



# SLIIT

*Discover Your Future*

## Information Assurance and Auditing

4<sup>th</sup> Year, 1<sup>st</sup> 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

<b>1. Introduction .....</b>	4
<b>2. Checklist.....</b>	5
<b>3. Tools.....</b>	6
<b>3.1. Zed Attack Proxy (ZAP) .....</b>	6
<b>3.2. Nessus .....</b>	9
<b>3.3. Qualys SSL Labs .....</b>	10
<b>4. Sample Websites .....</b>	11
<b>4.1. Sri Lanka Computer Emergency Response Team (SLCERT) .....</b>	11
<b>4.2. Rolls-Royce Motor Cars.....</b>	11
<b>5. Audit - Website Scanning .....</b>	12
<b>5.1. SLCERT Website Scan - ZAP .....</b>	12
<b>5.2. SLCERT Website Scan - Nessus.....</b>	18
<b>5.3. Rolls-Royce Website Scan - ZAP .....</b>	27
<b>5.4. Rolls-Royce Website Scan - Nessus.....</b>	31
<b>6. Audit - SSL and Certificate Testing .....</b>	34
<b>6.1. Test - SLCERT Website.....</b>	34
<b>6.2. Test - Rolls-Royce Website .....</b>	37
<b>7. Comparison.....</b>	40
<b>8. Problem Identification.....</b>	41
<b>9. Conclusion and Recommendation.....</b>	42
<b>10. References .....</b>	43

## 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]

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>• Injection</li><li>• Broken Authentication</li><li>• Sensitive Data Exposure</li><li>• XML External Entities (XXE)</li><li>• Broken Access Control</li><li>• Security Misconfiguration</li></ul> | <ul style="list-style-type: none"><li>• Cross-Site Scripting XSS</li><li>• Insecure Deserialization</li><li>• Using Components with Known Vulnerabilities</li><li>• Insufficient Logging and Monitoring</li></ul> |
|---|---|

## 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.

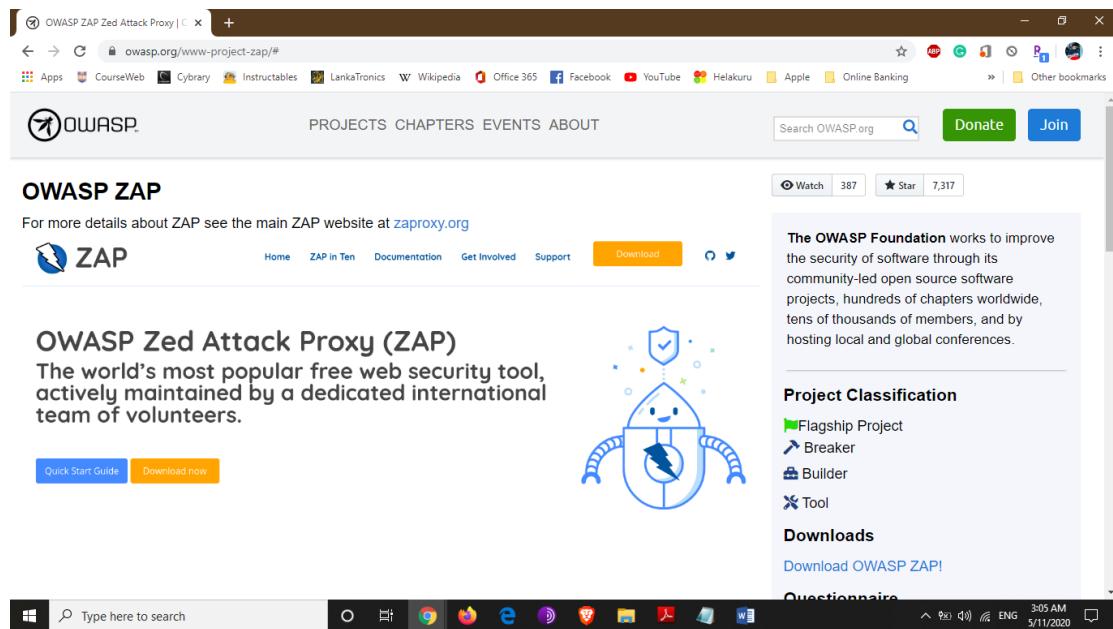
- Changing Content Management System (CMS) Settings to default
  - User Settings
  - Comment Settings
  - General Visibility of Information
- Selecting most suitable ones among the file permissions
  - Read (r), Write (w), Execute (x)
  - Owner, Group, Public
- Checking availability for software updates
  - 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

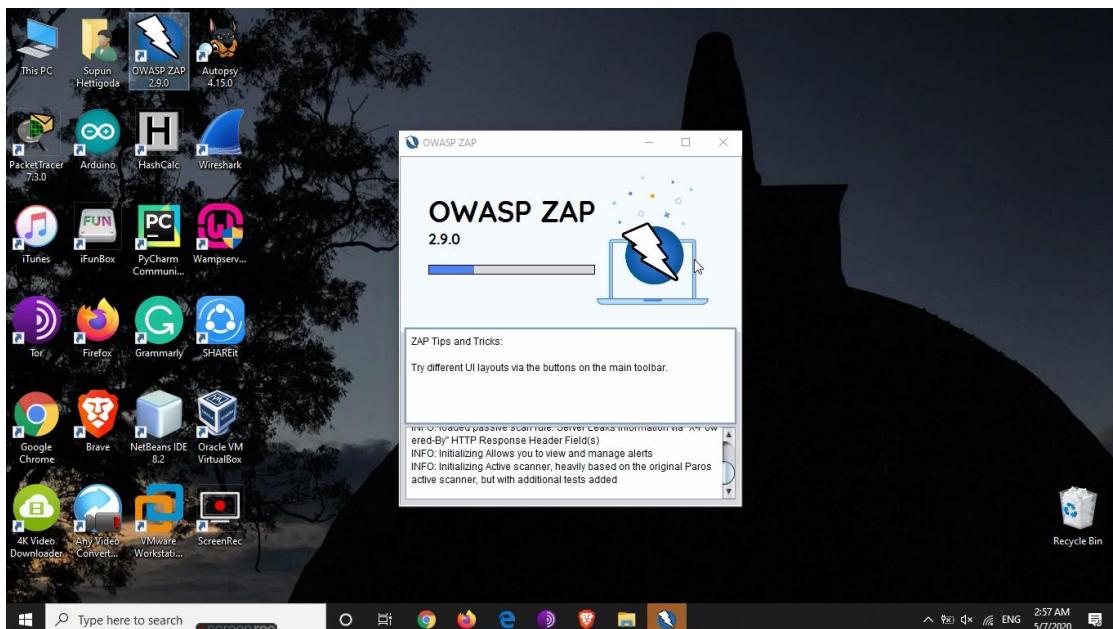
I'm going to use three tools for this audit. Two of them are open source and commercial web scanning tools. The other one is a SSL and Certificate testing tool.

#### 3.1.Zed Attack Proxy (ZAP)

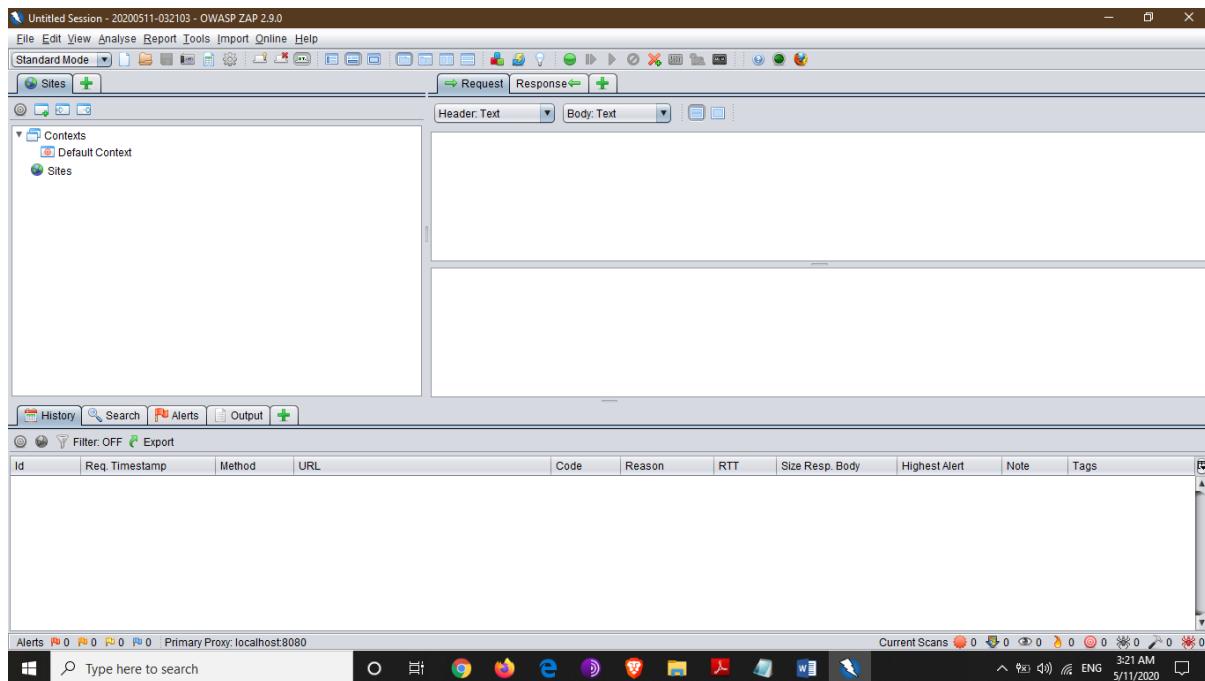
This is going to be the first tool that I'm using to perform this auditing. This is a free and open source tool which can be downloaded from the OWASP website.[5]



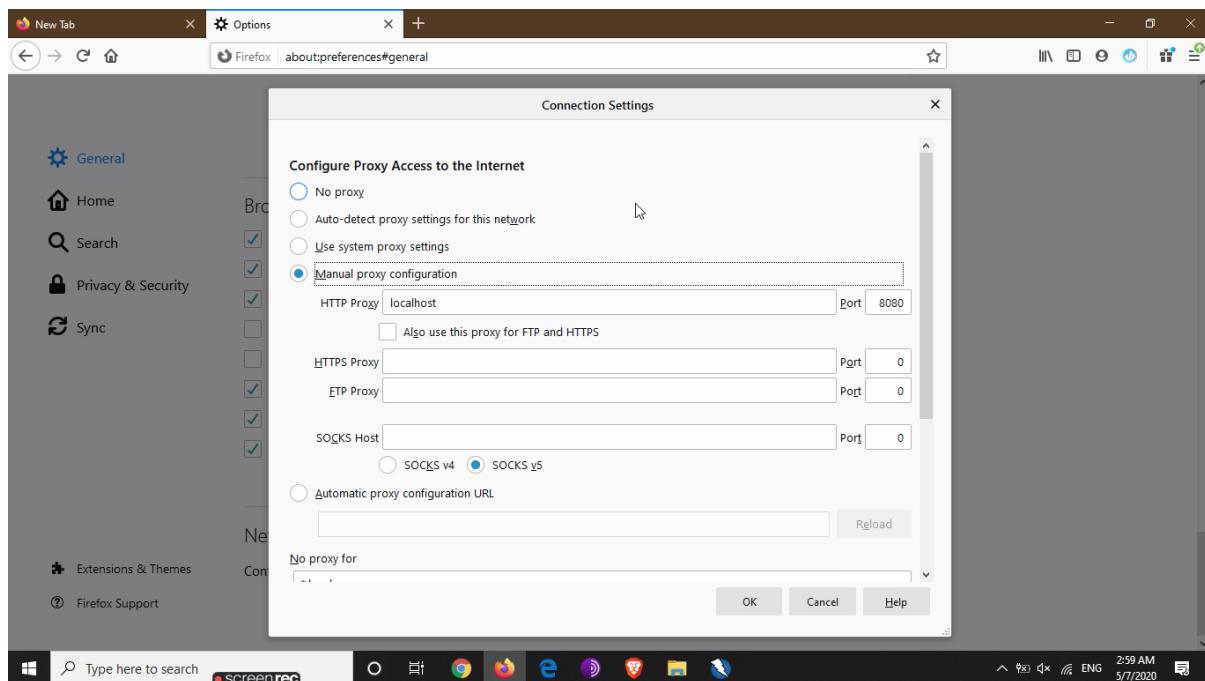
Simply install it using default settings same as the installation of a normal software. Then launch it. This is the up to date version available for now, OWASP ZAP 2.9.0



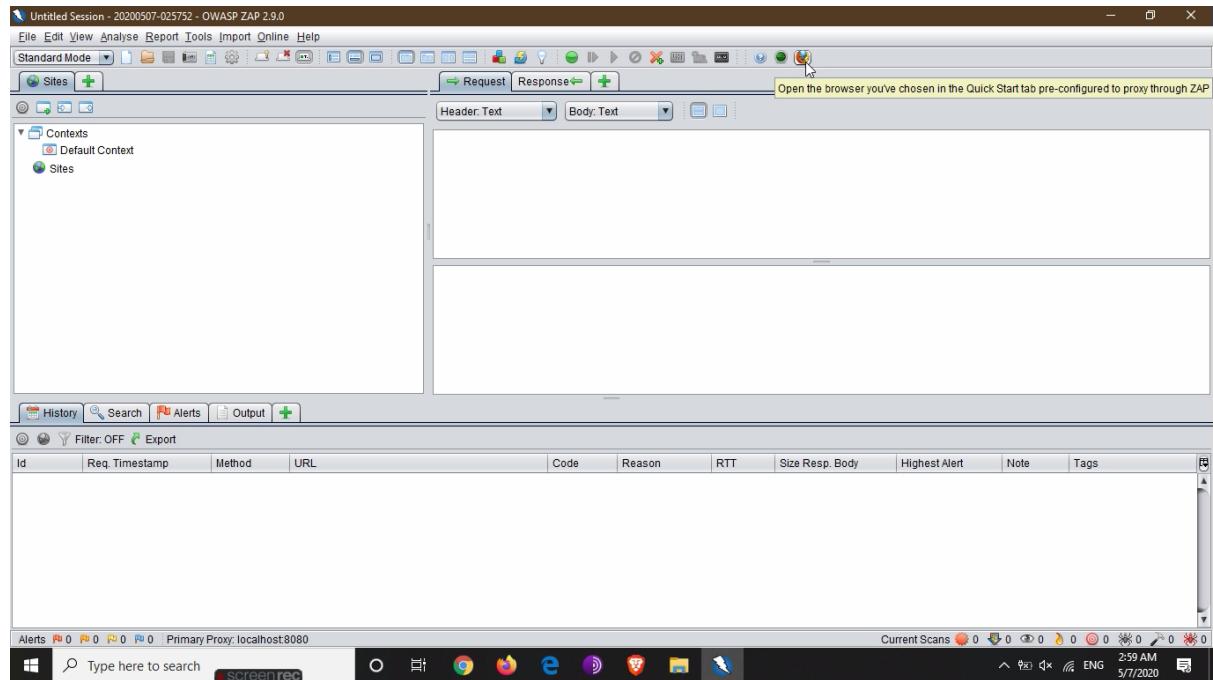
This is how the ZAP home screen looks like.



