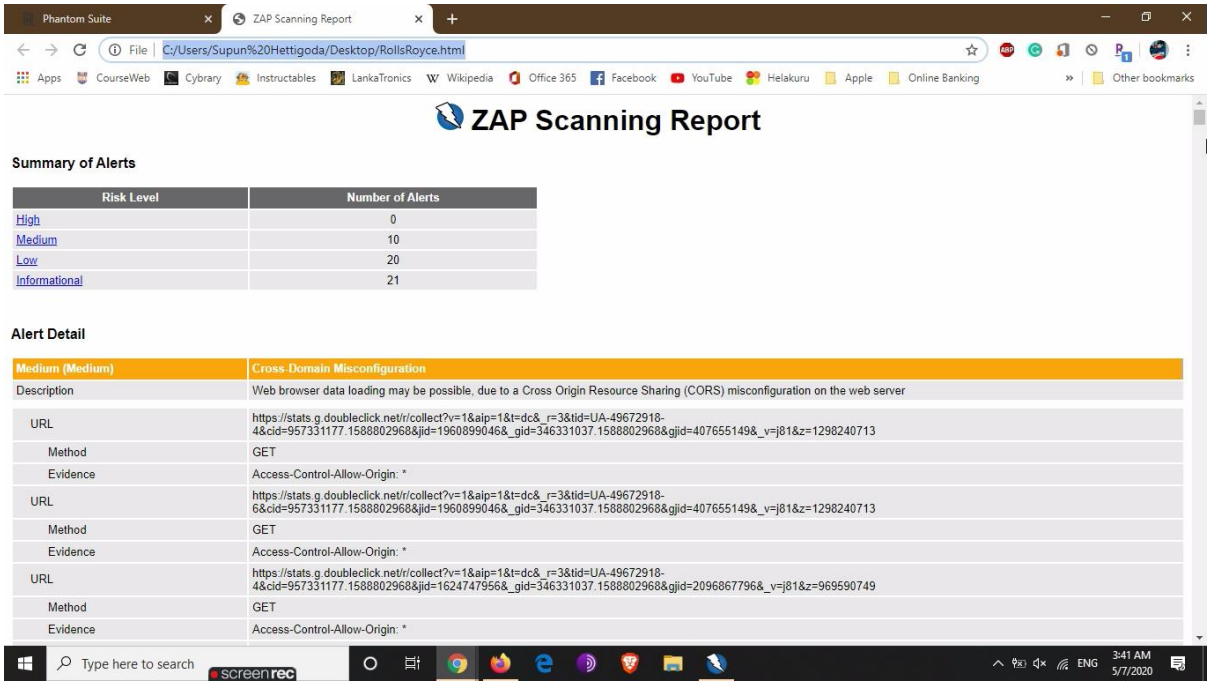
The Report is generated.



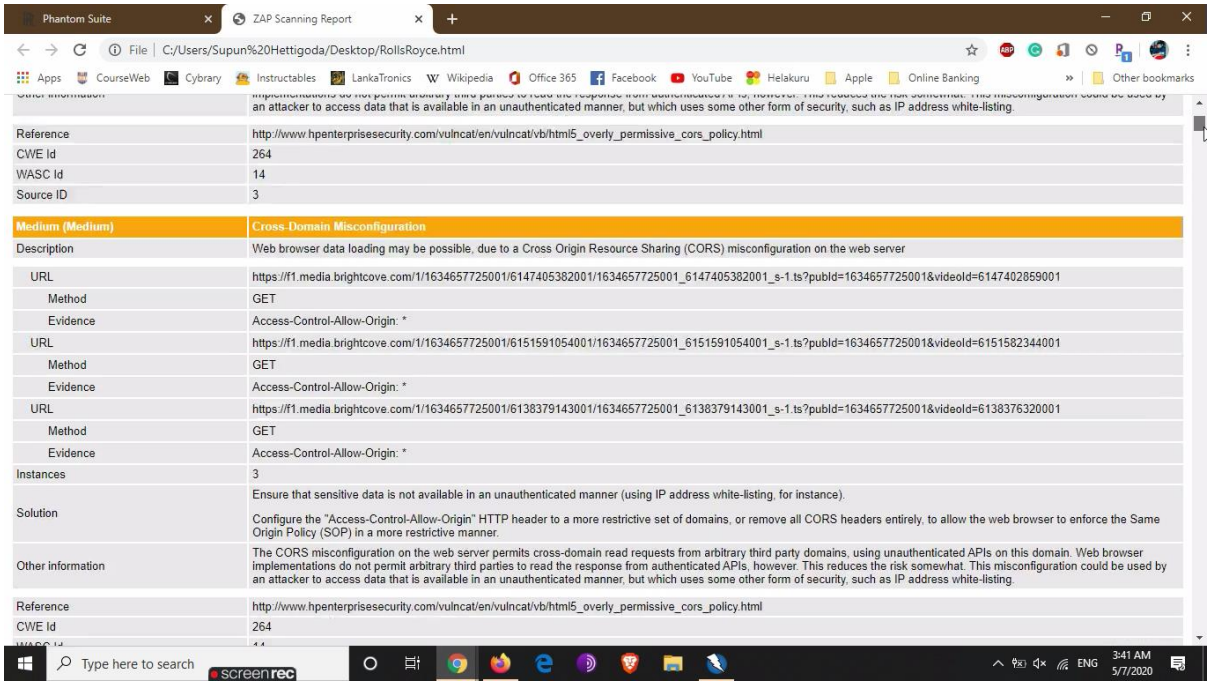
A new file name has to be given.



The .html formatted report is opened with the default web browser. There are 10 Medium level security alerts, 20 Low level security alerts and 21 Informational level security alerts.



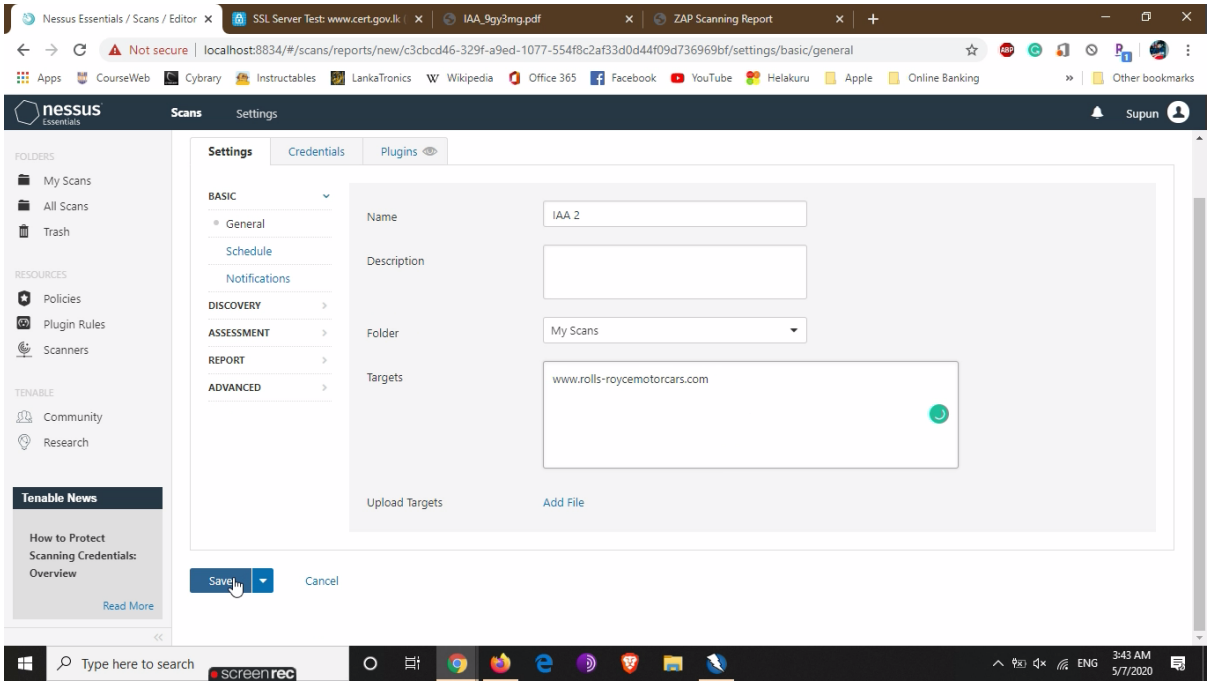
Descriptions and the Solutions are given regarding the vulnerabilities.



