



IE4040: Information Assurance and Auditing
4th Year – 1st Semester
Mini Project - Report

Registration No: IT17102056

Name : Shehan D.S

Batch : CSNE – Weekend

Declaration

I declare that this is my own work and this report does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID
Shehan D.S.	IT17102056

Abstract

In the present times, as a result of development in information technology the web applications are arise. Nowadays web applications or websites are become very popular in the world. Most of the organizations have their own web application. Even little companies also have their own web application. These organizations stored their valuable data in their web application. To protect their data or information they need a mechanism to check or analyze the security of their web application. As a solution for this matter Audits are arise. Security audit means basically scan the web application for vulnerabilities. For organizations identifying the weakness of their web applications is very important. By conducting a security audit, they can identify their web application's weakness and they can cure their vulnerabilities and maintain a better secured web application. There are so many freely and commercial web application testing tools are available to conduct these security audits. This report is about “www.sliit.lk” website’s security audit using a tool called “Nessus”.

Table of Contents

<i>Declaration</i>	1
1. <i>Introduction</i>	4
2. <i>Web application testing tools</i>	5
3. <i>Introduction to “Nessus” web application scanning tool</i>	7
4. <i>Steps to audit “www.sliit.lk” using “Nessus professional” tool</i>	9
5. <i>Additional website scanning</i>	13
1. GT-Metrix website performance testing	13
2. SEO test using “site-checker” tool.....	14
6. <i>Conclusion and Recommendation</i>	15
7. <i>Reference</i>	16

1. Introduction

Nowadays web applications are popular title in the world. Everyone in the world are known about web applications and most of them have used these web applications. All the business organizations are using these web applications to do their business. For these organizations very important to keep their website up and running and to give well secured user experience. To keep websites in a well secured way we have to perform websites monitoring and conduct regular security audits.

Actually, website security audit means, looking for the vulnerabilities of the website. That means we do a scan using a website testing tool and that tool gives us a report about all the weakness in our website and some tools also gives us solutions for these issues in our website.

Main purpose of the website audit is to find issues or problems in our website. Broken tags, broken links are some examples for these weaknesses that we are going to identify using these audits. Also website audit ensure the data protection of our website.

There are so many audits that we can perform to our website to analyze our website. They are,

- Backlink audit.
- Advanced client audit.
- Search Engine Optimization audit.(SEO)
- Vulnerability and security scans.

But when we talk about web application audit, main concern is the security audit. That is because these web applications are in the open network. That means in the internet. So, for these web applications security is the main problem. So that security audits are very important to web applications.

2. Web application testing tools

1. Abbey Scan.

- Owner is the “MisterScanner” company.
- This is free and open source tool.

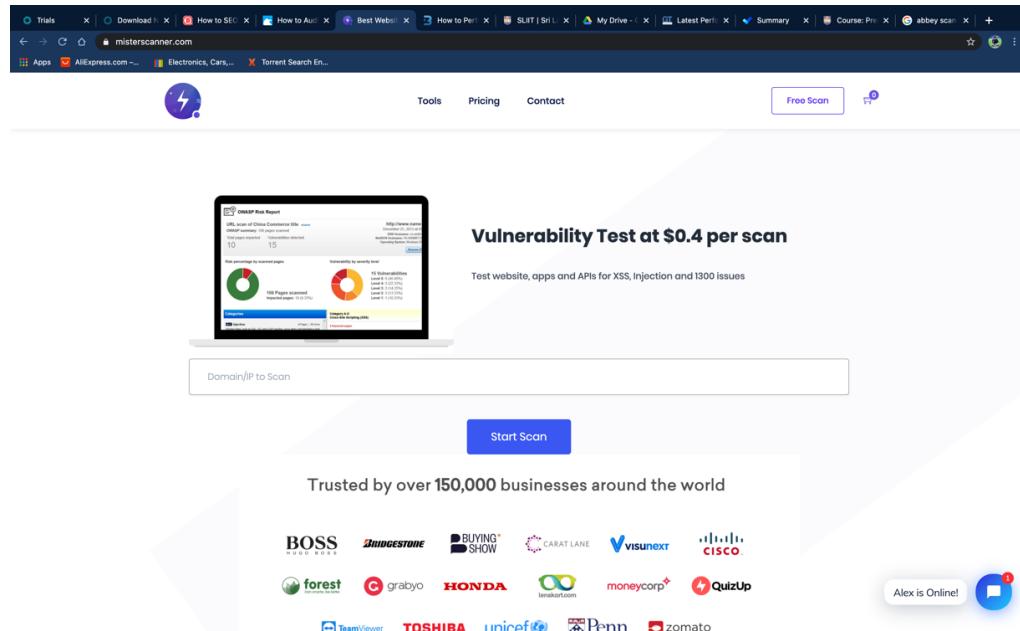


Fig: 1.1 : Abbey Scan tool interface.

2. Arachni.

- Owner is “Arachni” company.
- Free for most use cases.