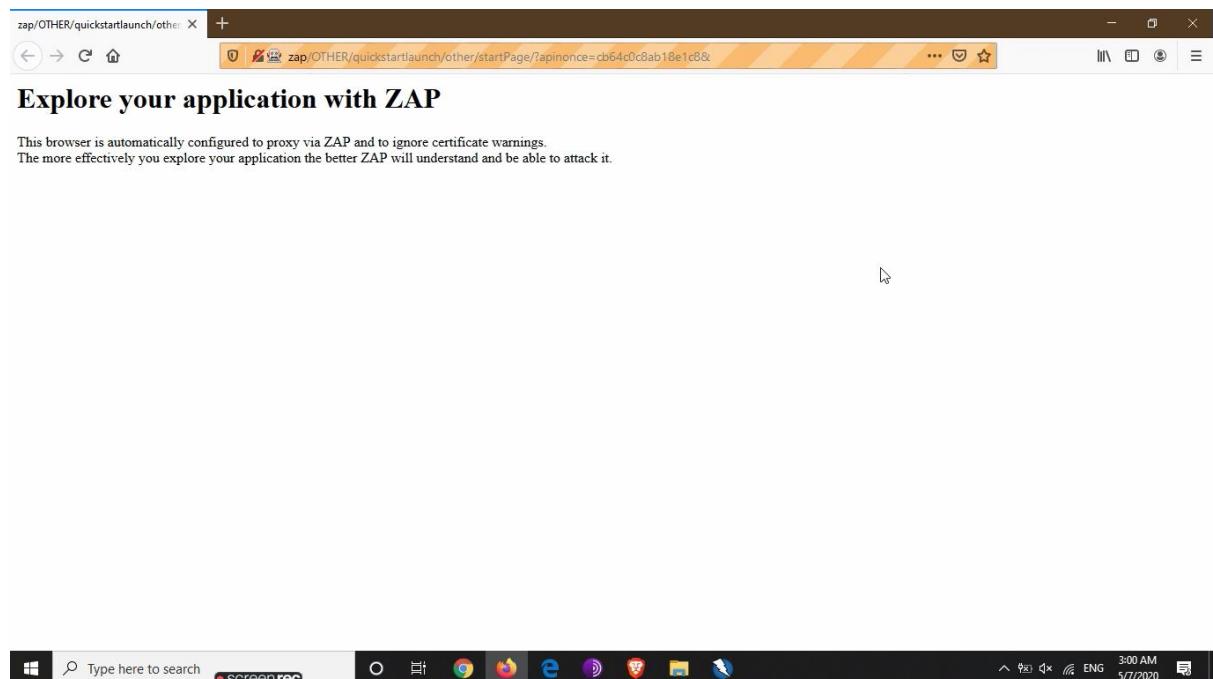
In order to do a scan, a supporting browser should be configured. In this case I use “Firefox”. A manual proxy is configured in the web browser as “localhost” and port number as “8080”



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

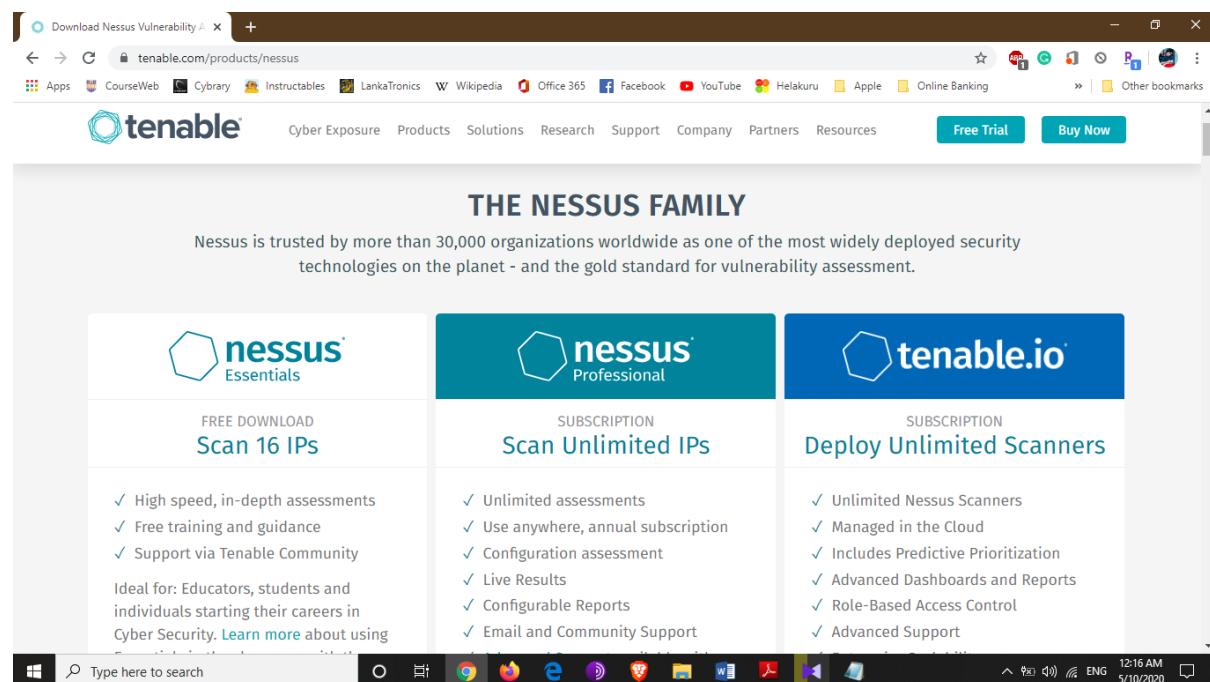


There is a visible difference in supporting browser tab, the address bar is having a different design than in a normal browser tab.

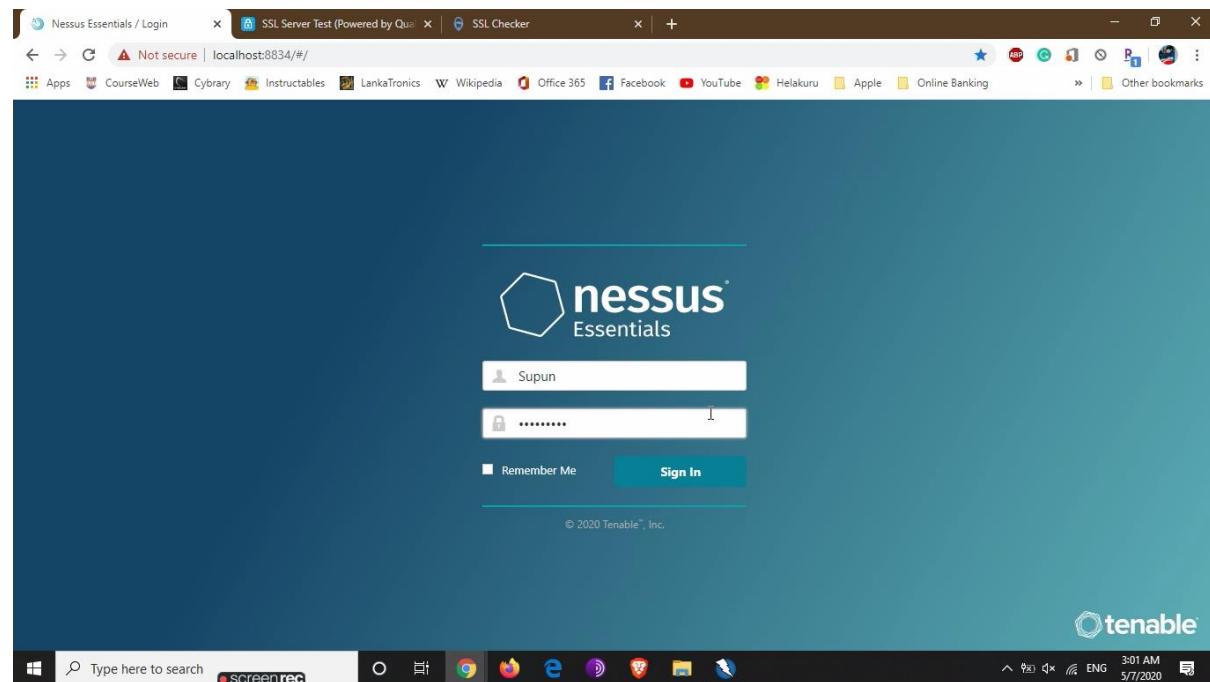


### 3.2. Nessus

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]

The screenshot shows a Microsoft Edge browser window with three tabs open: 'Nessus Essentials / Folders / Vie...', 'SSL Server Test (Powered by Qu...)', and 'IAA\_9gy3mg.pdf'. The main content area displays the Qualys SSL Labs logo and navigation links for Home, Projects, Qualys Free Trial, and Contact. Below this, it says 'You are here: Home > Projects > SSL Server Test' and features a heading 'SSL Server Test'. A note states: '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 field labeled 'Hostname:' contains a placeholder 'www.google.com'. To its right is a 'Submit' button and a checked checkbox for 'Do not show the results on the boards'. Below the form are three sections: 'Recently Seen' (listing sites like ecoach.tk.de, ti-mi-fit.de, tasvideos.org, id-api.apnic.net, rgs-stage-admin.ctros.com, and sohu.com), 'Recent Best' (listing sites like eap-assist.de, portal4.erhverv.nordjyskeban..., nc.polyma-service.net, healingmindwellness.com, www.acer.com, and www.pokemon.co.jp), and 'Recent Worst' (listing sites like noys-vr.talktalkbusiness.co..., mail.autohaus-hani.at, fishpond.online, srgcompanies.com, www.fishpond.online, and m.vlinform.com). The bottom of the screen shows the Windows taskbar with icons for File Explorer, Google Chrome, Mozilla Firefox, Microsoft Edge, Task View, and File History, along with a search bar containing 'screenrec'.