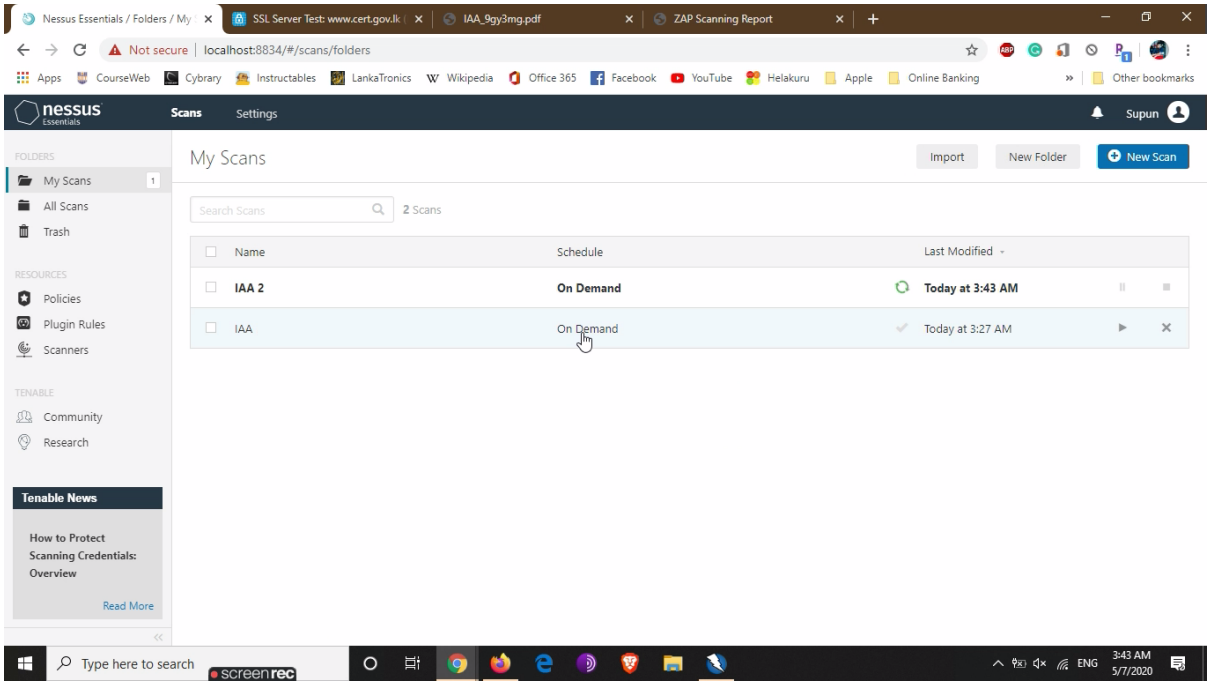
	an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html
CWE Id	264
WASC Id	14
Source ID	3
Medium (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://f1.media.brightcove.com/1/1634657725001/6147405382001/1634657725001_6147405382001_s-1.ts?pubId=1634657725001&videoId=6147402859001
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://f1.media.brightcove.com/1/1634657725001/6151591054001/1634657725001_6151591054001_s-1.ts?pubId=1634657725001&videoId=6151582344001
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://f1.media.brightcove.com/1/1634657725001/6138379143001/1634657725001_6138379143001_s-1.ts?pubId=1634657725001&videoId=6138376320001
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	3
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

5.4. Rolls-Royce Website Scan - Nessus

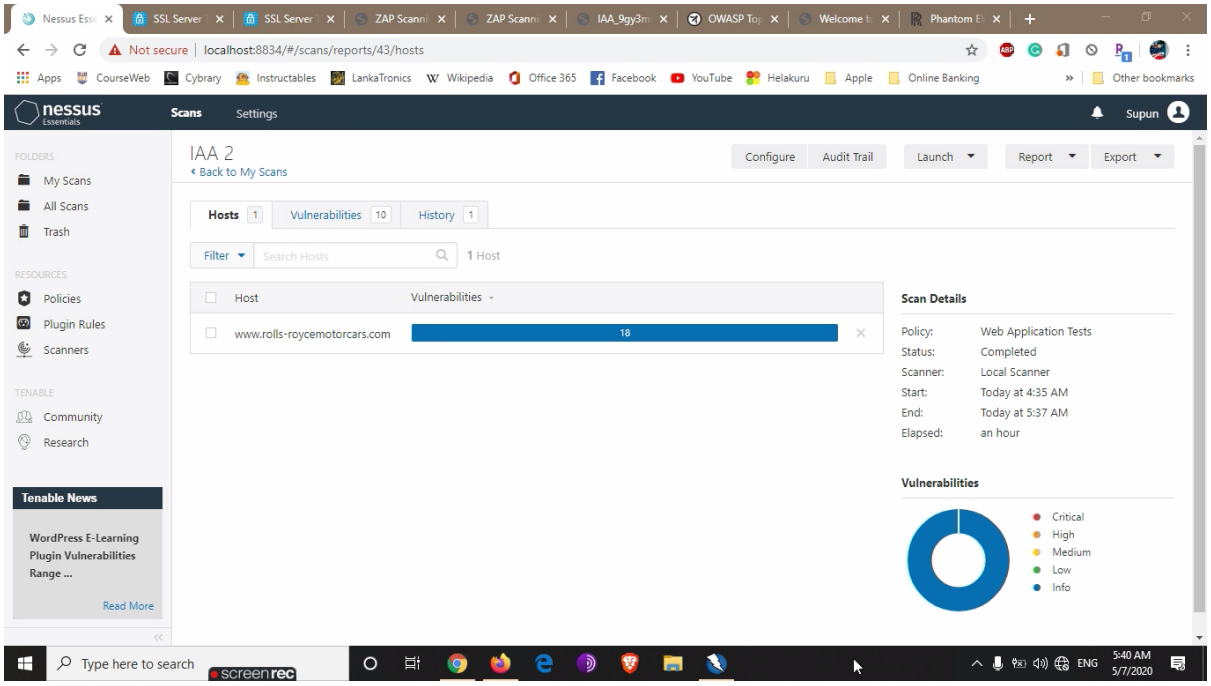
A new scan is configured for the second scanning which is done for the Rolls-Royce website.