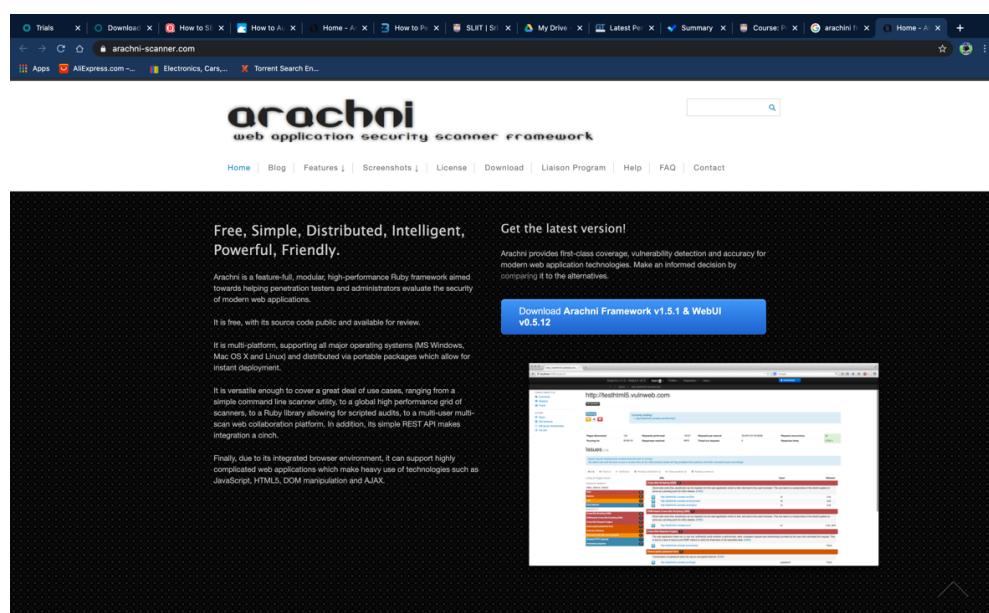


Fig: 1.2 : arachni tool website.

3. Detectify

- Owner is the “ Detectify” company.
- This is a paid tool.

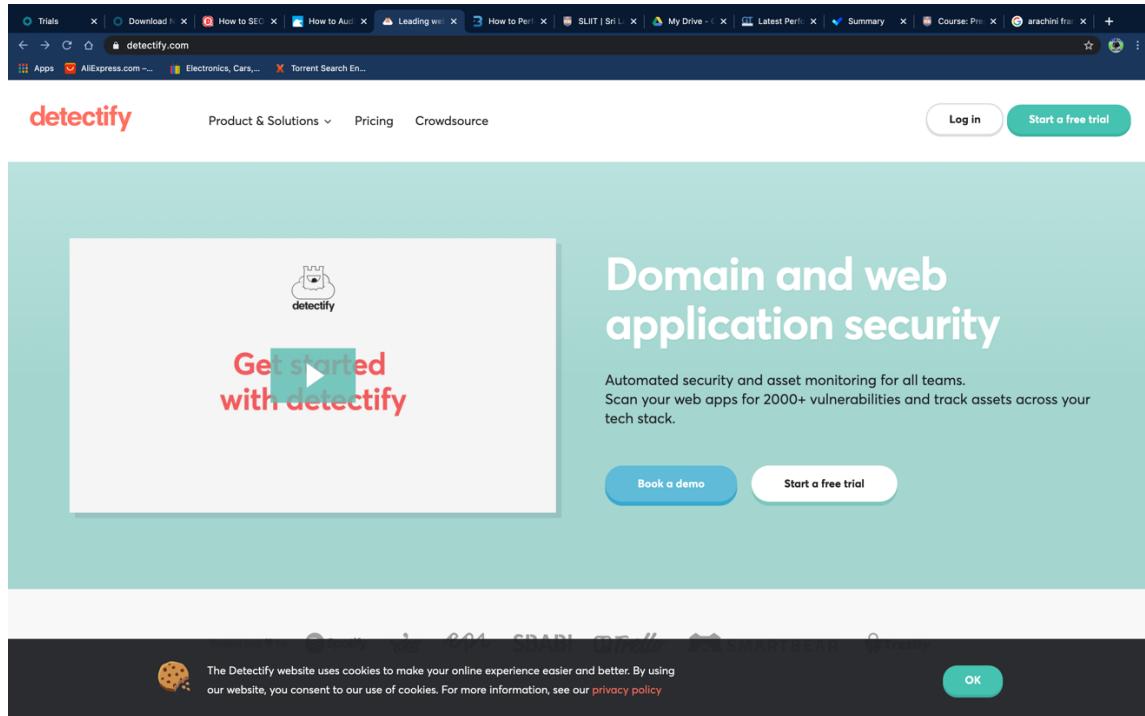


Fig 1.3: Detectify company website.

4. W3af.

- Owner is the “ w3af.org”.

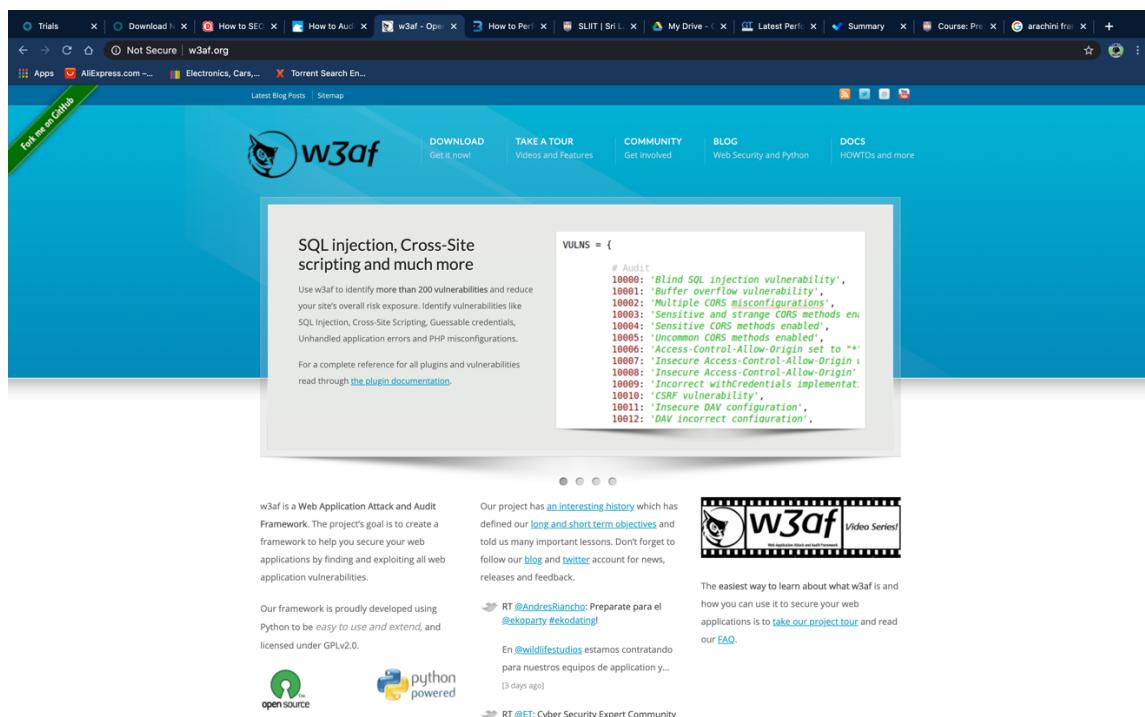


Fig 1.4 : w3af.org wesite interface.