## 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.

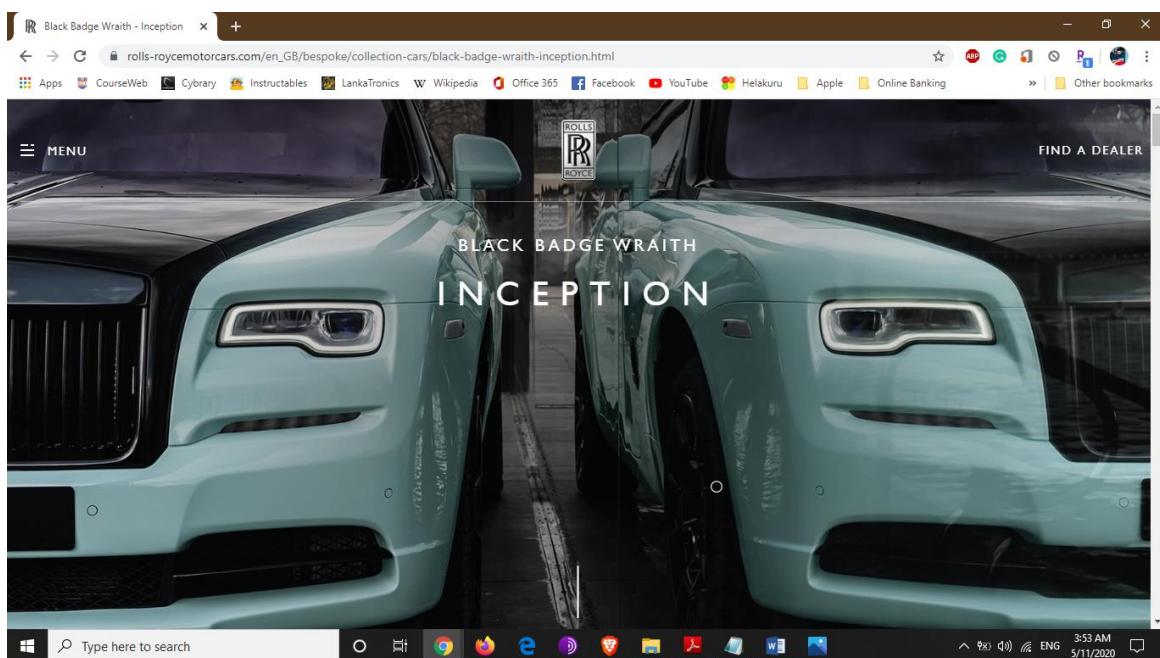
### 4.1. Sri Lanka Computer Emergency Response Team (SLCERT)

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]

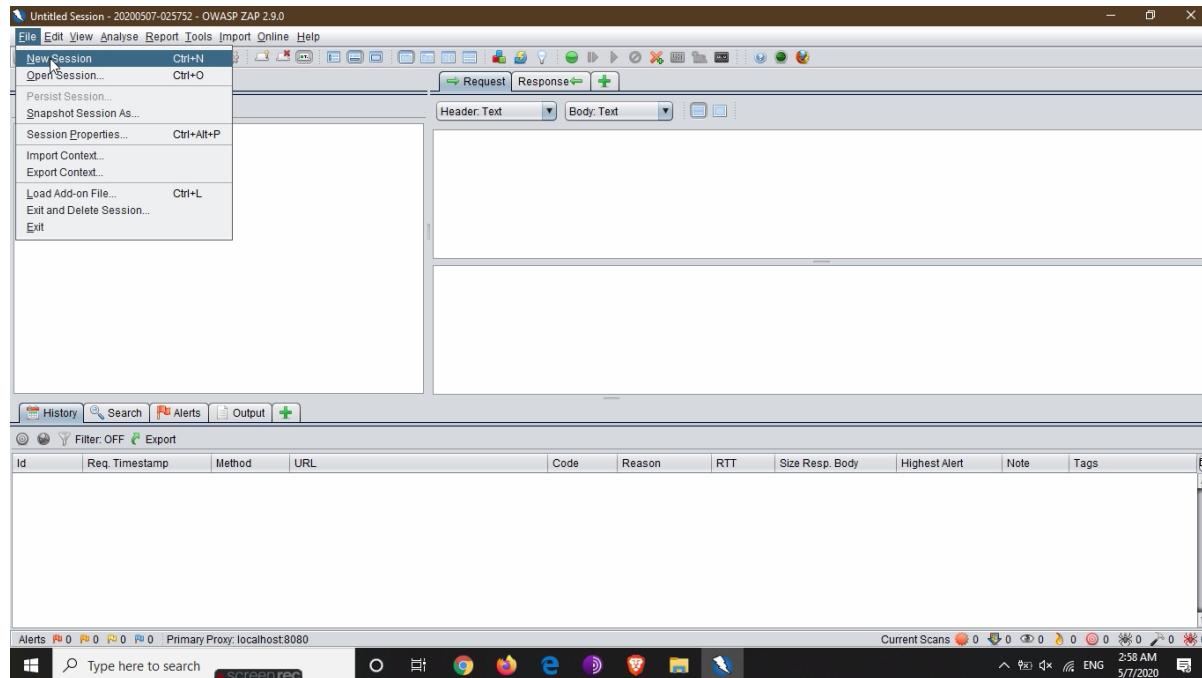


## **5. Audit - Website Scanning**

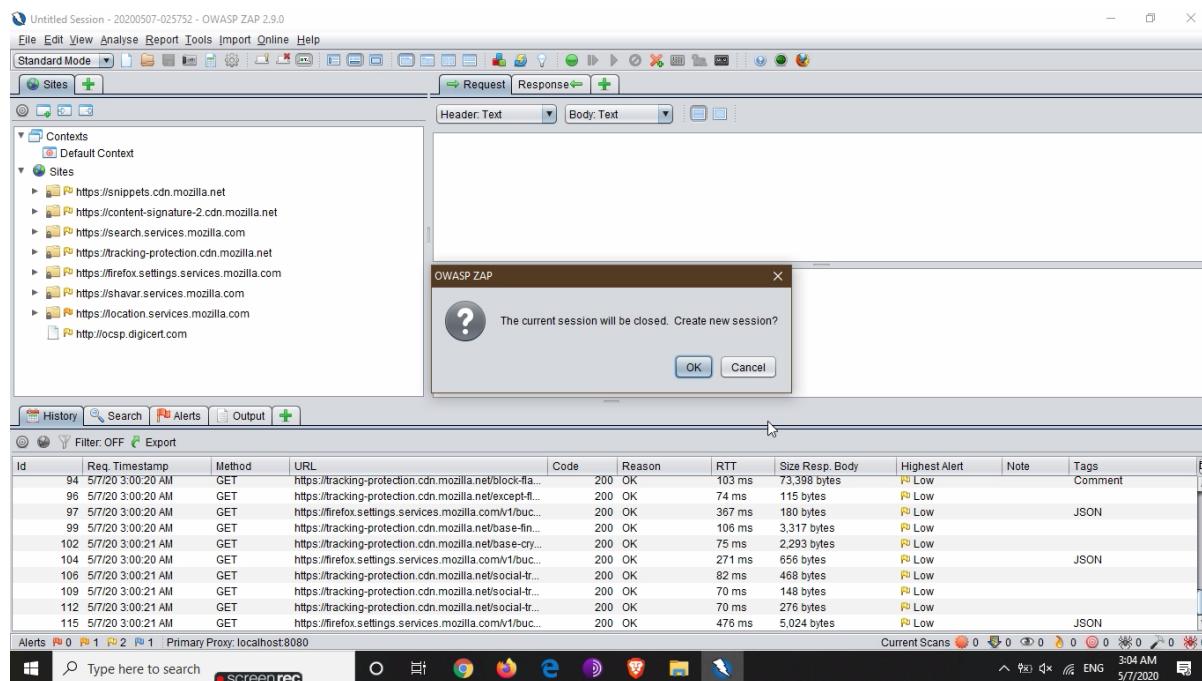
The aim is to find vulnerabilities and misconfigurations of these sample websites. On the other hand, we can have a comparison between websites.

## 5.1. SLCERT Website Scan - ZAP

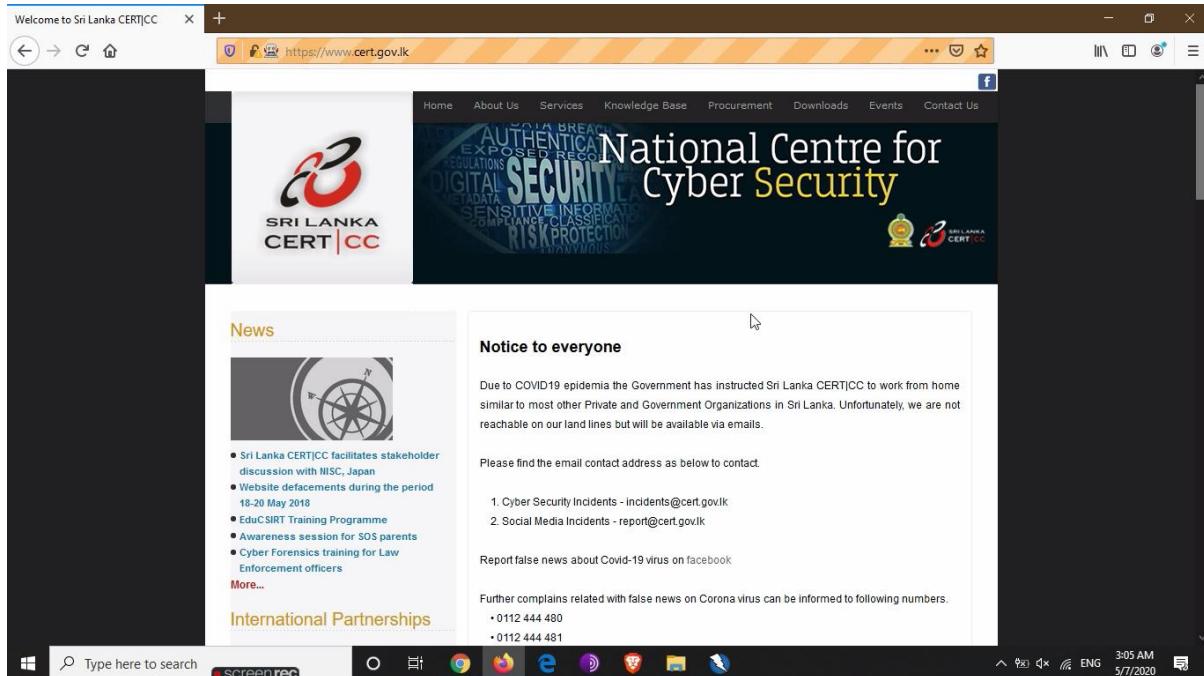
A new session should be started in order to scan the website.



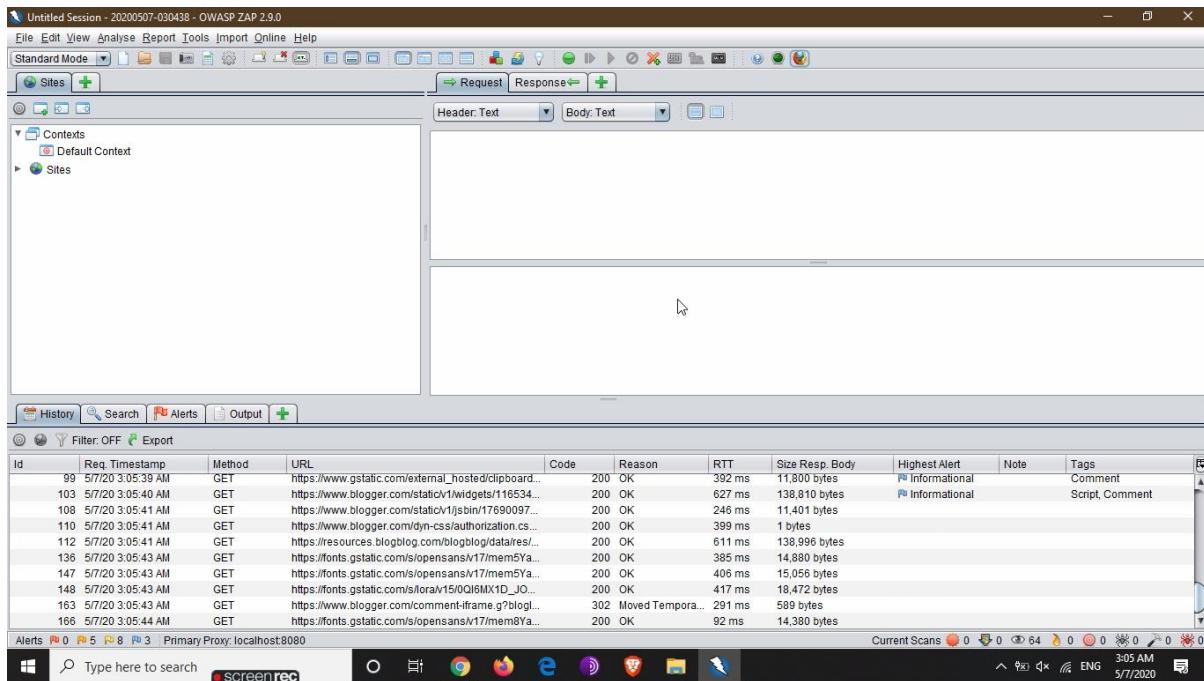
If there is a previous session, it will be closed before starting a new one.