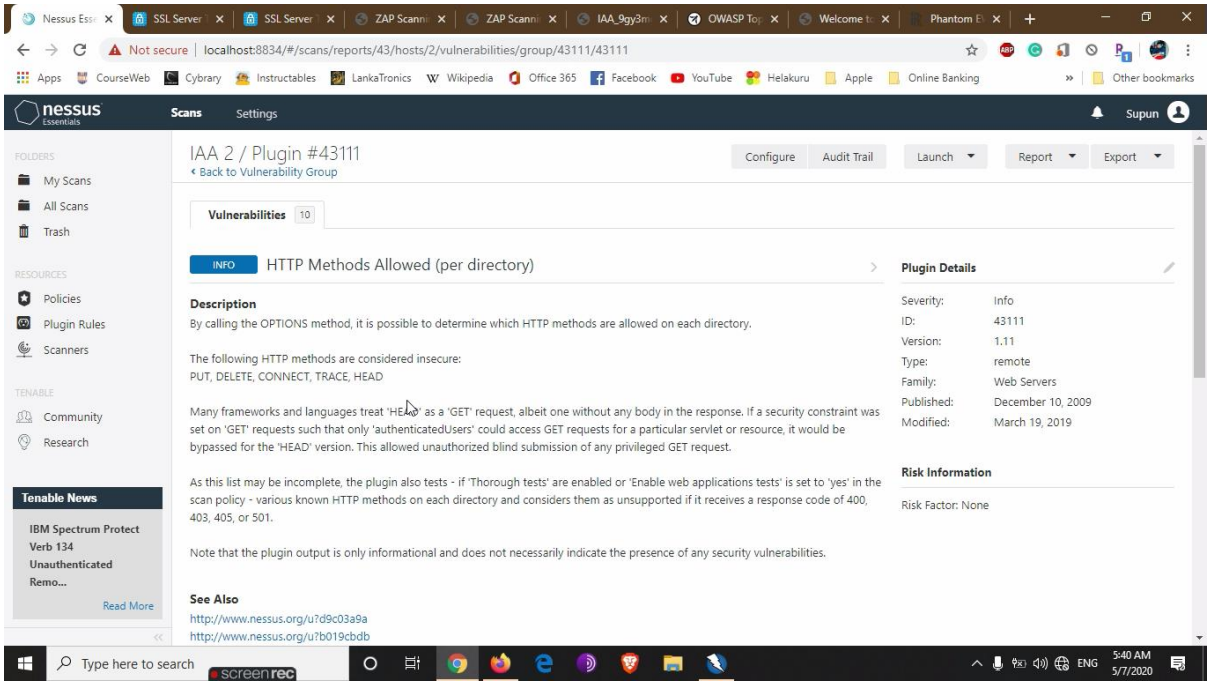
The scan is launched.



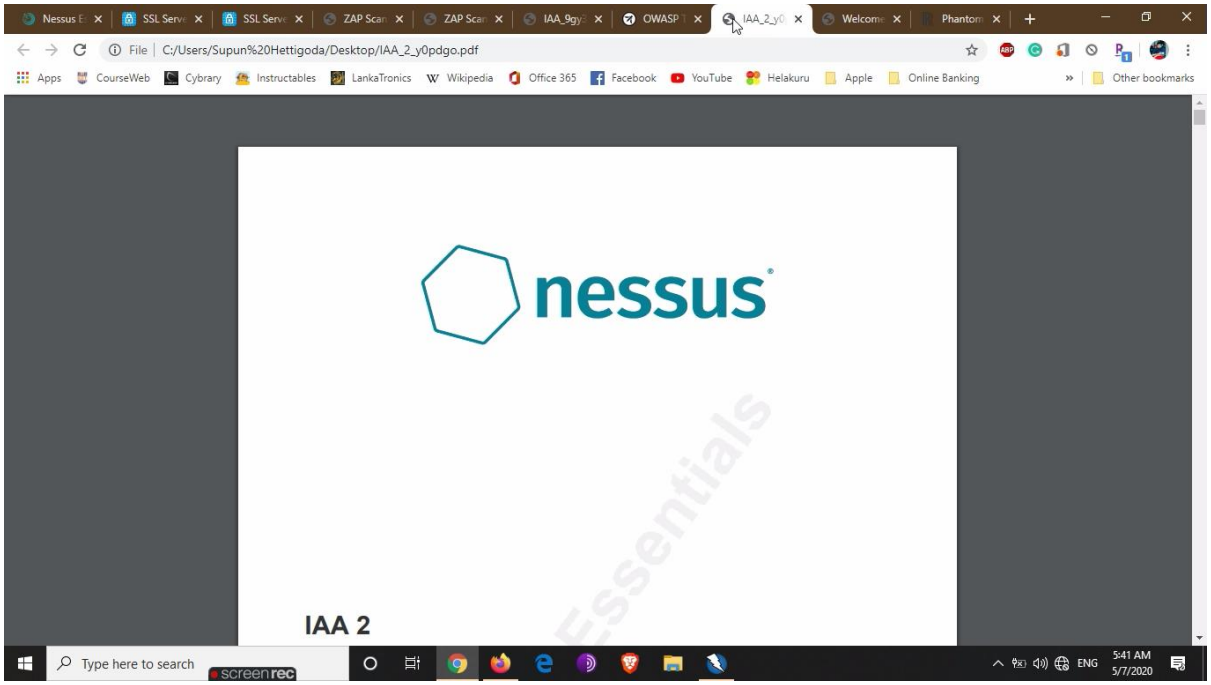
The scan completed. This time it took more than an hour. Only found informational level vulnerabilities.