3. Introduction to “Nessus” web application scanning tool

Nessus professional security scanning tool is a commercial web application testing tool. “tenable” is one of the major security provider in the world. “Nessus pro” is one of their tool. [1]

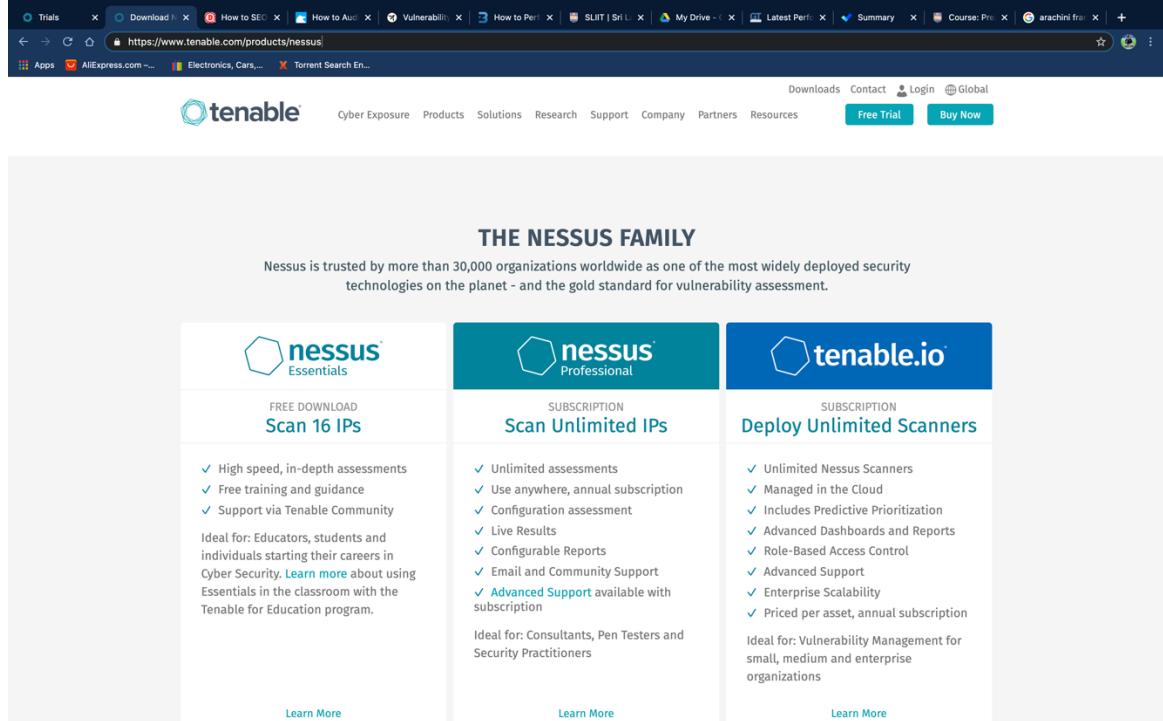


Fig 2.1: Tenable.com products page

“Nessus professional” login page. In here you have to provide your credentials to log into the nessses.

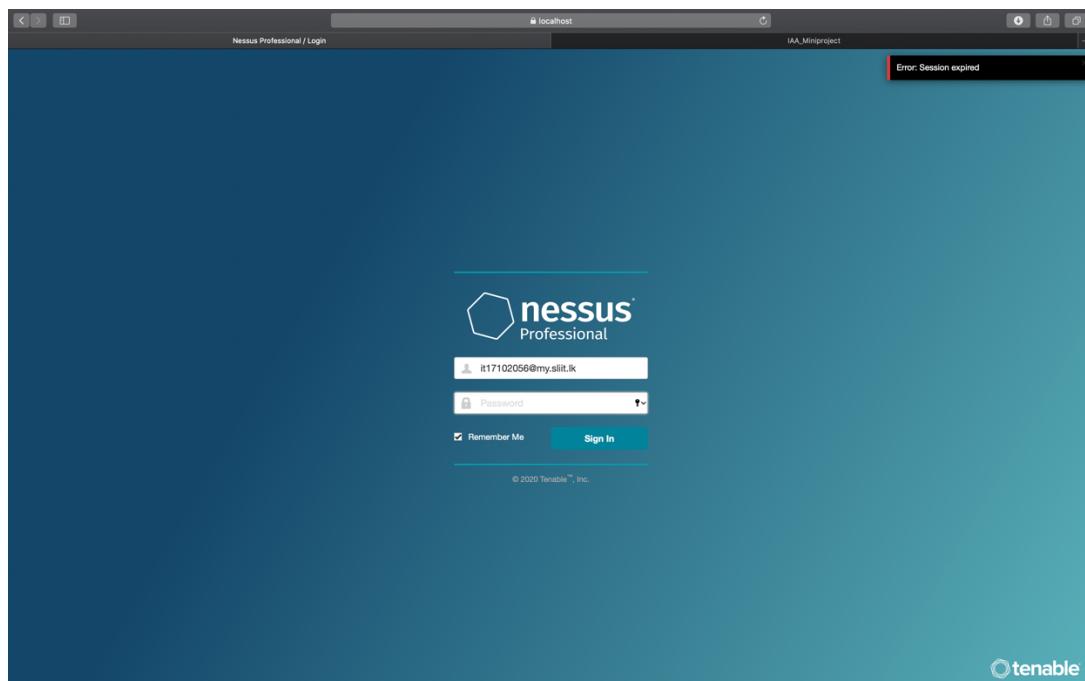


Fig 2.2 : Nessus professional login page.