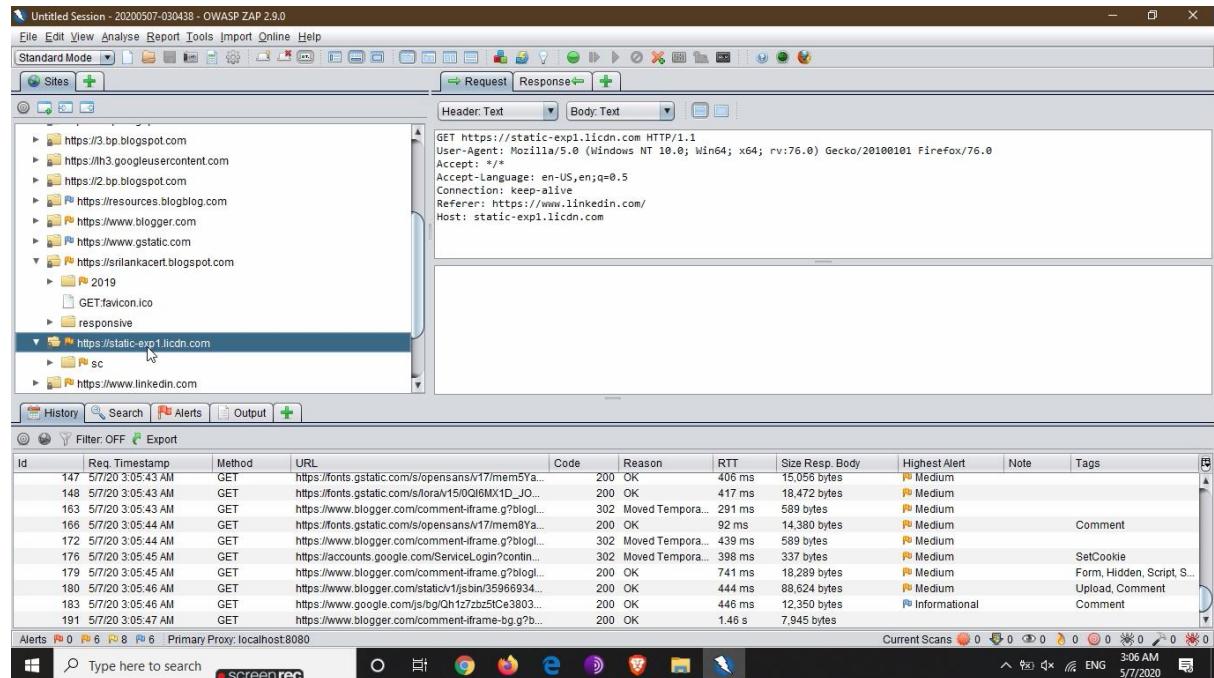
Go to the supporting web browser by clicking the web browser icon on the tool. Then give the URL, "www.cert.gov.lk"



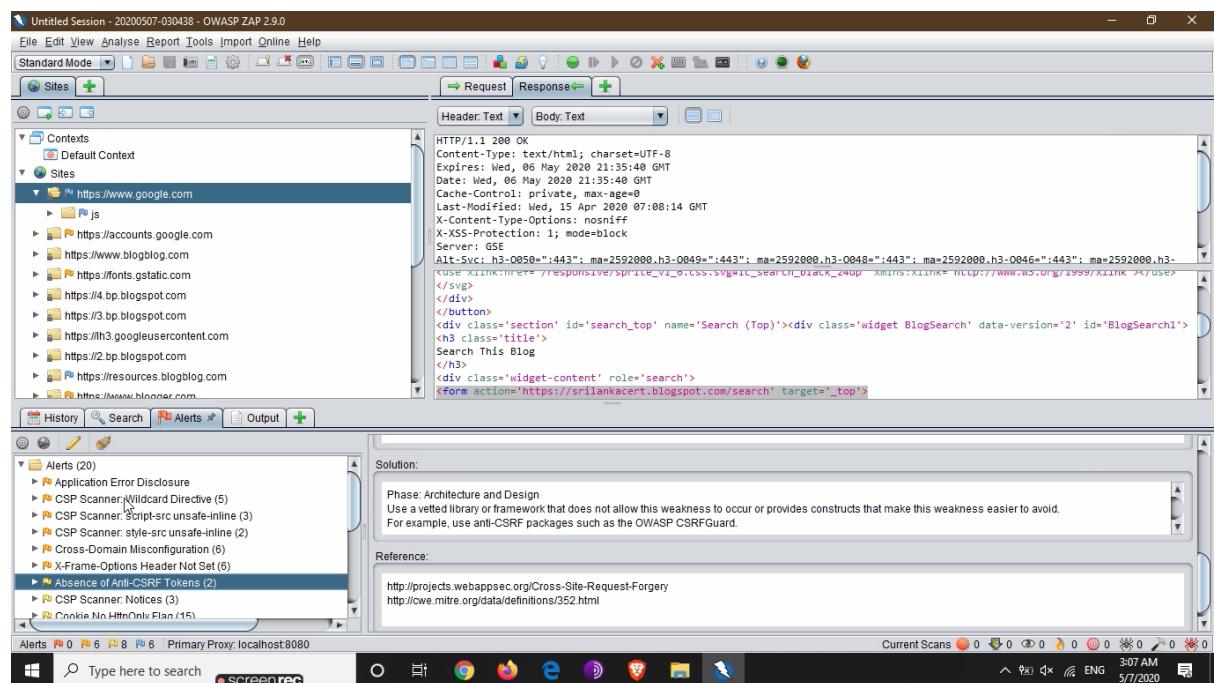
The scanning is started automatically in the application side.



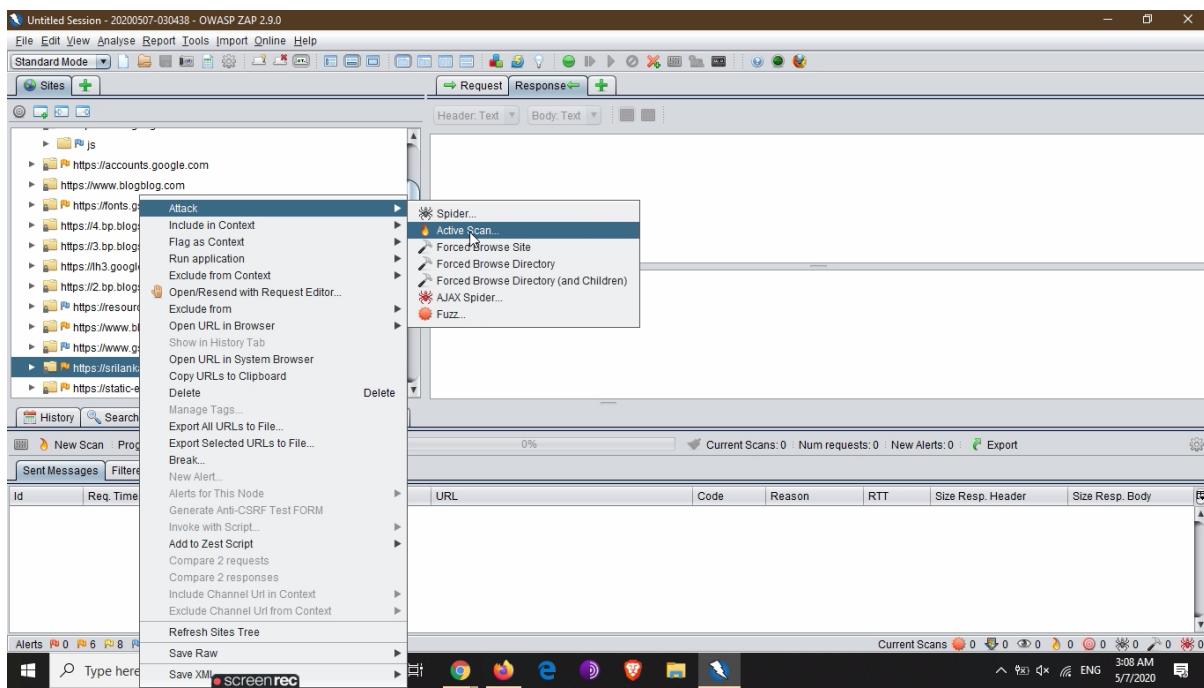
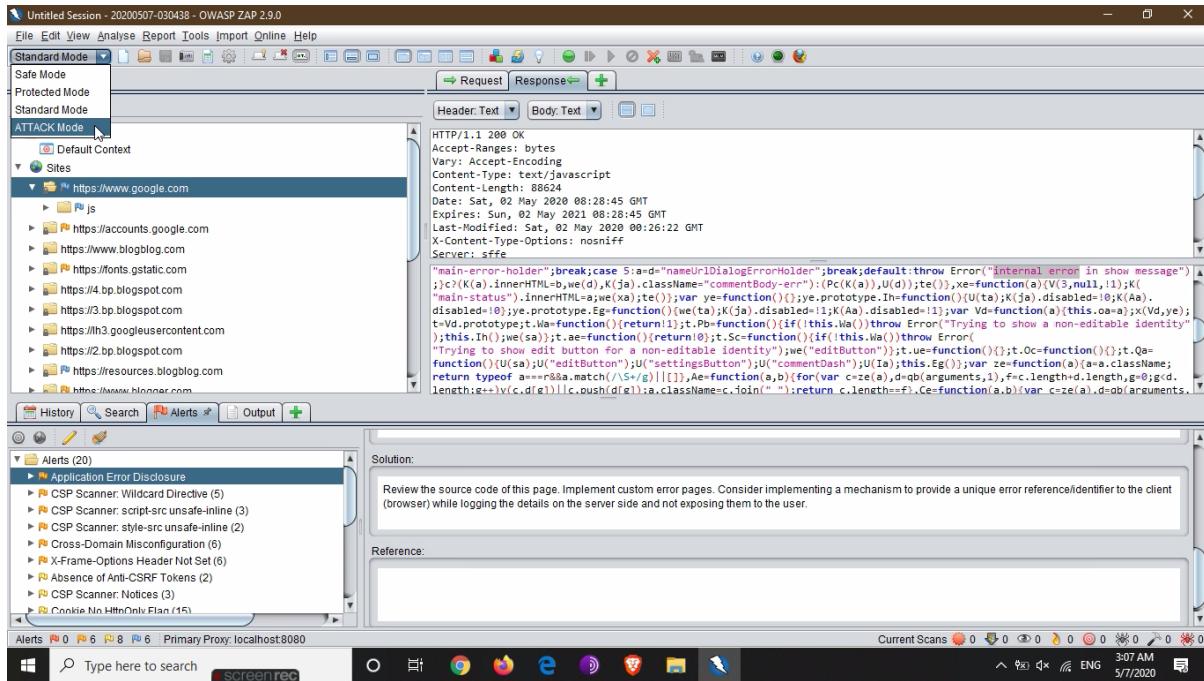
Number of found vulnerabilities are appeared Alerts bar below the application.



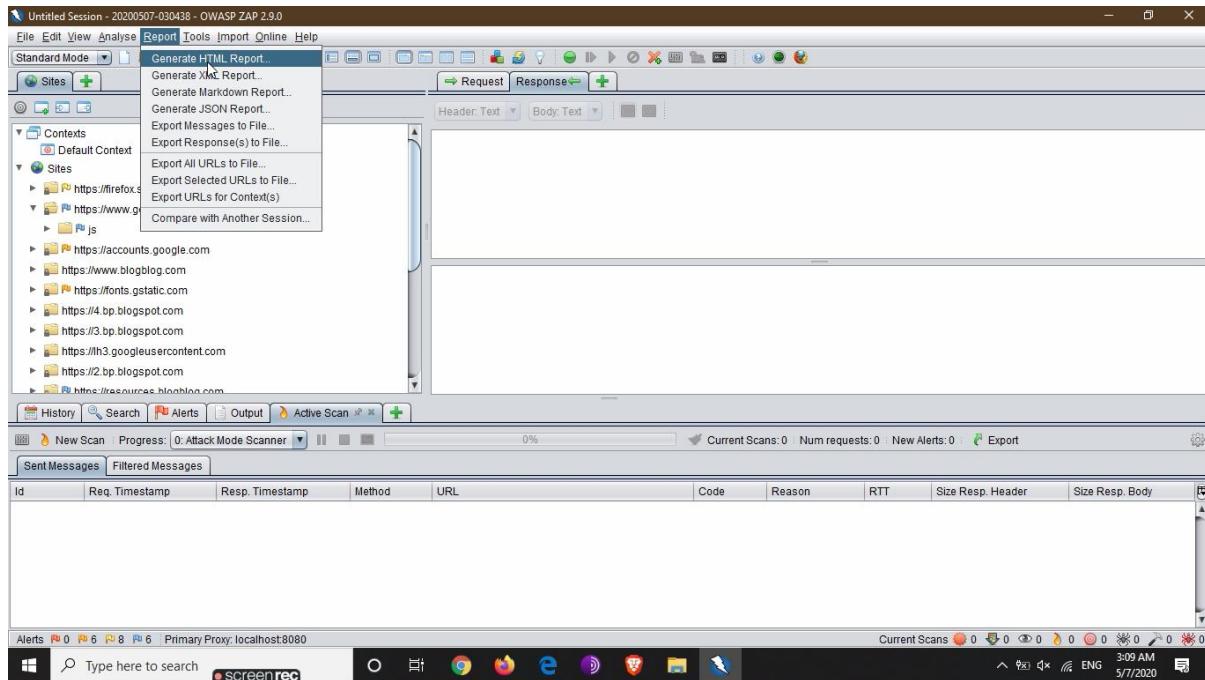
Click on a particular flag and then the part of the code is shown which the vulnerability is included along with the solution.