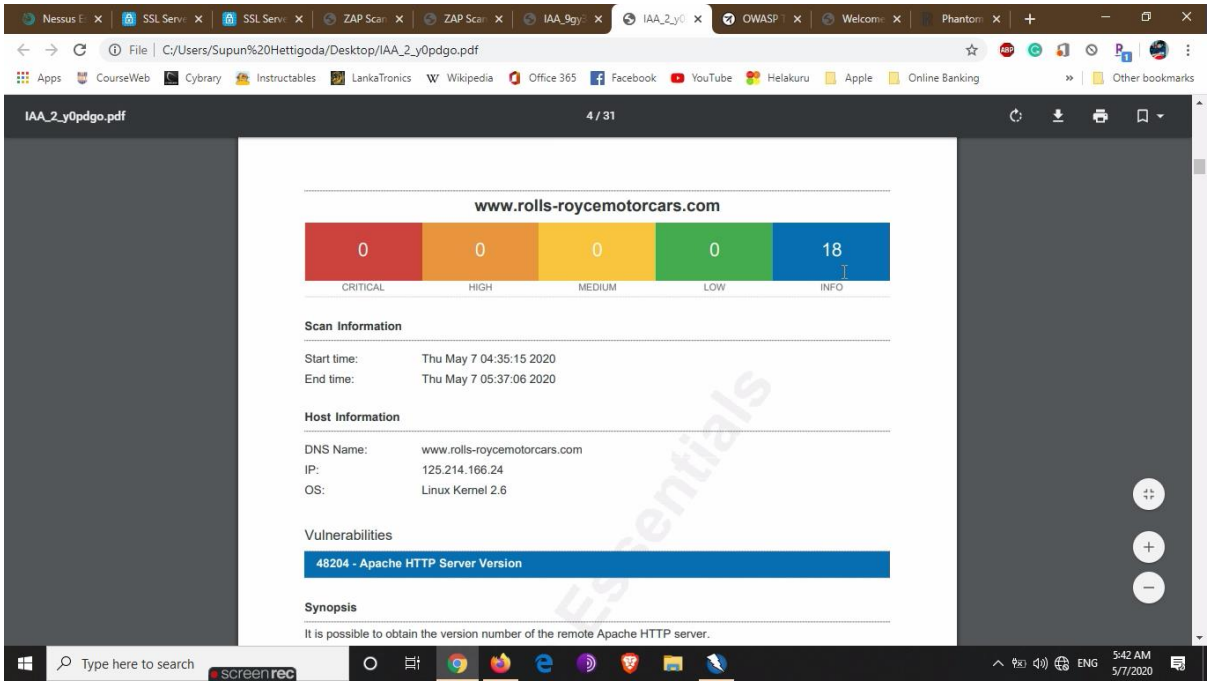


Here is an issue regarding HTTP



The report is generated same as the previous scan using Nessus.



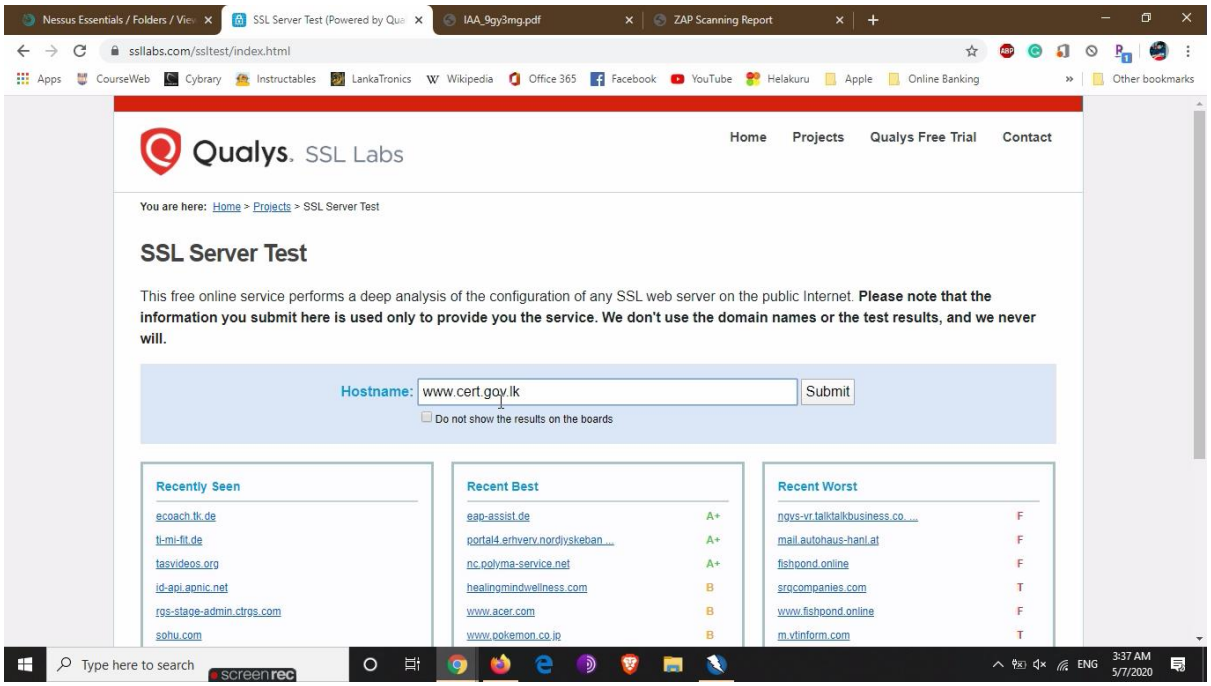


6. Audit - SSL and Certificate Testing

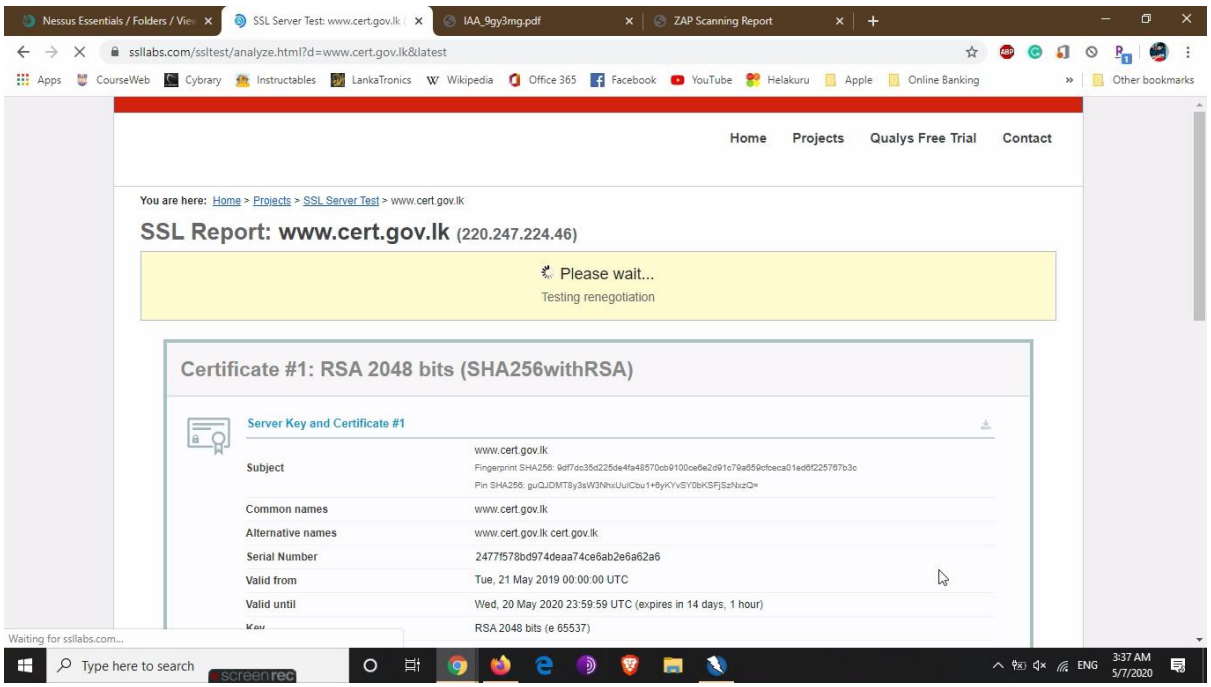
This audit performs a deep analyze of the web servers. It shows the protocol support, configuration errors and certificate validities. It shows a grade for the website which is tested according to the performance and update level of supported protocols.