Not only the website testing but also nessus pro tool can perform many things.

The screenshot shows the 'Scan Templates' section of the Nessus Professional interface. The left sidebar includes 'Scans' (selected), 'Settings', 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Customized Reports, Scanners), and 'Tenable' (Community, Research). The main content area is titled 'Scan Templates' with a 'Scanner' search bar and a 'Search Library' button. It is organized into three sections: 'DISCOVERY', 'VULNERABILITIES', and 'COMPLIANCE'. The 'DISCOVERY' section contains one item: 'Host Discovery'. The 'VULNERABILITIES' section contains twelve items: 'Basic Network Scan', 'Advanced Scan', 'Advanced Dynamic Scan', 'Malware Scan', 'Mobile Device Scan' (marked as 'UNOFFICIAL'), 'Web Application Tests', 'Credentialed Patch Audit', 'Bash Shellshock Detection', 'DROWN Detection', 'Intel AMT Security Bypass', 'Shadow Brokers Scan', 'Spectre and Meltdown', and 'WannaCry Ransomware'. The 'COMPLIANCE' section contains six items: 'Audit Cloud Infrastructure', 'Internal PCI Network Scan' (marked as 'UNOFFICIAL'), 'MDM Config Audit' (marked as 'UPGRADE'), 'Offline Config Audit', 'PCI Quarterly External Scan' (marked as 'UNOFFICIAL'), and 'Policy Compliance Auditing'.

Fig 2.3 : nessus scan templates page.

4. Steps to audit “www.sliit.lk” using “Nessus professional” tool

1. After logging to the “Nessus Pro” tool, click on the new scan button on top right of the page.

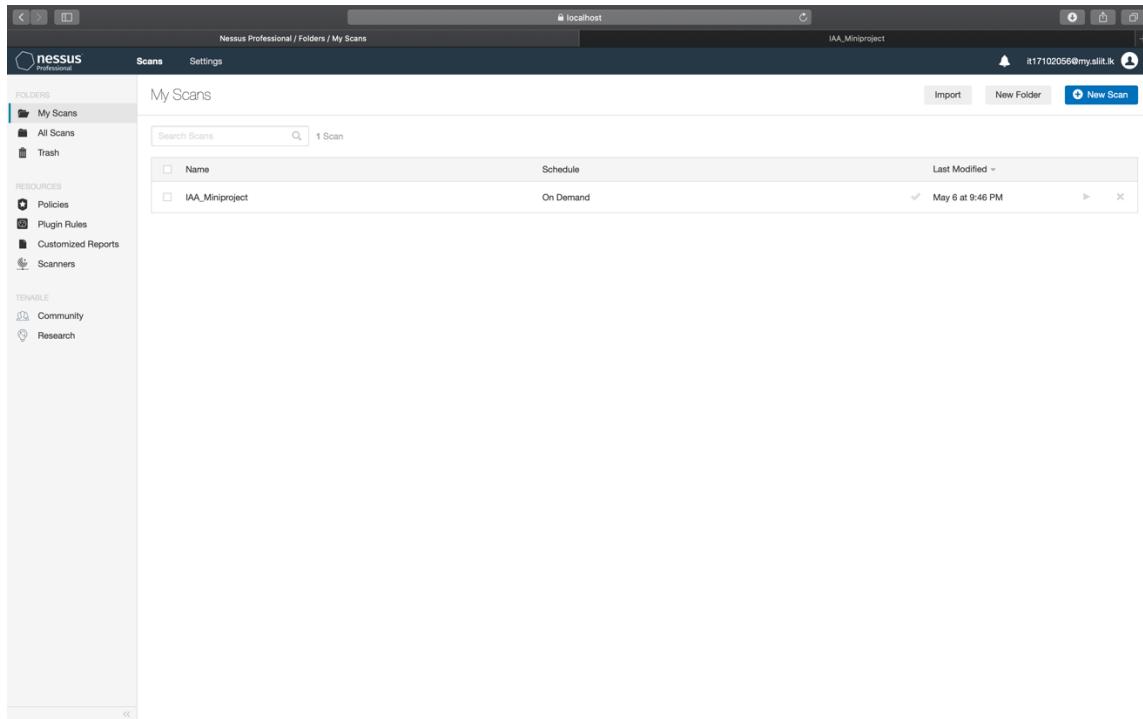


Fig 3.1: My scans page on Nessus pro tool.