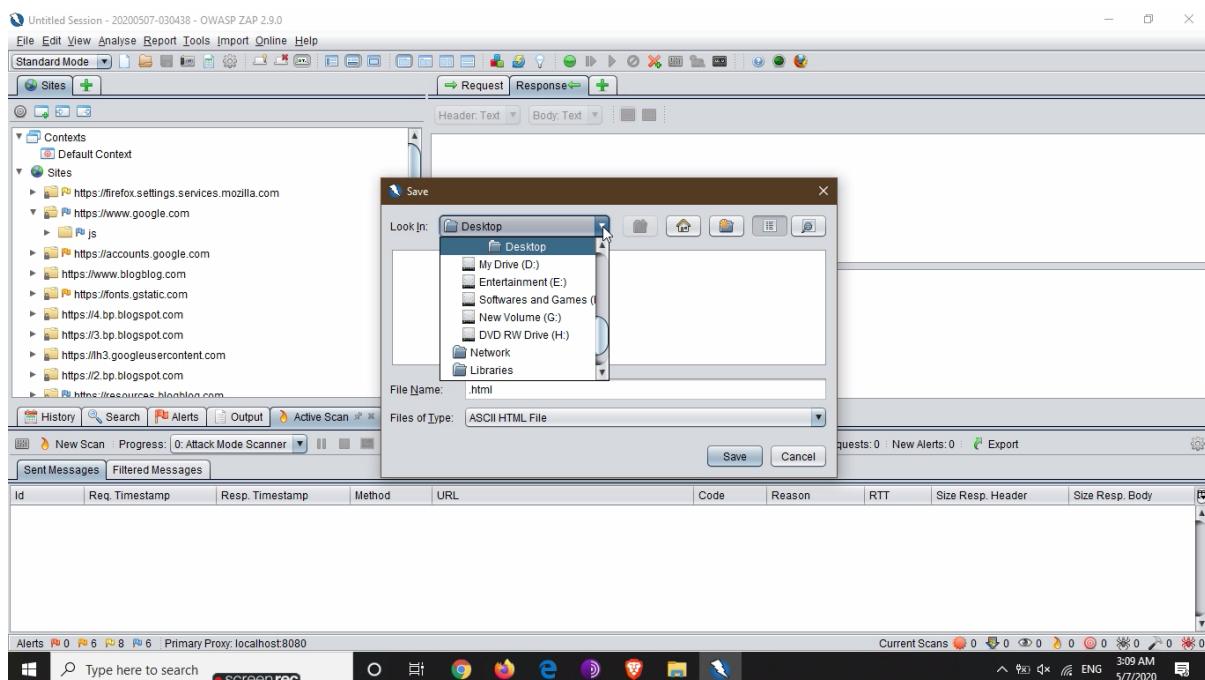
For now, only a “Passive Scan” was done. If a deeper scanning is needed, “ATTACK Mode” and “Active Scan” can be used. But, for now it is not allowed. Since, I’m doing this without the permission of the SLCERT.



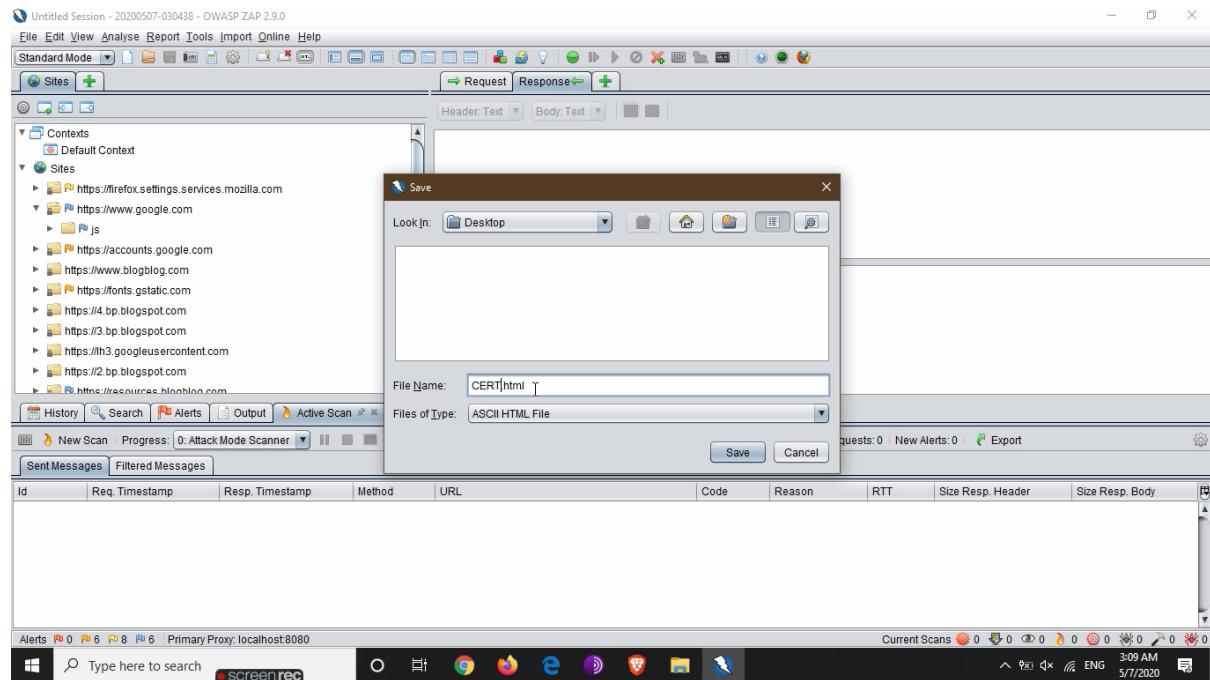
A Detailed Report can be generated using the Report tab.



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.

Risk Level	Number of Alerts
High	0
Medium	13
Low	24
Informational	23

## 5.2. SLCERT Website Scan - Nessus

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

The screenshot shows the Nessus Essentials web interface. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Scanners), and TENABLE (Community, Research). A Tenable News sidebar lists "Instacart Patches SMS Spoofing Vulnerability" with a "Read More" link. The main content area is titled "My Scans" and displays a message: "This folder is empty. Create a new scan." There are buttons for Import, New Folder, and + New Scan. The top navigation bar shows tabs for "Folders / My" (selected), "SSL Server Test (Powered by Qualys)" (Not secure), and "SSL Checker". The address bar shows "localhost:8834/#/scans/folders/my-scans". The taskbar at the bottom includes icons for screenrec, search, and other applications.

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

The screenshot shows the Nessus Essentials web interface on the "Scan Templates" page. The left sidebar is identical to the previous screenshot. The main content area is titled "VULNERABILITIES" and features a grid of scan templates. The "Web Application Tests" template is highlighted with a cursor icon over its thumbnail. Other templates include Basic Network Scan, Advanced Scan, Advanced Dynamic Scan, Malware Scan, Mobile Device Scan, Web Application Tests, Credentialed Patch Audit, Badlock Detection, Bash Shellshock Detection, DROWN Detection, Intel AMT Security Bypass, Shadow Brokers Scan, Spectre and Meltdown, and WannaCry Ransomware. The top navigation bar and taskbar are also visible.

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

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Scanners), and 'Tenable' (Community, Research). A 'Tenable News' section is also present. The main area is titled 'Scans' and has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', the 'BASIC' tab is selected, showing fields for 'Name' (IAA), 'Description' (empty), 'Folder' (My Scans), and 'Targets' (containing 'www.cert.gov.lk'). Below these fields are 'Upload Targets' and 'Add File' buttons. At the bottom of the main area are 'Save' and 'Cancel' buttons, with 'Cancel' being clicked. The status bar at the bottom shows the date and time as 5/7/2020 3:04 AM.

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

The screenshot shows the Nessus Essentials interface again. The sidebar and news section are identical to the previous screenshot. The main area now displays a scan named 'IAA'. It includes a 'Configure' and 'Launch' button. Below the scan name, there are tabs for 'Hosts' (0), 'Vulnerabilities' (0), and 'History' (0). A message says 'No hosts are available.' To the right, there's a 'Scan Details' section with 'Status: Empty' and 'Scanner: Local Scanner'. The status bar at the bottom shows the date and time as 5/7/2020 3:04 AM.

The scan was launched.

A screenshot of the Nessus Essentials web interface. The main title bar shows "SSL Server Test (Powered by Qualys)" and "SSL Checker". The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Scanners), and TENABLE (Community, Research). A "Tenable News" box is present. The central content area is titled "IAA" and shows a "History" tab with one entry. The entry details a scan started "Today at 3:04 AM" with status "Running". The "Scan Details" pane shows the policy is "Web Application Tests", status is "Running", scanner is "Local Scanner", and start time is "Today at 3:04 AM". Below this is a table with columns "Start Time", "Last Modified", and "Status". The bottom of the screen shows a Windows taskbar with icons for various applications like File Explorer, Google Chrome, and Microsoft Edge.

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

A screenshot of the Nessus Essentials web interface, similar to the previous one but showing a completed scan. The main title bar shows "SSL Server Test (Powered by Qualys)" and "ZAP Scanning Report". The central content area is titled "IAA" and shows a "Hosts" tab with one host entry: "www.cert.gov.lk". The "Scan Details" pane shows the policy is "Web Application Tests", status is "Completed", scanner is "Local Scanner", start time is "Today at 3:04 AM", end time is "Today at 3:27 AM", and elapsed time is "23 minutes". Below this is a "Vulnerabilities" section with a donut chart and a legend: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The bottom of the screen shows a Windows taskbar with icons for various applications like File Explorer, Google Chrome, and Microsoft Edge.

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

The screenshot shows the Nessus interface with a scan report titled "IAA". The "Vulnerabilities" tab is selected, showing 19 findings. A single critical vulnerability is highlighted on the host "www.cert.gov.lk". The "Scan Details" panel indicates the scan was completed by a local scanner, starting at 3:04 AM and ending at 3:27 AM, with an elapsed time of 23 minutes. A pie chart in the "Vulnerabilities" section shows the distribution of severity levels: 3% Critical, 0% High, 0% Medium, 0% Low, and 97% Info.

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.

This screenshot shows a detailed view of PHP vulnerabilities found during the scan. Three critical issues are listed: "PHP Unsupported Version Detection" (CGI abuses), "PHP 5.3.x < 5.3.28 Multiple OpenSSL V..." (CGI abuses), and "PHP 5.3.x < 5.3.29 Multiple Vulnerabiliti..." (CGI abuses). The "Scan Details" panel shows the same completion information as the previous screenshot. A pie chart in the "Vulnerabilities" section shows the distribution of severity levels: 33% Critical, 66% High, 0% Medium, 0% Low, and 1% Info.

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.

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Scanners), and 'Tenable News' (Ubiquiti UniFi Cloud, Key - Unprotected root, UART A...). The main area displays a scan result for 'IAA / Plugin #11213'. The 'Vulnerabilities' tab is selected, showing one item: 'HTTP TRACE / TRACK Methods Allowed' (Medium severity). The 'Description' section states: 'The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.' The 'Solution' section advises: 'Disable these HTTP methods. Refer to the plugin output for more information.' The 'Output' section contains configuration code for Apache:

```
To disable these methods, add the following lines for each virtual host in your configuration file :
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
```

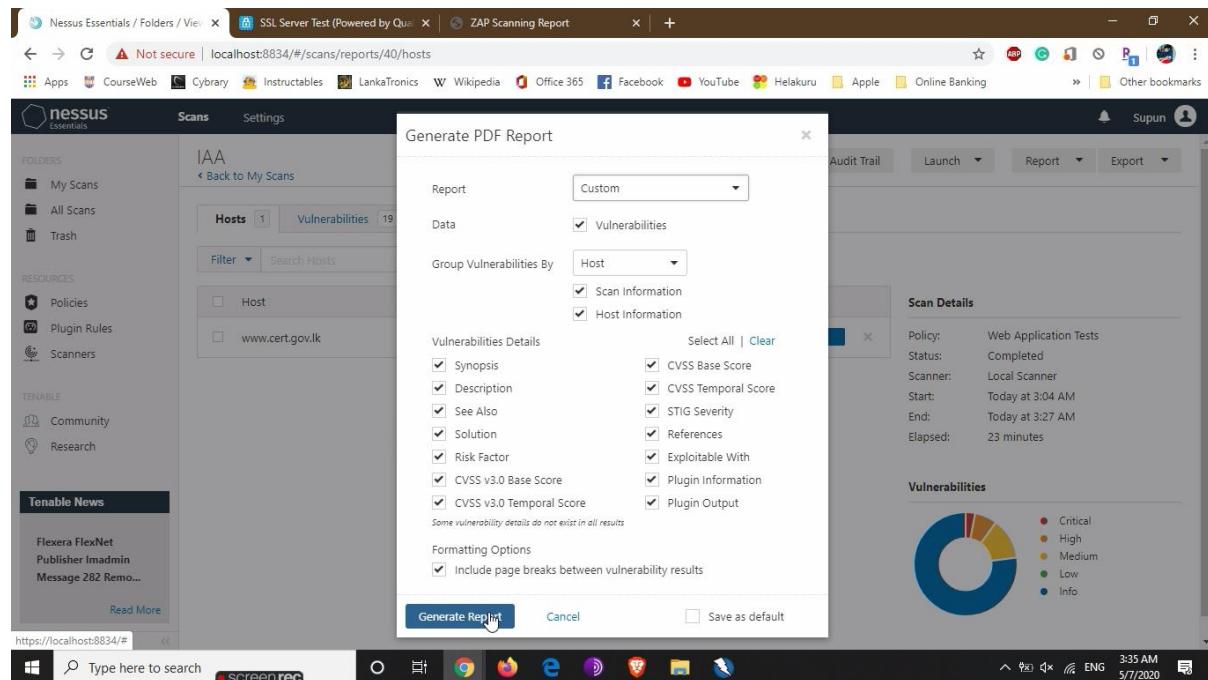
The 'Plugin Details' panel on the right provides metadata: Severity: Medium, ID: 11213, Version: 1.72, Type: remote, Family: Web Servers, Published: January 23, 2003, Modified: April 27, 2020. The 'Risk Information' panel shows CVSS v3.0 details: Base Score 5.3, Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N, Temporal Vector: CVSS:3.0/E:U/RLO/RC:C, Temporal Score: 4.6, CVSS Base Score: 5.0, CVSS Temporal Score: 3.7. The bottom status bar indicates the system is running screenrec, ENG, and the date/time is 5/7/2020 at 3:30 AM.