6.1. Test - SLCERT Website

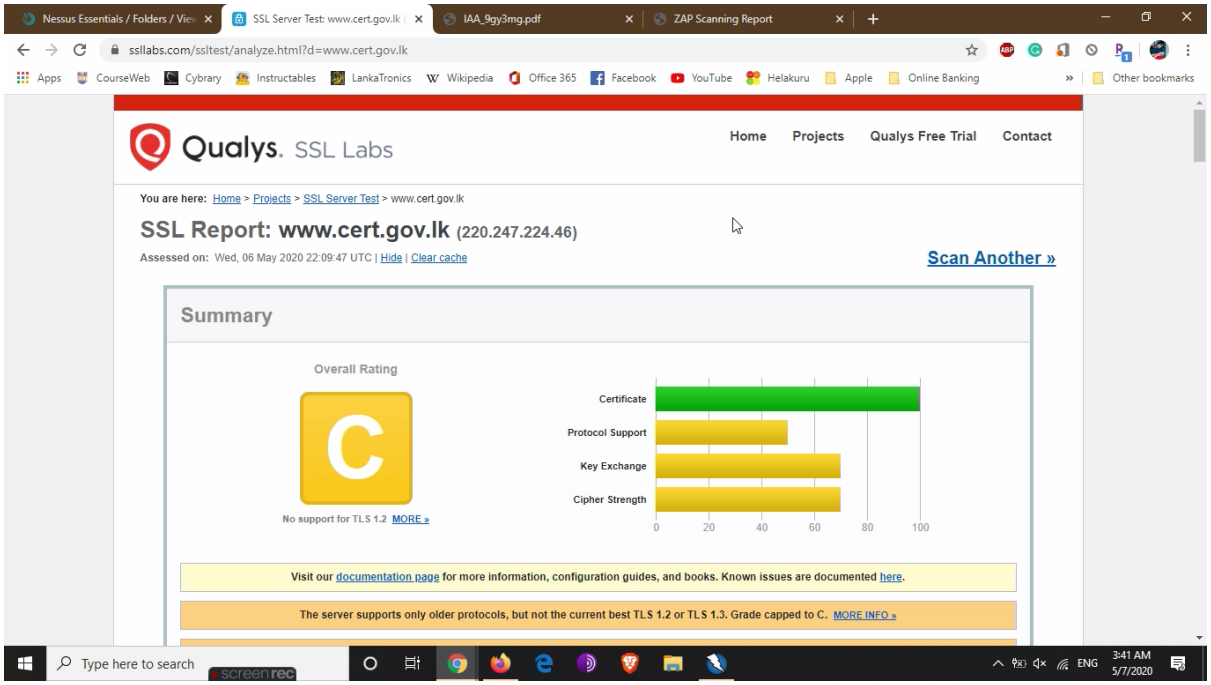
Type the URL of SLCERT which is needed to be tested.



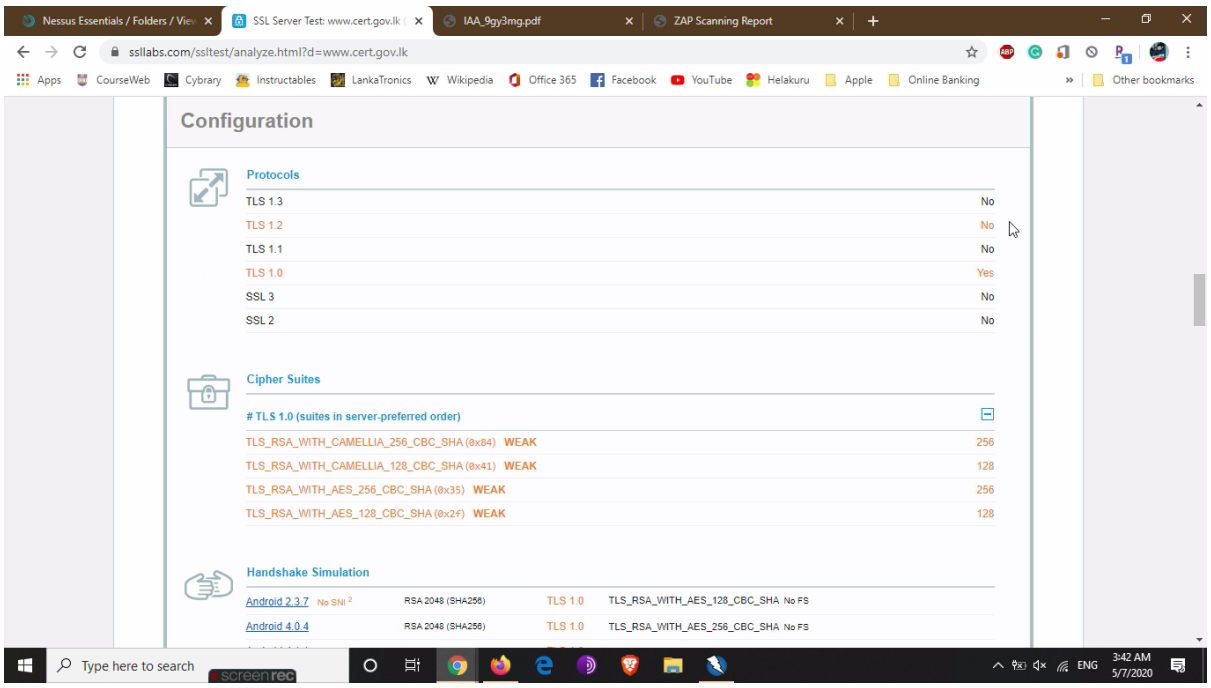
Then the web tool is performing the testing.



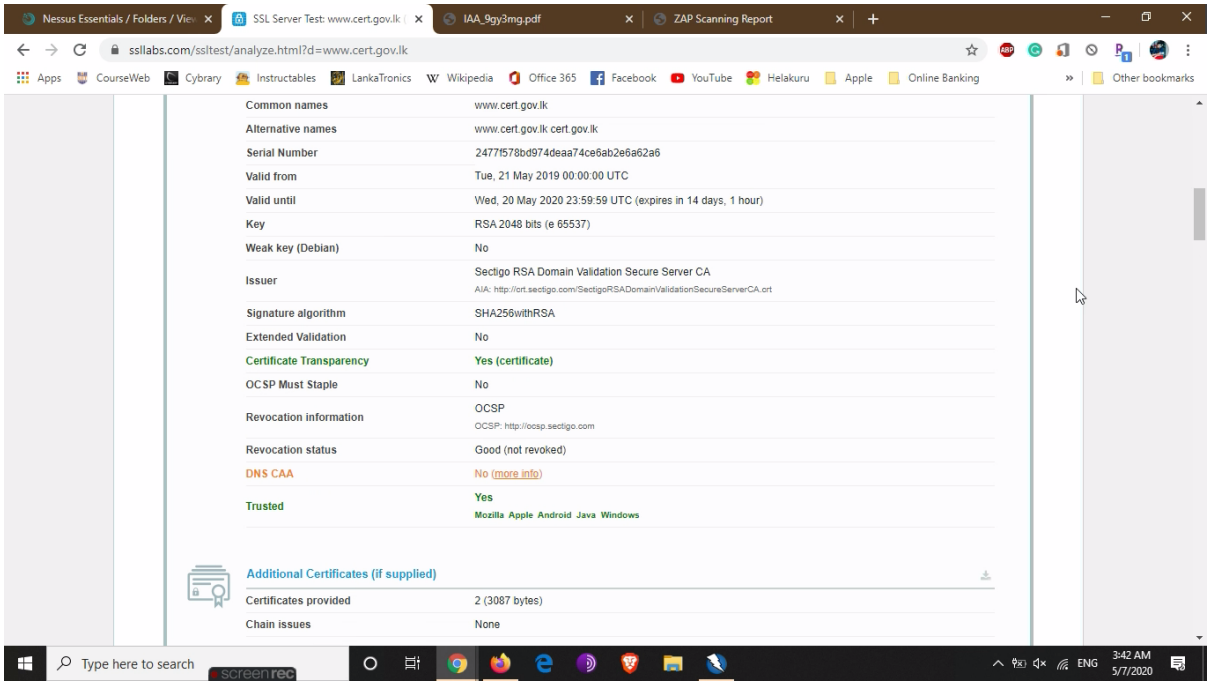
The SLCERT website is having a grade as “C”.