2. Then in the scan template page select the “ web application testing” .

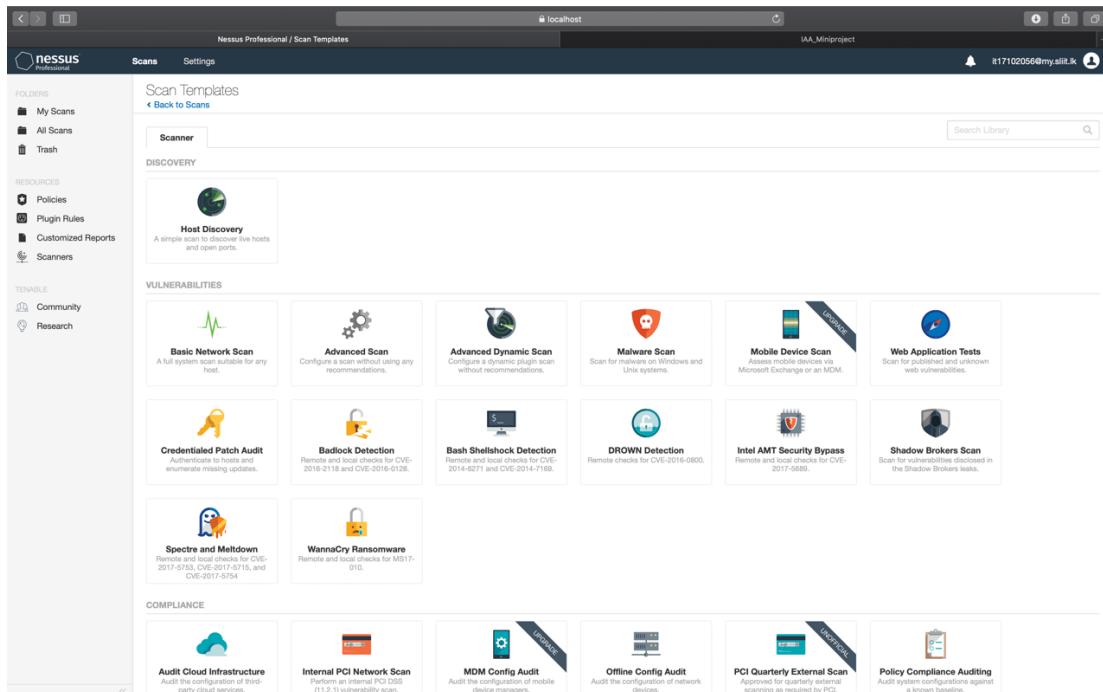


Fig: 3.2: Scan templates page

3. Then just put a scan name and set the target as “www.sliit.lk”. And press save.

The screenshot shows the 'Scans / Editor' section of the Nessus Professional interface. On the left, a sidebar lists 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Customized Reports, Scanners), and 'Tenable' (Community, Research). The main panel is titled 'New Scan / Web Application Tests' and contains a 'Back to Scan Templates' link. It has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', the 'BASIC' tab is selected, showing 'General' settings with 'Name' set to 'IAA_Miniproject', 'Description' empty, 'Folder' set to 'My Scans', and 'Targets' set to 'www.sliit.lk'. There are also sections for 'Post-Processing' and 'Upload Targets' (with an 'Add File' button). At the bottom are 'Save' and 'Cancel' buttons.

Fig: 3.3: web application testing configure page.

4. Then go to the my scan folder and select the scan that we save in the earlier step and launch it.

The screenshot shows the 'Folders / My Scans' section of the Nessus Professional interface. The sidebar is identical to Fig 3.3. The main panel displays a table titled 'My Scans' with two entries: 'IAA_Miniproject' (Schedule: On Demand, Last Modified: May 6 at 9:46 PM) and 'IAA_Miniproject1' (Schedule: On Demand, Last Modified: N/A). A search bar at the top right shows '2 Scans'. At the bottom right are buttons for 'Import', 'New Folder', and 'New Scan'.

Fig: 3.4 : my scan folder.