This screenshot shows another Nessus Essentials scan result for 'IAA / Plugin #10756'. The 'Vulnerabilities' tab is selected, showing one item: 'Apple Mac OS X Find-By-Content .DS\_Store Web Directory Listing' (Medium severity). The 'Description' section states: 'It is possible to read a '.DS\_Store' file on the remote web server. This file is created by Mac OS X Finder; it is used to remember the icons position on the desktop, among other things, and contains the list of files and directories present in the remote directory.' The 'Solution' section provides mitigation steps: 'Configure your web server so as to prevent the download of .DS\_Store files - Mac OS X users should configure their workstation to disable the creation of .DS\_Store files on network shares.' The 'See Also' section lists links: <https://support.apple.com/en-us/HT1629>, <https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html>, and <http://www.greyc.cc/?p=10>. The 'Plugin Details' panel shows: Severity: Medium, ID: 10756, Version: 1.31, Type: remote, Family: Web Servers, Published: September 14, 2001, Modified: November 15, 2018. The 'Risk Information' panel shows CVSS v3.0 details: Base Score 5.0, Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N, Temporal Vector: CVSS:3.0/E:U/RLO/RC:C, Temporal Score: 3.7. The bottom status bar indicates the system is running screenrec, ENG, and the date/time is 5/7/2020 at 3:31 AM.

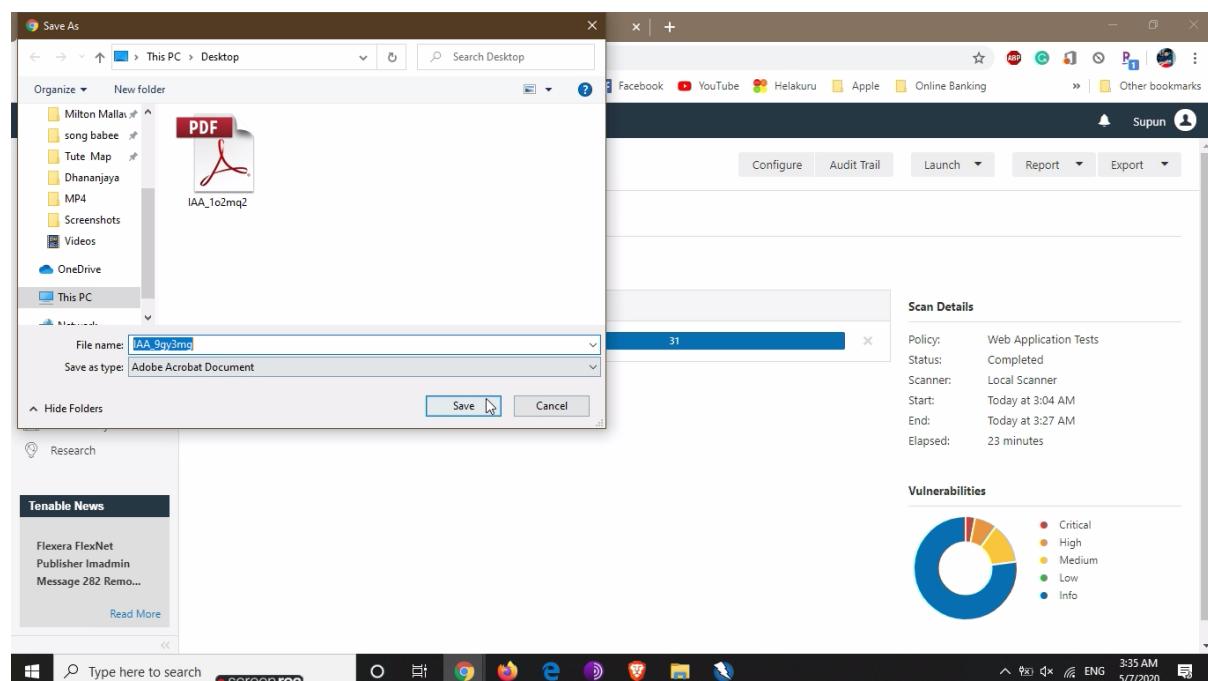
A Report can be generated using the “Report” button which is having PDF format or others. For the ease of use, this time PDF format is selected.

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.

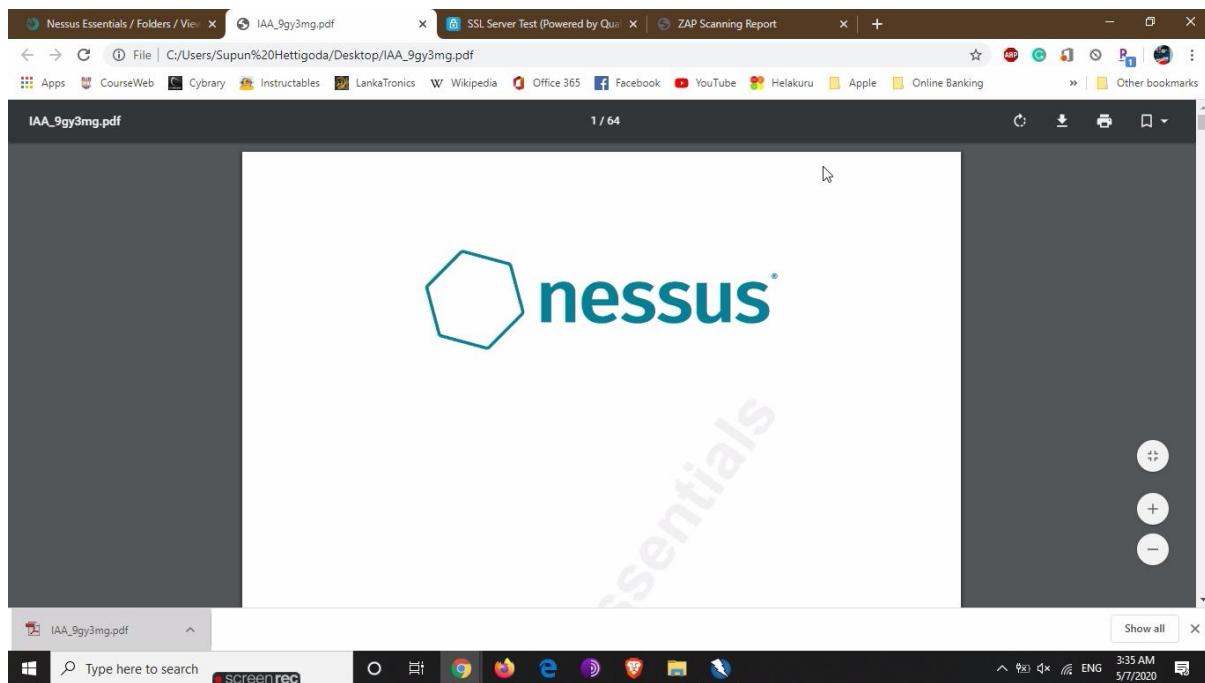
Report can be customized by checking the boxes as the auditor wish.



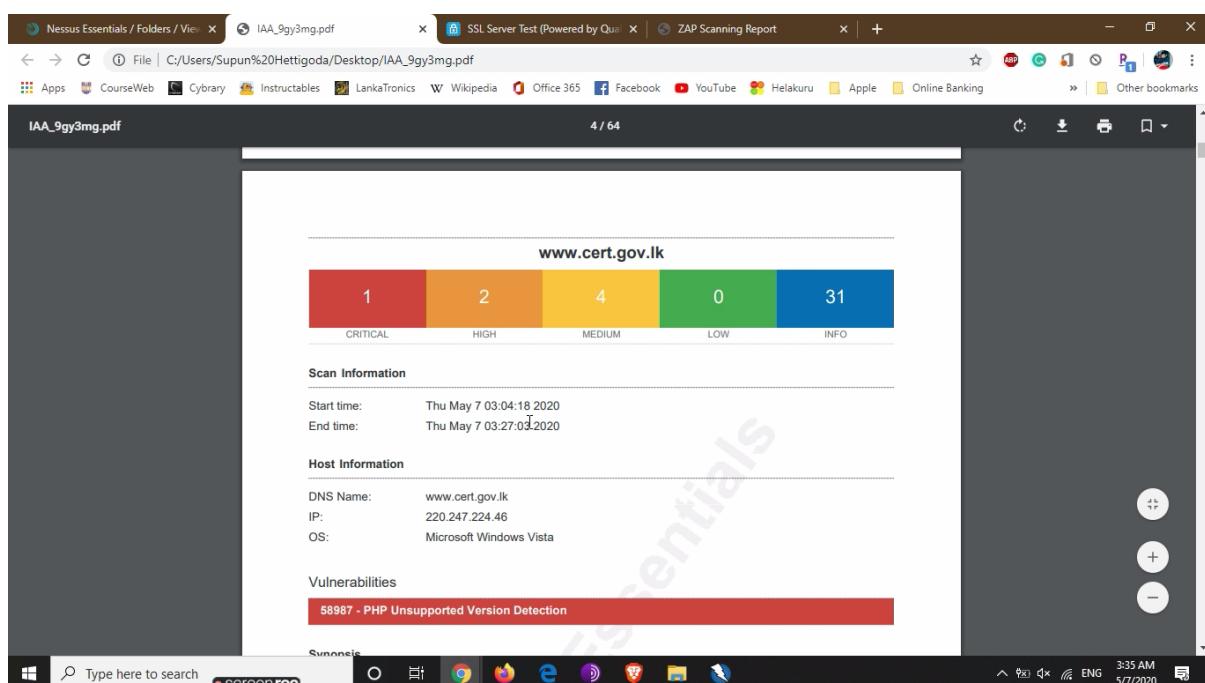
The file location should be selected. A file name also can be given.



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.

The remote host contains an unsupported version of a web application scripting language.

**Description**

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**See Also**

<http://php.net/eol.php>  
<https://wiki.php.net/rfc/releaseprocess>

**Solution**

Upgrade to a version of PHP that is currently supported.