Transport Layer Security (TLS) configuration is not supporting TLS 1.2 or 1.3. It only supports for TLS 1.0 which is a much older and outdated version. This is also a reason for having a grade C.

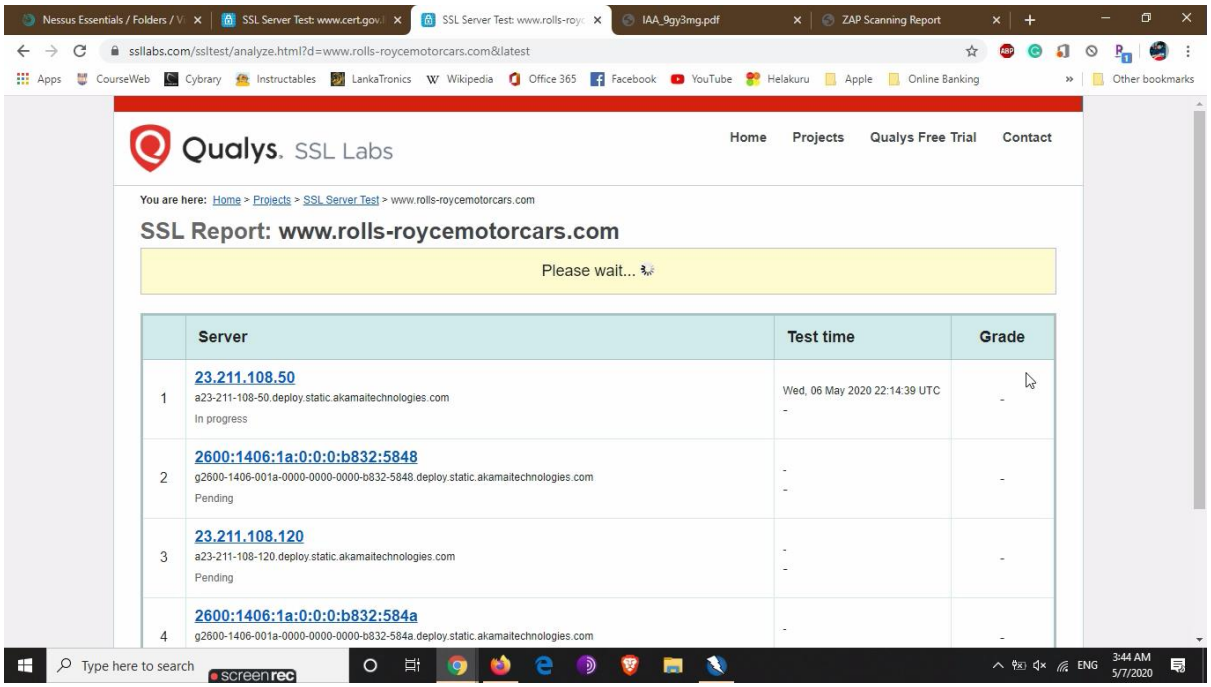


But, there is no problem with Certificate. It is valid. But, expires within 14 days.