5. Now the scan is on running mode. Wait till it end.

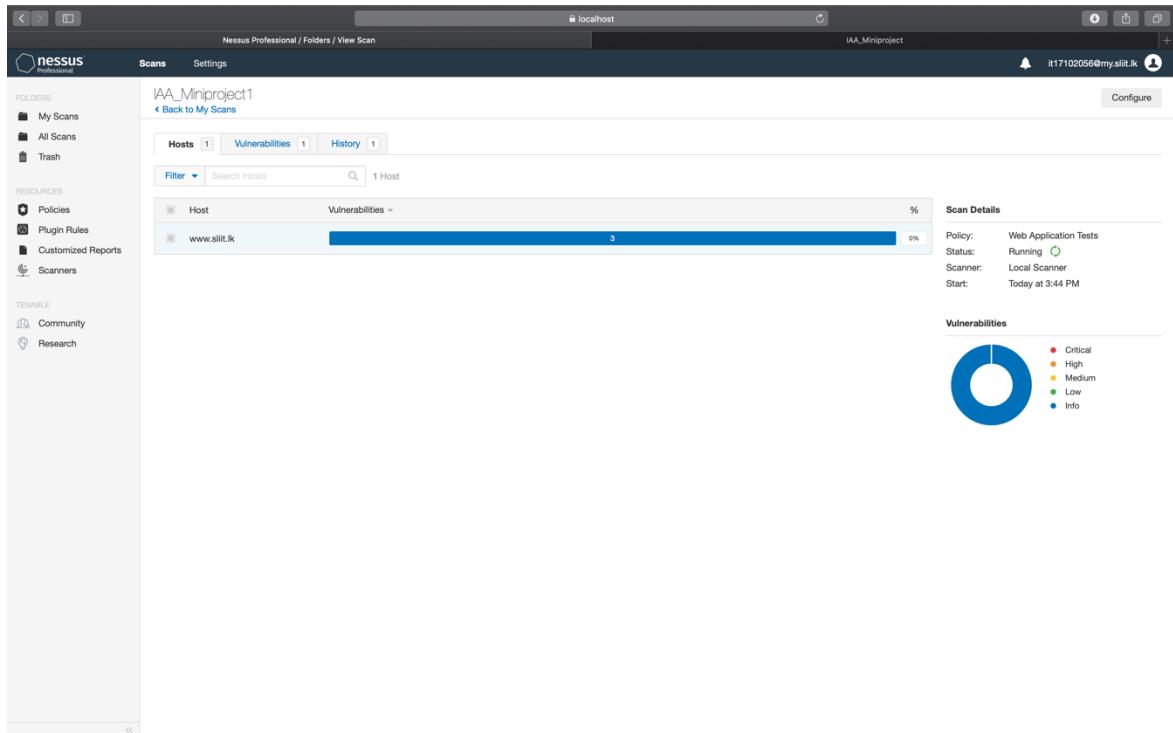


Fig:3.5: scan running page

6. After scan ends we can get a report.

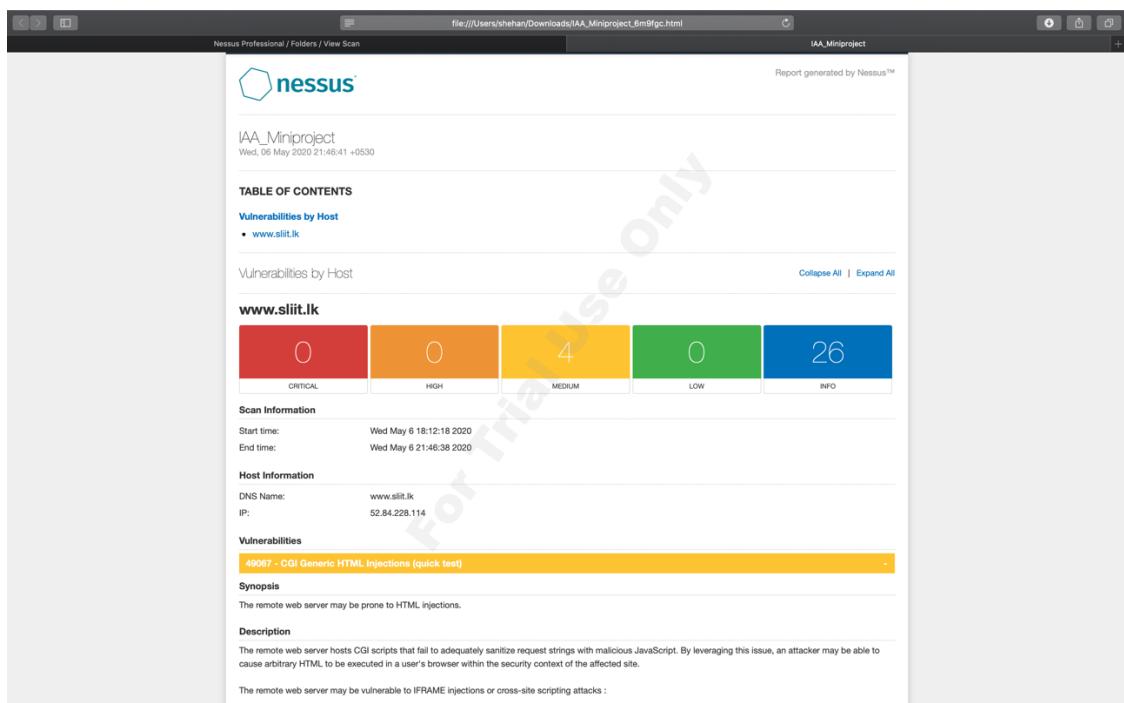


Fig: 3.6: IAA_Miniproject report picture 1

```

file:///Users/shehan/Downloads/IAA_Miniproject_6m9/gc.html
IAA_Miniproject

+ The 'field1' parameter of the /student-life/accommodations/ CGI :
/student-life/accommodations/?field1=%0<<<"gviby%20>>>

----- output -----
<link rel="alternate" type="application/json+oembed" href="https://[...]
<link rel="alternate" type="text/xml+oembed" href="https://www.sli [...]
t-life/accommodations/?field1=%0<<<"gviby%20>>>"><link rel="alternat
e" hreflang="si-LK" href="https://www.sliit.lk/si/student-life/accommo
dations/?field1=%0<<<"gviby%20>>>"><link rel="alternate" hreflang="ta
-IN" href="https://www.sliit.lk/ta/student-life/accommodations/?field1=%0
<<<"gviby%20>>>"><meta name="theme-color"
content="#033769">
<meta name="viewport" content="width=device-width, initial-scale=1 [...]
----- output -----
```

+ The 'field1' parameter of the /student-life/sports/ CGI :

```

/student-life/sports/?field1=%0<<<"gviby%20>>>

----- output -----
<link rel="alternate" type="application/json+oembed" href="https://[...]
<link rel="alternate" type="text/xml+oembed" href="https://www.sli [...]
t-life/sports/?field1=%0<<<"gviby%20>>>"><link rel="alternate" href=
ang="si-LK" href="https://www.sliit.lk/si/student-life/sports/?field1=%0
0<<<"gviby%20>>>"><link rel="alternate" hreflang="ta-IN" href="https:
/www.sliit.lk/ta/student-life/sports/?field1=%0<<<"gviby%20>>>">
<meta name="theme-color"
content="#033769">
<meta name="viewport" content="width=device-width, initial-scale=1 [...]
----- output -----
```

+ The 'field1' parameter of the /computing/programmes/computer-systems-network-engineering-degree/ CGI :

```

/computing/programmes/computer-systems-network-engineering-degree/?field
1=%0<<<"gviby%20>>>

----- output -----
<link rel="alternate" type="application/json+oembed" href="https://[...]
<link rel="alternate" type="text/xml+oembed" href="https://www.sli [...]
[...] engineering-degree/?field1=%0<<<"gviby%20>>>"><meta name="theme-color"
content="#033769">
<meta name="viewport" content="width=device-width, initial-scale=1 [...]
----- output -----
```

+ The 'field1' parameter of the /computing/programmes/software-engineering-degree/ CGI :

```

/computing/programmes/software-engineering-degree/?field1=%0<<<"gviby
%20>>>

----- output -----
<link rel="alternate" type="application/json+oembed" href="https://[...]
<link rel="alternate" type="text/xml+oembed" href="https://www.sli [...]
[...] engineering-degree/?field1=%0<<<"gviby%20>>>"><meta name="theme-color"
content="#033769">
<meta name="viewport" content="width=device-width, initial-scale=1 [...]
----- output -----
```

+ The 'field1' parameter of the /computing/programmes/information-systems-engineering-degree/ CGI :

```

/computing/programmes/information-systems-engineering-degree/?field1=%0
<<<"gviby%20>>>
```

Fig: 3.7 : IAA_Miniproject report picture 2

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize parameters name of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

See Also

https://en.wikipedia.org/wiki/Cross-site_scripting
<http://cpecc.mitre.org/data/definitions/86.html>
<http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting>