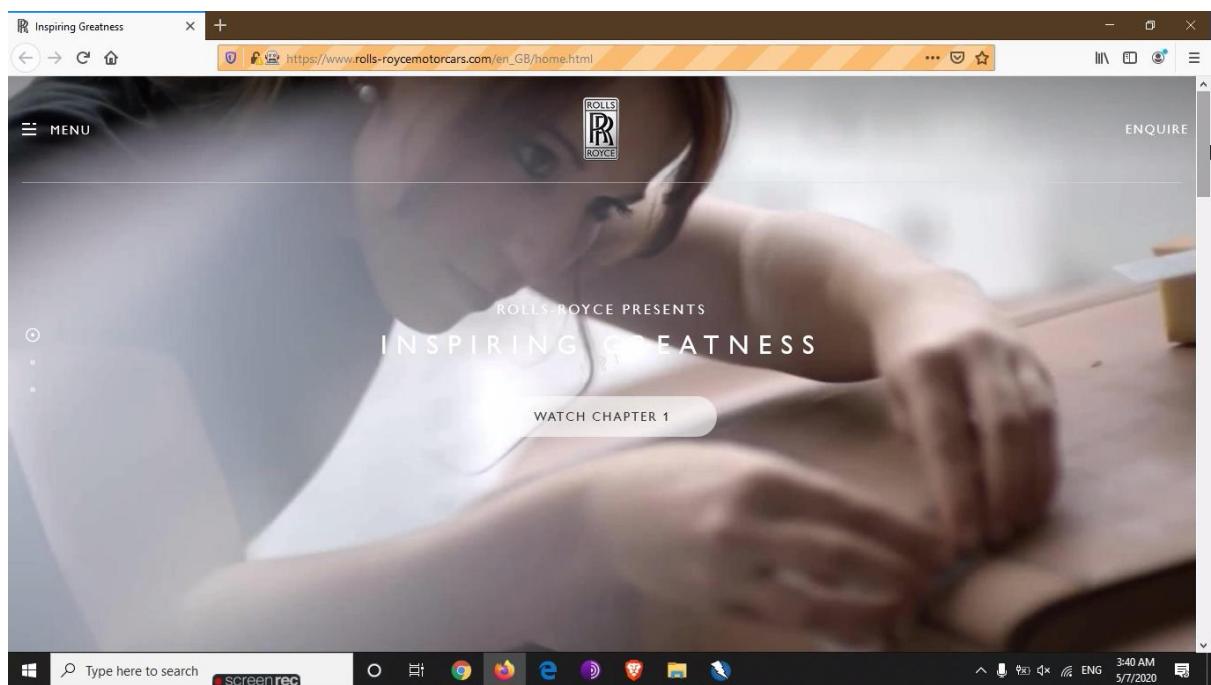
**Risk Factor**

Critical

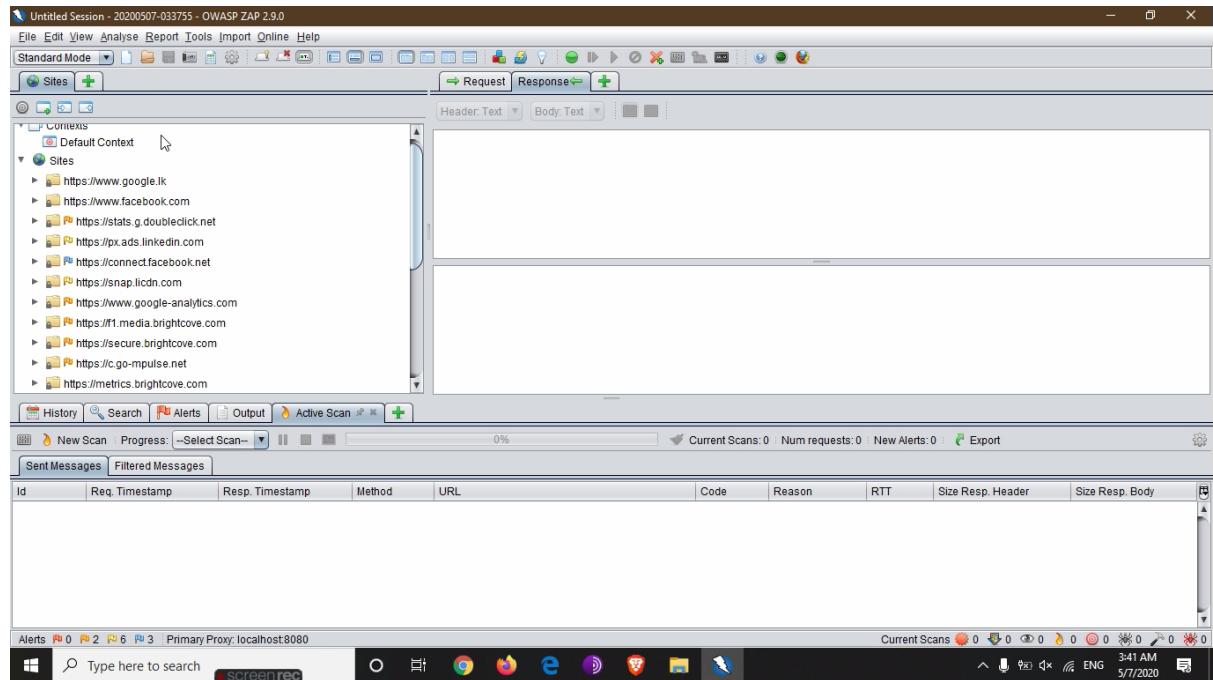
www.cert.gov.lk 4

### 5.3. Rolls-Royce Website Scan - ZAP

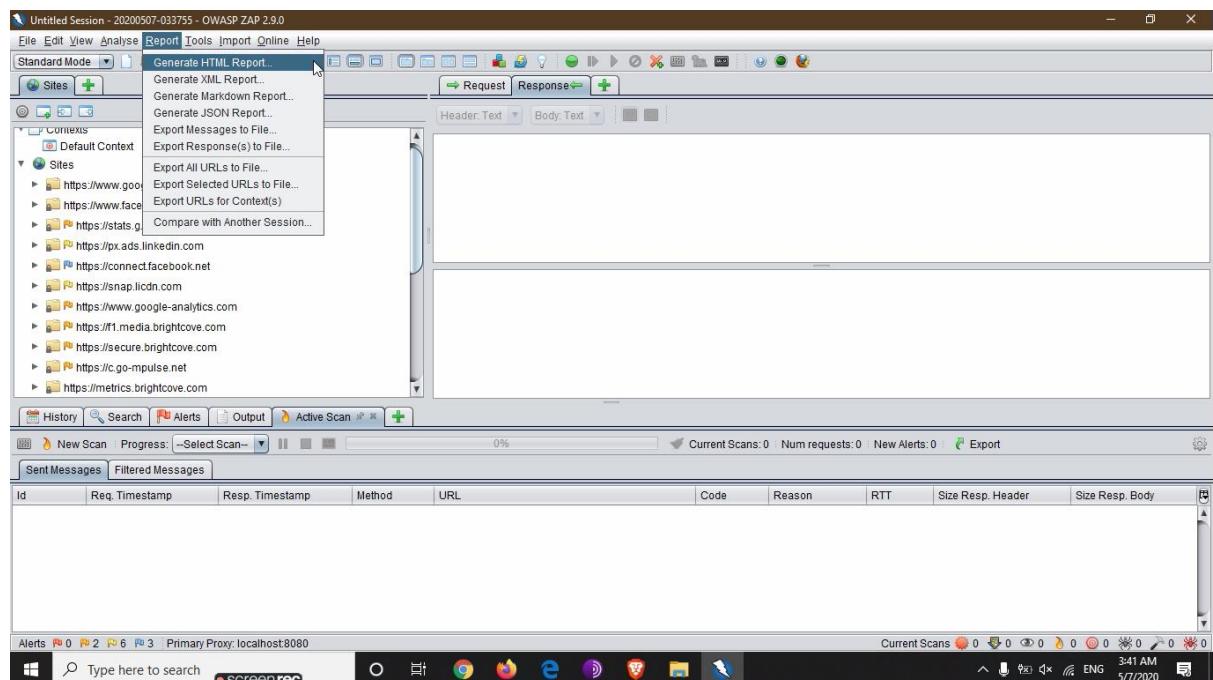
Browse the URL “www.rolls-roycemotorcars.com” using the supporting web browser.



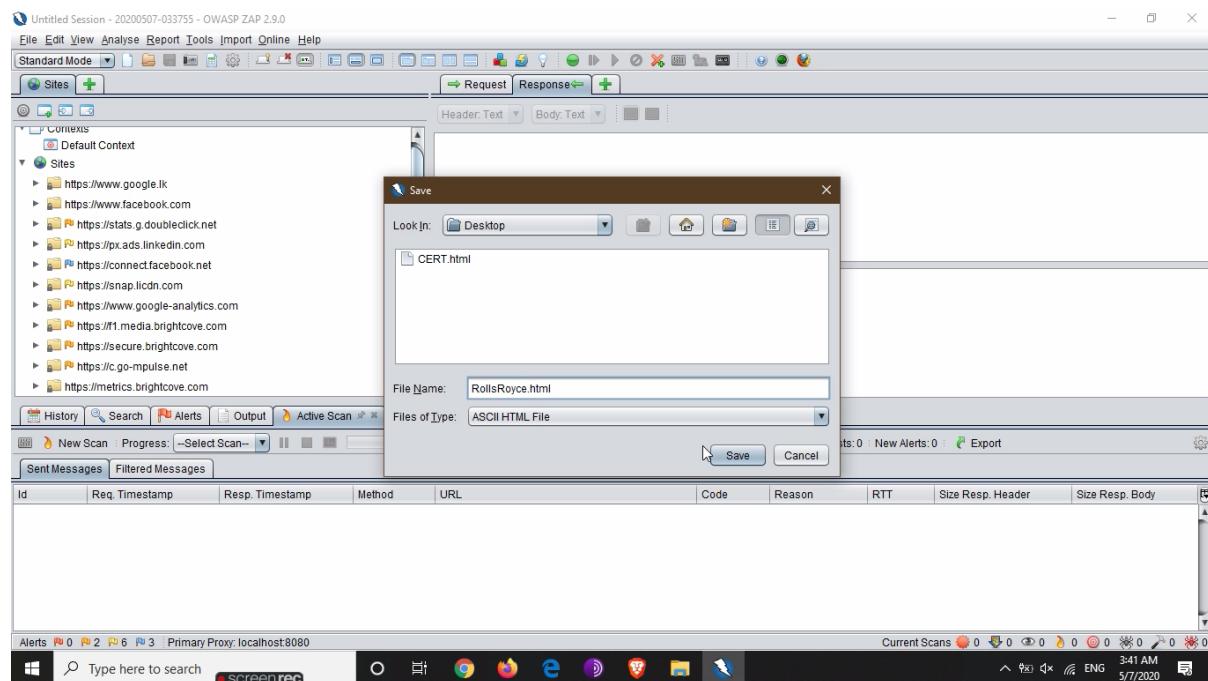
The scan is automatically started. Number of alerts can be seen.



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 alerts.

A screenshot of a web browser window titled 'ZAP Scanning Report'. The page displays a summary of alerts with a table showing the number of alerts per risk level: High (0), Medium (10), Low (20), and Informational (21). Below this, there's a section titled 'Alert Detail' which lists multiple entries, each with a URL, method (GET), and evidence related to Cross Domain Misconfiguration. The browser's address bar shows the file path 'C:/Users/Supun%20Hettigoda/Desktop/RollsRoyce.html'. The taskbar at the bottom shows various application icons and the system tray indicates it's 3:41 AM on 5/7/2020.

Descriptions and the Solutions are given regarding the vulnerabilities.

The screenshot shows a Microsoft Edge browser window with the title "ZAP Scanning Report". The address bar displays "File | C:/Users/Supun%20Hettigoda/Desktop/RollsRoyce.html". The main content area is a table from the ZAP report:

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	<a href="https://f1.media.brightcove.com/1/1634657725001/6147405382001/1634657725001_6147405382001_s-1.ts?pubId=1634657725001&amp;videoId=6147402859001">https://f1.media.brightcove.com/1/1634657725001/6147405382001/1634657725001_6147405382001_s-1.ts?pubId=1634657725001&amp;videoId=6147402859001</a>
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://f1.media.brightcove.com/1/1634657725001/6151591054001/1634657725001_6151591054001_s-1.ts?pubId=1634657725001&amp;videoId=6151582344001">https://f1.media.brightcove.com/1/1634657725001/6151591054001/1634657725001_6151591054001_s-1.ts?pubId=1634657725001&amp;videoId=6151582344001</a>
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://f1.media.brightcove.com/1/1634657725001/6138379143001/1634657725001_6138379143001_s-1.ts?pubId=1634657725001&amp;videoId=6138376320001">https://f1.media.brightcove.com/1/1634657725001/6138379143001/1634657725001_6138379143001_s-1.ts?pubId=1634657725001&amp;videoId=6138376320001</a>
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	3
Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).	
Solution	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	<a href="http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html">http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html</a>
CWE Id	264
WASC Id	14

The taskbar at the bottom shows the Windows Start button, a search bar with "screenrec", and icons for various applications like File Explorer, Google Chrome, Microsoft Edge, and others. The system tray shows the date and time as "5/7/2020 3:41 AM".

## 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 screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Scanners), and 'Tenable' (Community, Research). A 'Tenable News' sidebar is also present. The main area is titled 'Scans' and has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', the 'BASIC' tab is selected, showing fields for 'Name' (IAA 2), 'Description', 'Folder' (My Scans), and 'Targets' (www.rolls-roycemotorcars.com). Below these are 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons. The browser taskbar at the bottom shows the URL as localhost:8834/#/scans/reports/new/c3bcd46-329f-a9ed-1077-554fb2af33d0d44f09d736969bf/settings/basic/general.

The scan is launched.

The screenshot shows the Nessus Essentials interface. The sidebar is identical to the previous screen. The main area is titled 'My Scans' and shows a table with two rows. The columns are 'Name', 'Schedule', and 'Last Modified'. The first row is for 'IAA 2' with 'On Demand' schedule and 'Today at 3:43 AM' last modified. The second row is for 'IAA' with 'On Demand' schedule and 'Today at 3:27 AM' last modified. There are 'Import', 'New Folder', and 'New Scan' buttons at the top right of the table area. The browser taskbar at the bottom shows the URL as localhost:8834/#/scans/folders.

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

**Scan Details**

- Policy: Web Application Tests
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 4:35 AM
- End: Today at 5:37 AM
- Elapsed: an hour

**Vulnerabilities**

Severity	Count
Critical	0
High	0
Medium	0
Low	0
Info	18

Here is an issue regarding HTTP

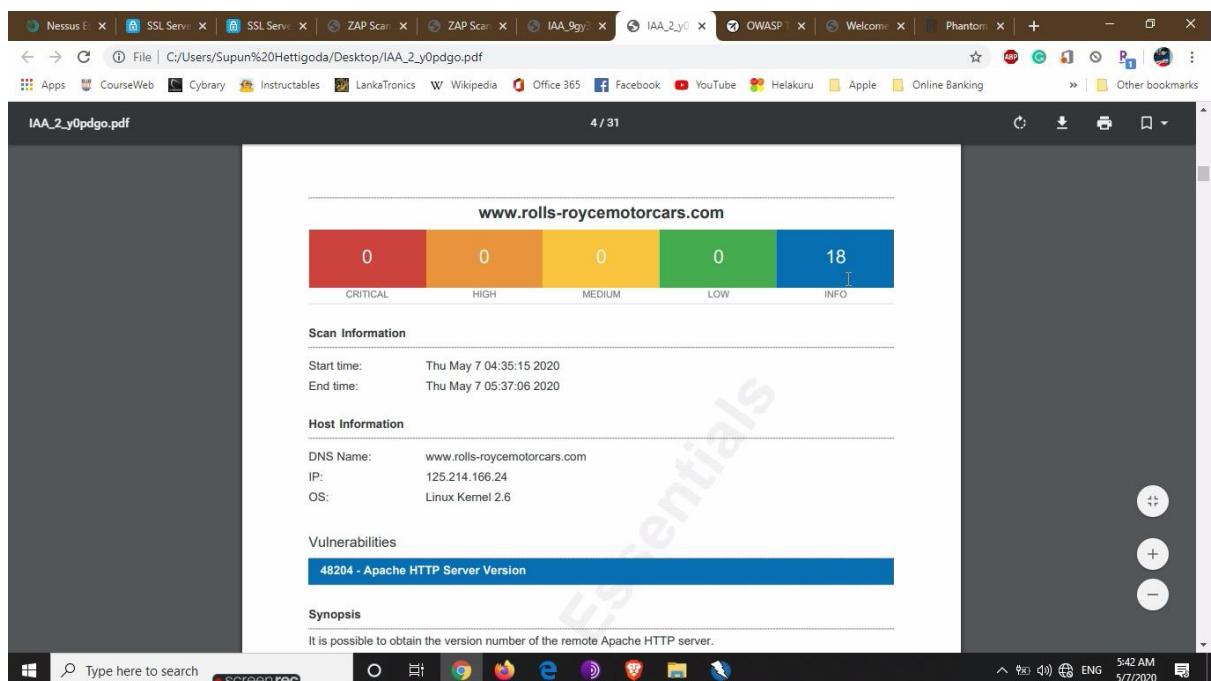
**Plugin Details**

- Severity: Info
- ID: 43111
- Version: 1.11
- Type: remote
- Family: Web Servers
- Published: December 10, 2009
- Modified: March 19, 2019