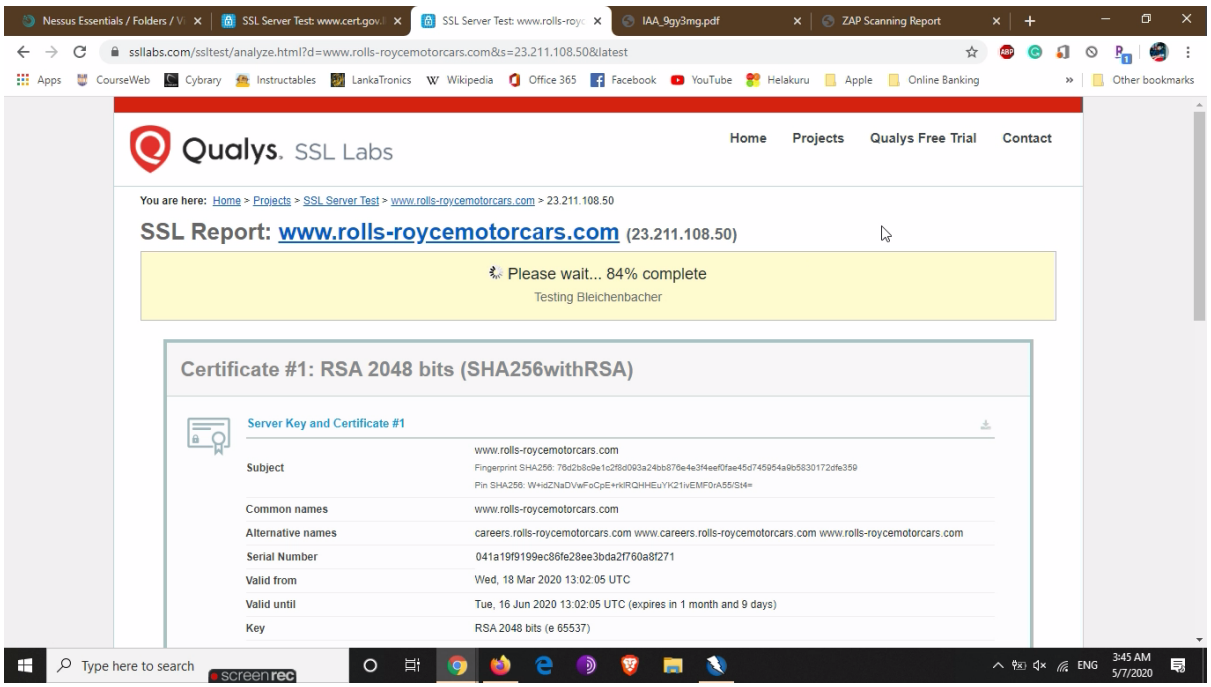


6.2. Test - Rolls-Royce Website

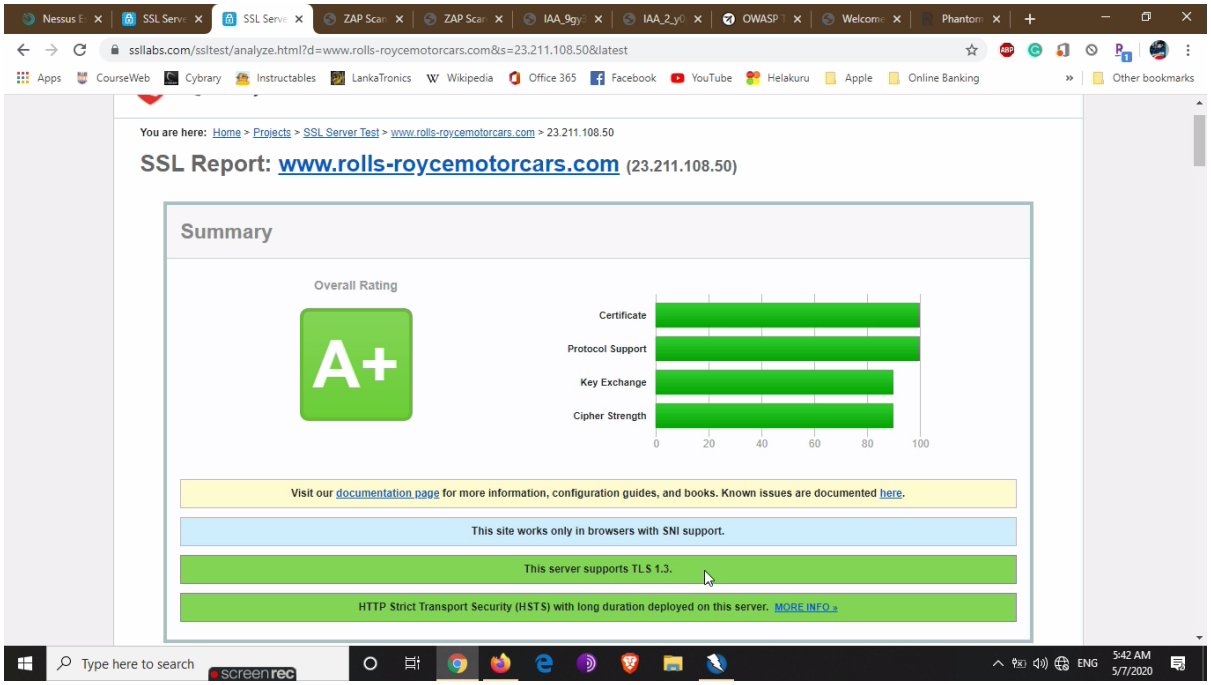
Same as previous test, type the URL of Rolls-Royce website. Then the web tool finds a relevant IP addresses. Click on the IP address.



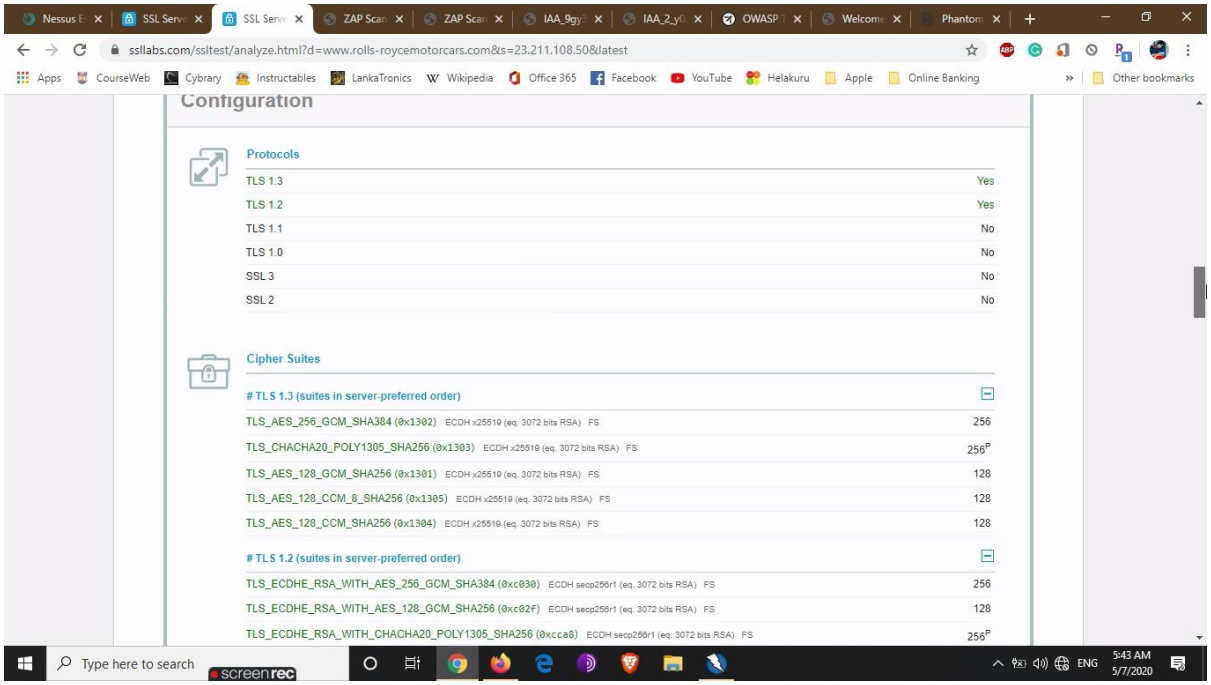
The web tool performs the scanning.



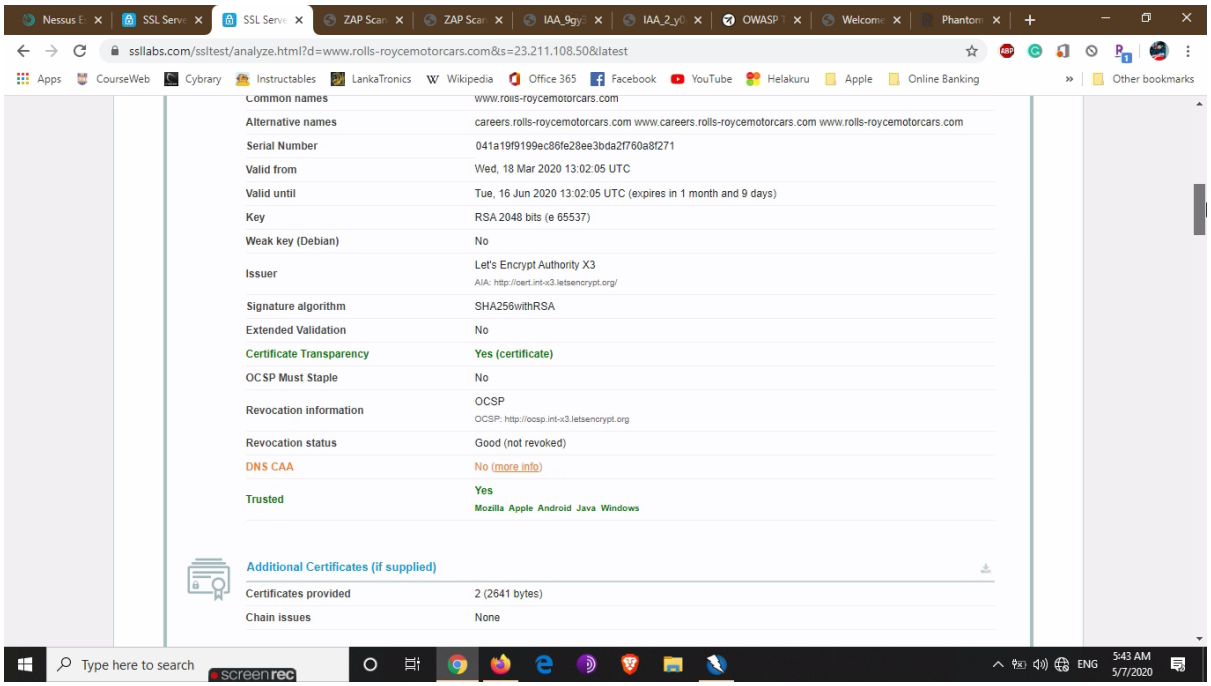
The Rolls-Royce website is having a grade as “A+”.