Solution

Contact the vendor for a patch or upgrade.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE-20
XREF	CWE-74
XREF	CWE-79
XREF	CWE-80
XREF	CWE-81
XREF	CWE-83
XREF	CWE-116
XREF	CWE-442
XREF	CWE-712
XREF	CWE-722
XREF	CWE-725

Fig:3.8: IAA_Miniproject report picture 3

5. Additional website scanning

1. GT-Metrix website performance testing

This is a freely available website performance testing tool in the internet. We can test the performance such as website upload speed by using this tool.[2]

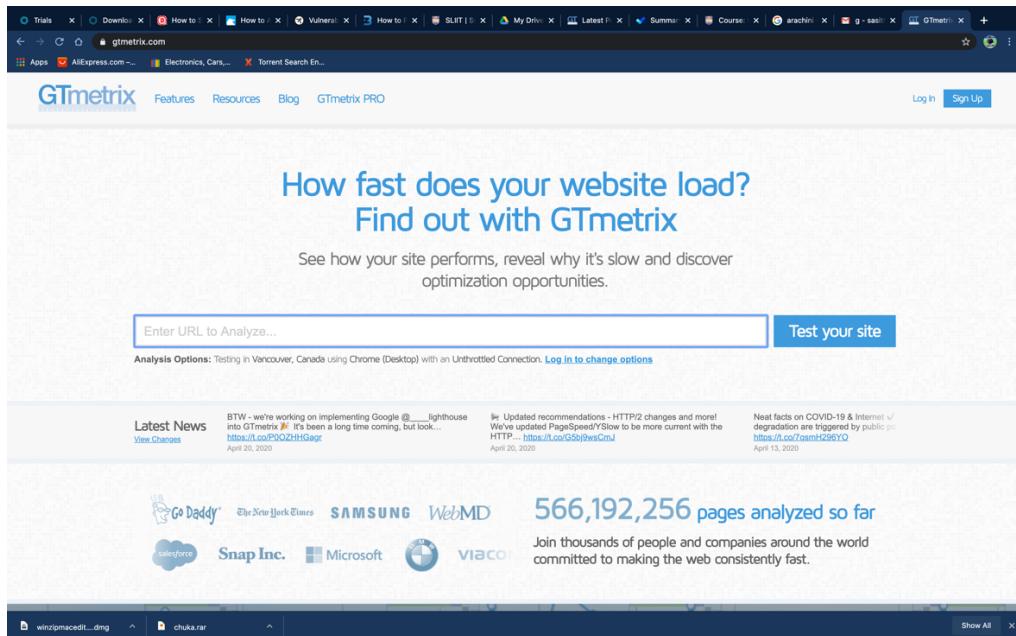


Fig 4.1 : GT-Metrix tool interface.

www.sliit.lk website's gt-metrix results

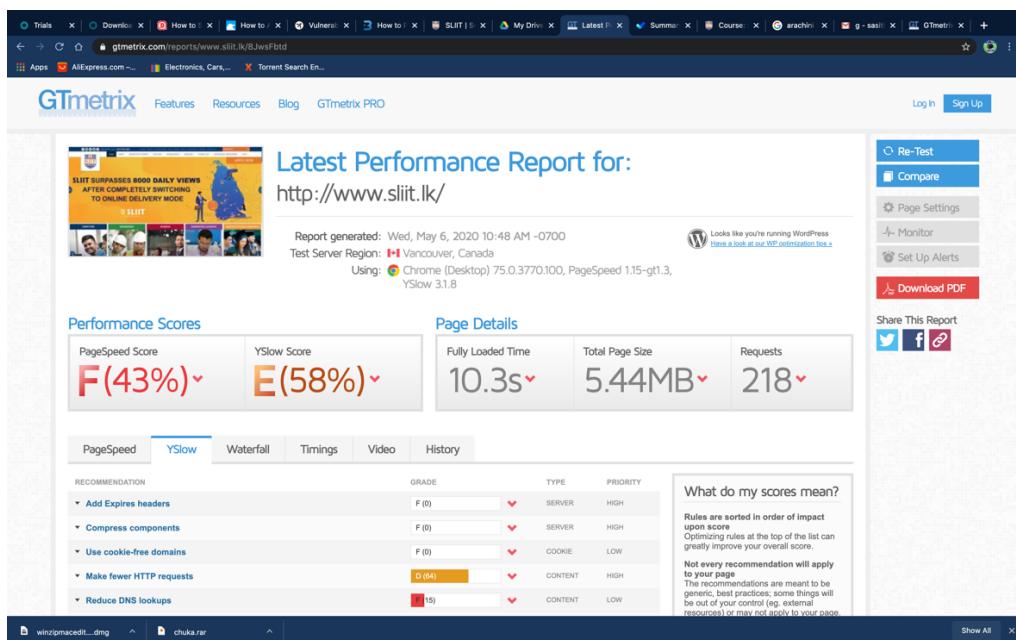


Fig: 4.2: “www.sliit.lk” GT-Metrix results.

2. SEO test using “site-checker” tool

“sitechecker” is freely available Search Engine Optimization tool.[3]