**Risk Information**

Risk Factor: None

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

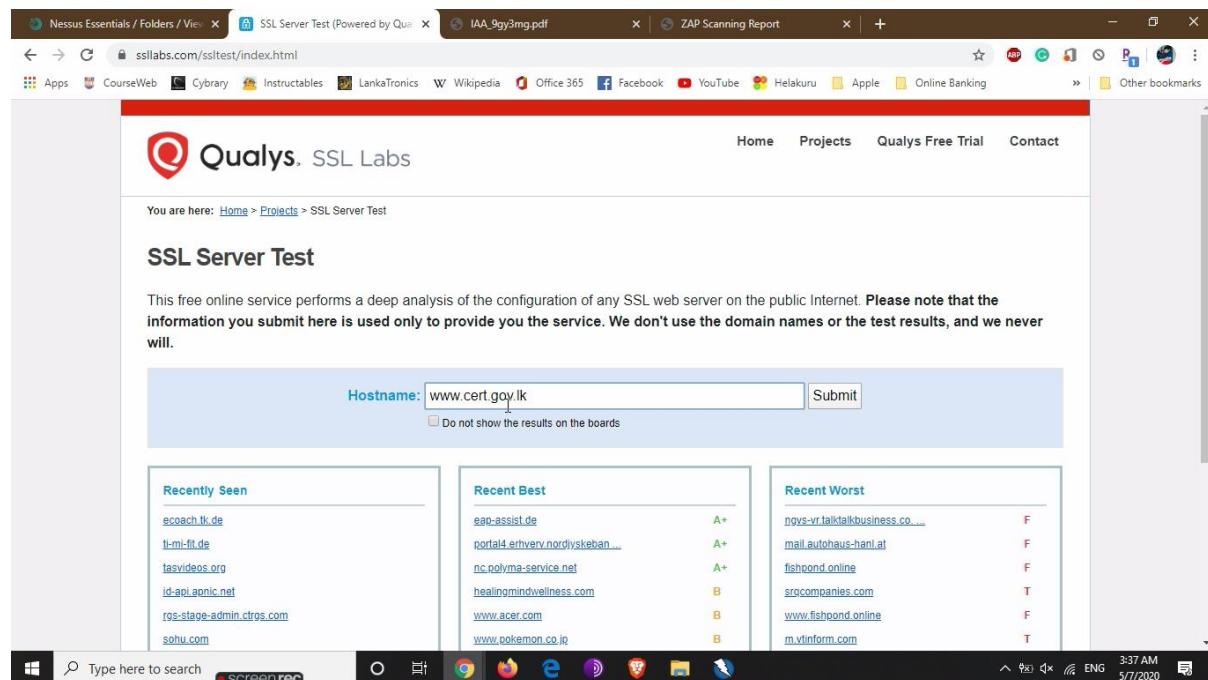


## 6. Audit - SSL and Certificate Testing

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.

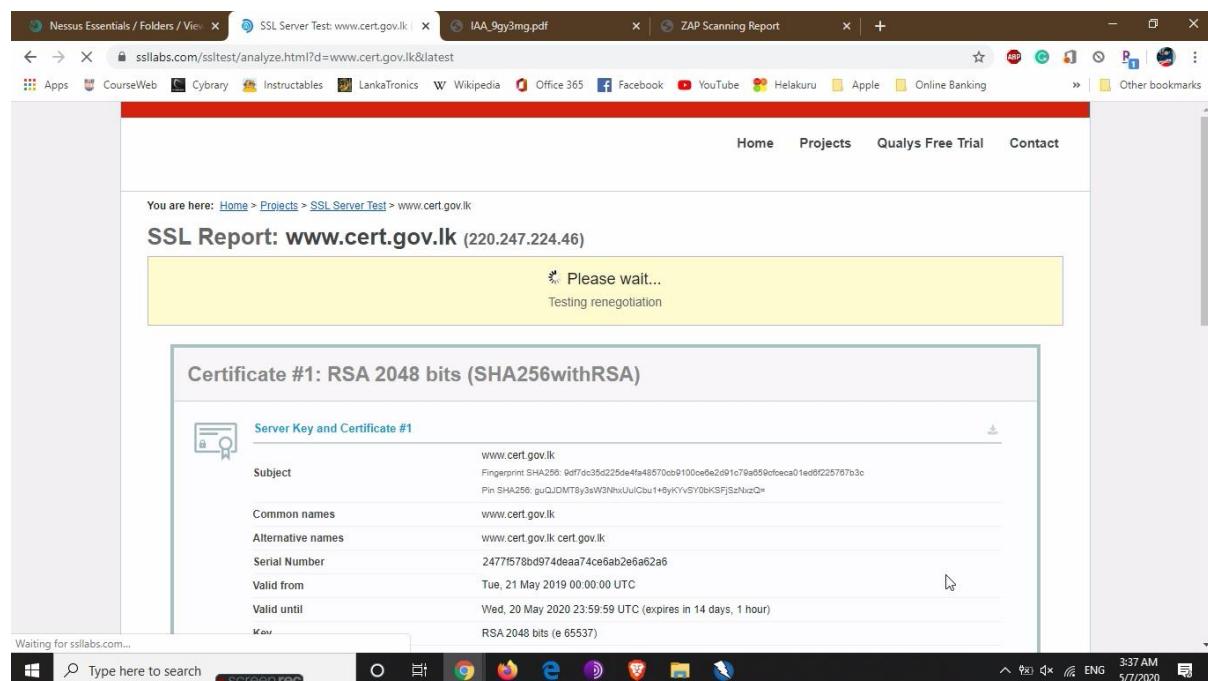
### 6.1. Test - SLCERT Website

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



The screenshot shows a Microsoft Edge browser window. The address bar contains `ssllabs.com/sslttest/index.html`. The main content area displays the Qualys SSL Server Test interface. At the top, there's a navigation bar with links to Home, Projects, Qualys Free Trial, and Contact. Below that, a message states: "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 field labeled "Hostname:" contains `www.cert.gov.lk`, with a "Submit" button next to it. Below the form is a checkbox labeled "Do not show the results on the boards". Under the "Recent Best" section, the website `www.cert.gov.lk` is listed with a grade of "A+". The "Recent Worst" section lists several websites with grades ranging from "F" to "T". The browser's taskbar at the bottom shows other open tabs for Nessus Essentials, Folders, View, ZAP Scanning Report, and IAA\_9gy3mg.pdf. The system tray indicates the date and time as 5/7/2020 3:37 AM.

Then the web tool is performing the testing.



The screenshot shows a Microsoft Edge browser window displaying the SSL Report for `www.cert.gov.lk`. The title bar says "SSL Report: www.cert.gov.lk (220.247.224.46)". A yellow box contains the message "Please wait... Testing renegotiation". Below this, a detailed view of "Certificate #1: RSA 2048 bits (SHA256withRSA)" is shown. The "Server Key and Certificate #" section includes fields for Subject (www.cert.gov.lk), Common names (www.cert.gov.lk), Alternative names (www.cert.gov.lk cert.gov.lk), Serial Number (24771578bd974deaa74ce6ab2e6a62a6), Valid from (Tue, 21 May 2019 00:00:00 UTC), Valid until (Wed, 20 May 2020 23:59:59 UTC), and Key (RSA 2048 bits (e 65537)). The browser taskbar shows other open tabs for Nessus Essentials, Folders, View, ZAP Scanning Report, and IAA\_9gy3mg.pdf. The system tray indicates the date and time as 5/7/2020 3:37 AM.

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

The screenshot shows a browser window with multiple tabs open. The active tab is the Qualys SSL Labs report for the website [www.cert.gov.lk](https://www.cert.gov.lk). The report summary indicates an overall rating of 'C'. A chart shows the following scores:

Category	Score
Certificate	98
Protocol Support	48
Key Exchange	68
Cipher Strength	68

Below the chart, two messages are displayed:

- "Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).
- "The server supports only older protocols, but not the current best TLS 1.2 or TLS 1.3. Grade capped to C. [MORE INFO](#)"

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.

The screenshot shows the 'Configuration' section of the Qualys SSL Labs report for [www.cert.gov.lk](https://www.cert.gov.lk). The 'Protocols' section lists supported protocols:

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

The 'Cipher Suites' section lists supported cipher suites in server-preferred order:

Cipher Suite	Key Size	Status
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256	WEAK
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	128	WEAK
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256	WEAK
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128	WEAK

The 'Handshake Simulation' section shows handshake results between the server and two clients:

Client	Protocol	Cipher Suite	Key Size	Status
Android 2.3.7	No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 4.0.4		RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS

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

The screenshot shows a Microsoft Edge browser window with several tabs open. The active tab displays the SSL Labs test results for the website www.cert.gov.lk. The results are presented in a table format:

Common names	www.cert.gov.lk
Alternative names	www.cert.gov.lk cert.gov.lk
Serial Number	2477f578bd974dea974ce6ab2e6a62a6
Valid from	Tue, 21 May 2019 00:00:00 UTC
Valid until	Wed, 20 May 2020 23:59:59 UTC (expires in 14 days, 1 hour)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Domain Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Below the main table, there is a section titled "Additional Certificates (if supplied)" which lists "Certificates provided" (2 (3087 bytes)) and "Chain issues" (None).

The browser's taskbar at the bottom shows various pinned icons and the system tray indicates the date and time as 5/7/2020 3:42 AM.

## 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 screenshot shows a web browser window with multiple tabs open. The active tab is titled "SSL Report: www.rolls-roycemotorcars.com". The page displays a table with four rows, each representing a server. The columns are "Server", "Test time", and "Grade". The first row shows "23.211.108.50" with a status of "In progress" and a grade of "-". The second row shows "2600:1406:1a:0:0:b832:5848" with a status of "Pending" and a grade of "-". The third row shows "23.211.108.120" with a status of "Pending" and a grade of "-". The fourth row shows "2600:1406:1a:0:0:b832:584a" with a status of "Pending" and a grade of "-". A yellow banner at the top of the report page says "Please wait... 3%". The browser's taskbar at the bottom shows various icons and the text "screenrec".

The web tool performs the scanning.

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "SSL Report: www.rolls-roycemotorcars.com (23.211.108.50)". The page displays a table with several rows of certificate information. The first row is "Certificate #1: RSA 2048 bits (SHA256withRSA)". The subsequent rows provide details about the server key and certificate, including the subject, common names, alternative names, serial number, valid from, valid until, and key details. A yellow banner at the top of the report page says "Please wait... 84% complete Testing Bleichenbacher". The browser's taskbar at the bottom shows various icons and the text "screenrec".

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

The screenshot shows the SSL Labs SSL Report for the website [www.rolls-roycemotorcars.com](http://www.rolls-roycemotorcars.com). The overall rating is **A+**. The report includes four bar charts: Certificate (green, ~98%), Protocol Support (green, ~98%), Key Exchange (green, ~88%), and Cipher Strength (green, ~88%). Below the charts, there are four informational boxes: "Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.", "This site works only in browsers with SNI support.", "This server supports TLS 1.3.", and "HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO](#)". The status bar at the bottom indicates it's 5:42 AM on 5/7/2020.

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+.

The screenshot shows the SSL Labs Configuration section for the same website. Under the "Protocols" heading, TLS 1.3 and TLS 1.2 are listed with "Yes" next to them, while TLS 1.1, TLS 1.0, SSL 3, and SSL 2 are listed with "No". Under the "Cipher Suites" heading, two sections are shown: "# TLS 1.3 (suites in server-preferred order)" and "# TLS 1.2 (suites in server-preferred order)". Both sections list various cipher suites with their key sizes (e.g., 256, 128) and other details. The status bar at the bottom indicates it's 5:43 AM on 5/7/2020.

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

The screenshot shows a web browser window with multiple tabs open at the top. The active tab displays the SSL Labs test results for the URL [ssllabs.com/sslttest/analyze.html?d=www.roolls-roycemotorcars.com&s=23.211.108.50&latest](https://www.roolls-roycemotorcars.com). The results are presented in a table format:

Setting	Value
Common names	www.roolls-roycemotorcars.com
Alternative names	careers.roolls-roycemotorcars.com www.careers.roolls-roycemotorcars.com www.roolls-roycemotorcars.com
Serial Number	041a19f9199ec86fe28ee3bda2f760a8f271
Valid from	Wed, 18 Mar 2020 13:02:05 UTC
Valid until	Tue, 16 Jun 2020 13:02:05 UTC (expires in 1 month and 9 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: <a href="http://cert.int-x3.letsencrypt.org/">http://cert.int-x3.letsencrypt.org/</a>
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP: <a href="http://ocsp.int-x3.letsencrypt.org">http://ocsp.int-x3.letsencrypt.org</a>
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Below the main table, there is a section titled "Additional Certificates (if supplied)" which lists "Certificates provided" as 2 (2641 bytes) and "Chain issues" as None.

## 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	 SRI LANKA CERT   CC	
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 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](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](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].