Transport Layer Security (TLS) configuration is supporting TLS 1.2 and 1.3. Which are the latest versions of TLS. This is also a reason for having a grade A+.



There is no problem with Certificate. It is valid. But, expires within 1 month and 9 days.



7. Comparison

All of the auditing is done for both websites within the limitations. There were big differences between those websites. We can have a comparison between them by considering some aspects. While comparing these both websites we can have some idea about both the scanning tools we used, their performance wise. Check the table 7.1.

	SLCERT	**Rolls-Royce**
Logo		
Headquarters	BMICH, Colombo 07, Sri Lanka.	Goodwood, England.
Alerts with ZAP	60	51
Alerts with Nessus	38	18
Critical Vulnerabilities (Red Alerts)	Yes	No
TLS Support	1.0	1.2 and 1.3
Grading	C	A+
Certificate Validity	Yes (14 Days)	Yes (39 Days)
Developed By	SLCERT, Sri Lanka.	Akmai Technologies, USA.

8. Problem Identification

Basically, most of the problems are in the **SLCERT** website as follows. Seemingly it is in a weaker level.

- It is using an unsupported PHP version. It is the reason for critical vulnerability.

62% of websites in the Internet is using unsupported versions of PHP.[10] An attacker could potentially exploit this flaw to conduct "**Man-In-The-Middle**" attacks to spoof SSL servers in this case.

- Cross-origin resource sharing (CORS) misconfiguration.

CORS is a mechanism for browsers which provides a controlled access to resources which are in outside of the domain. It provides more flexibility for same-origin policy (SOP). Anyway, it also paves the way for cross-domain attacks, if a web application's CORS policy is misconfigured. It will be a door for cross-origin attacks such as "**Cross-Site Request Forgery**" (CSRF).[11]

- X-Frame-Options (XFO) header is not included in the HTTP response.

This one will be a huge opportunity for hackers who are willing to deliver "**ClickJacking**" attacks. It takes place when an attacker uses various transparent layers to trick a user into clicking on a button or link on a framed page when they were intending to click on another page. So, the hacker is "hijacking" clicks meant for their page and routing them another page.[12]

- Allow wildcard sources (or ancestors), are not defined, or are overly broadly defined.

This type of misconfigurations may case for an "**Injection**" attack. Since those definitions are not provided clearly for the database and access levels.

- Supporting only for older version of TLS, TLS 1.0.

All the old SSL and TLS versions are having multiple vulnerabilities such as **BEAST, POODLE, DROWN** and etc. According to the "Global Sign" most of the web browsers stops supporting for all the SSL and TLS 1.0 from the first half of 2020.[13]

- Disclose sensitive information like the location of the file in exceptions.

Simply, this will be a guide to figure out the file hierarchy of the website. Since, it gives the file location of some files.

Rolls-Royce website is also having problems which have already been explained.

- Cross-origin resource sharing (CORS) misconfiguration.
- X-Frame-Options (XFO) headers were found.

9. Conclusion and Recommendation

After considering the Problem Identification section and Scan Reports. There are some major updates and configurations to be done.

- PHP version should be updated in SLCERT.
- TLS support should be updated to TLS 1.2 or 1.3 in SLCERT
- CORS should be re-configured in both websites.
- XFO header should be defined and well configured in both websites.
- Both websites should consider the Certificate renewal.

By following these recommendations, the SLCERT website will be more efficient and it will also gain a grade as A+.

10. References

[1]"The Scope Of A Cyber Security Audit", *Cybersecurityintelligence.com*, 2020. [Online]. Available: https://www.cybersecurityintelligence.com/blog/the-scope-of-a-cyber-security-audit-4734.html. [Accessed: 08- May- 2020].

[2]*Nserc-crsng.gc.ca*, 2020. [Online]. Available: https://www.nserc-crsng.gc.ca/_doc/Reports-Rapports/Audits-Verifications/ESSecurity01-SESecurite01_eng.pdf. [Accessed: 08- May- 2020].

[3]"OWASP Top Ten Web Application Security Risks | OWASP", *Owasp.org*, 2020. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed: 07- May- 2020].

[4]P. Garcia, "How to Perform a Website Security Audit (with Checklist)", *Sucuri Blog*, 2020. [Online]. Available: https://blog.sucuri.net/2019/07/how-to-perform-a-website-security-audit-with-checklist.html. [Accessed: 08- May- 2020].

[5]"OWASP ZAP Zed Attack Proxy | OWASP", *Owasp.org*, 2020. [Online]. Available: https://owasp.org/www-project-zap/. [Accessed: 05- May- 2020].

[6]"Nessus Product Family", *Tenable®*, 2020. [Online]. Available: https://www.tenable.com/products/nessus. [Accessed: 05- May- 2020].

[7]"SSL Server Test (Powered by Qualys SSL Labs)", *Ssllabs.com*, 2020. [Online]. Available: https://www.ssllabs.com/ssltest/index.html. [Accessed: 07- May- 2020].

[8]*Sri Lanka Computer Emergency Response Team*, 2020. [Online]. Available: http://www.cert.gov.lk/. [Accessed: 11- May- 2020].

[9]"Configure Your Rolls-Royce", *Rolls-roycemotorcars.com*, 2020. [Online]. Available: https://www.rolls-roycemotorcars.com/en_GB/bespoke/configure-your-rolls-royce.html. [Accessed: 06- May- 2020].

[10]C. Cimpanu, "Around 62 percent of all Internet sites will run an unsupported PHP version in 10 weeks | ZDNet", *ZDNet*, 2020. [Online]. Available: https://www.zdnet.com/article/around-62-of-all-internet-sites-will-run-an-unsupported-php-version-in-10-weeks/. [Accessed: 10- May- 2020].

[11]W. Academy, "What is CORS (cross-origin resource sharing)? Tutorial & Examples | Web Security Academy", *Portswigger.net*, 2020. [Online]. Available: https://portswigger.net/web-security/cors. [Accessed: 10- May- 2020].

[12]"Missing X-Frame-Options Header | Netsparker", *Netsparker.com*, 2020. [Online]. Available: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-x-frame-options-header/. [Accessed: 10- May- 2020].

[13]"It’s Time to Disable TLS 1.0 (and All SSL Versions) If You Haven’t Already", *Globalsign.com*, 2020. [Online]. Available: https://www.globalsign.com/en/blog/disable-tls-10-and-all-ssl-versions. [Accessed: 10- May- 2020].