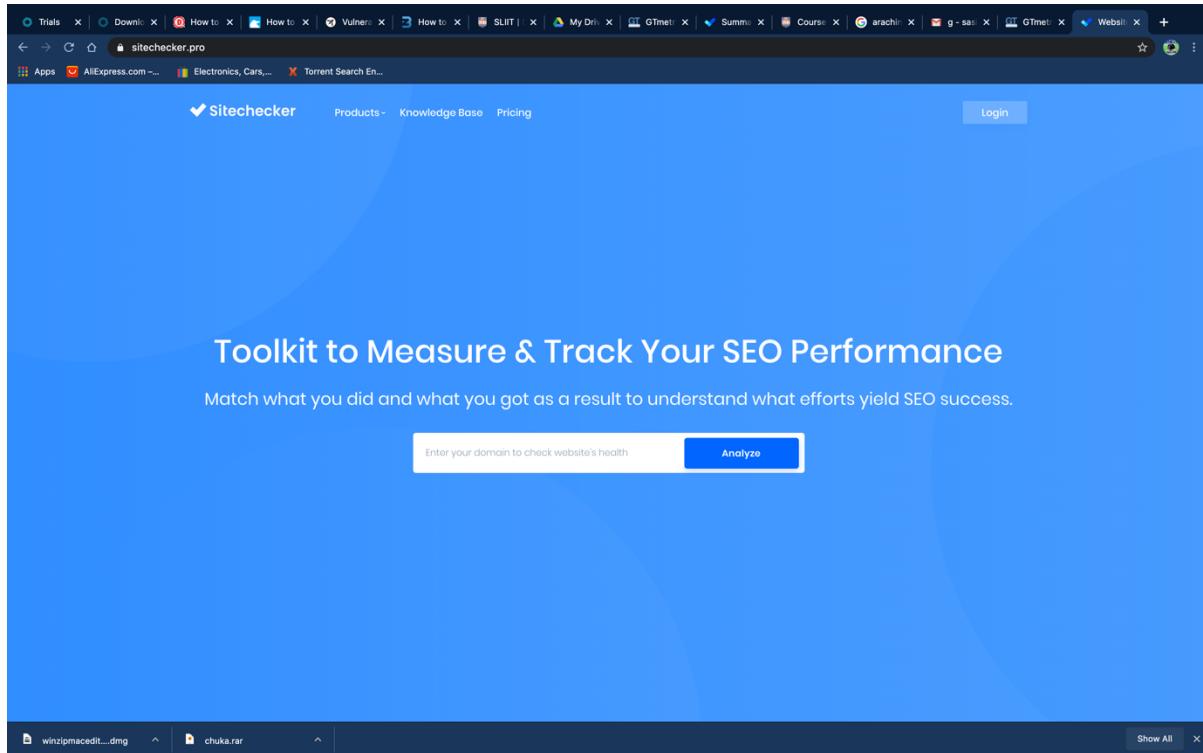


Fig: 4.3: “sitechecker” tool interface

“www.sliit.lk” sitechecker results.

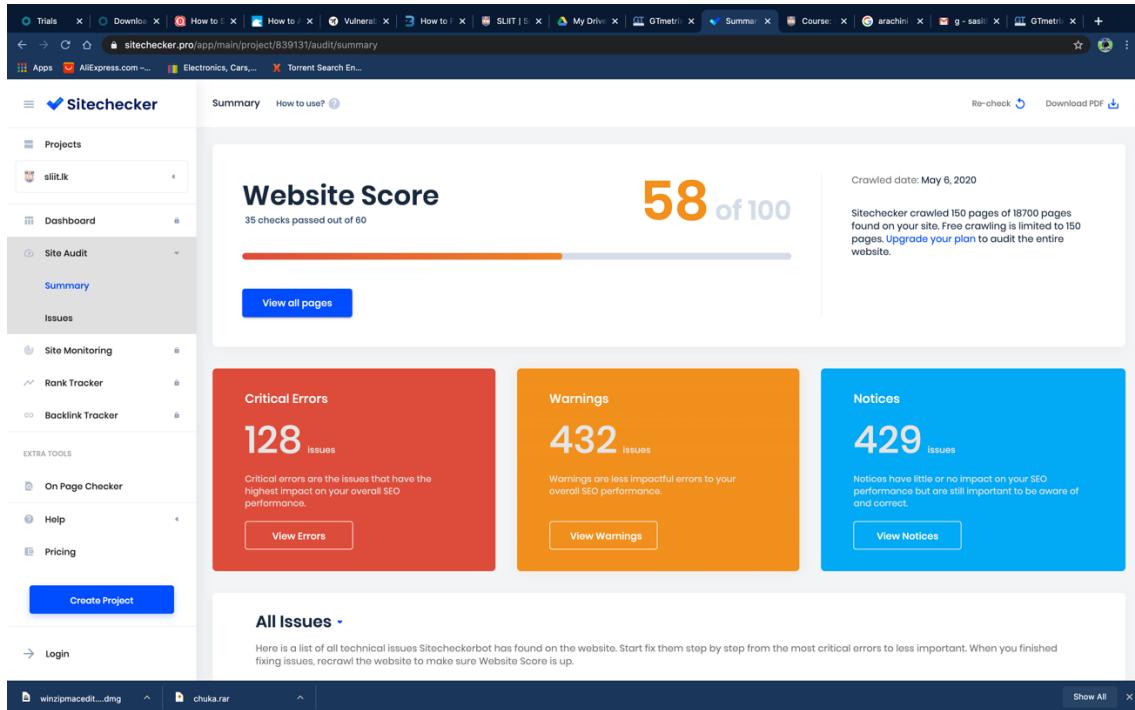


Fig: 4.5 : “sitechecker” results.

6. Conclusion and Recommendation

It is best to do regular audits on the websites in the right time. By doing audits we can identify what bare the weaknesses that are in our website and what can we do to those issues. And in this audit reports we have to go through all the problems and give solutions to them. After doing these solutions we can again scan our website and can see our solutions are worked. In the “www.sliit.lk” scan using Nessus pro tool we identified four medium problems. I recommended to give solutions for these issues and fix them before those medium size errors become critical.

7. Reference

- [1] Tenable.com. 2020. *Download Nessus Vulnerability Assessment | Tenable®*. [online] Available at: <<https://www.tenable.com/products/nessus>> [Accessed 4 May 2020].
- [2] Gtmetrix.com. 2020. *Gtmetrix | Website Speed And Performance Optimization*. [online] Available at: <<https://gtmetrix.com/>> [Accessed 5 May 2020].
- [3] Sitechecker. 2020. *Free On-Page SEO Checker – Get Your SEO Score Now*. [online] Available at: <<https://sitechecker.pro/>> [Accessed 5 May 2020].