

Information Assurance & Auditing

4th Year - 1st Semester

Mid-Term Assignment

Registration No : IT 17 3919 00

Name : W.A.U.D.Amarathunga

Batch : CSN-WE

**Introduction**

Website auditing is a prominent technique used in any business which is related with the digital marketing services. The website audit can be represented as an analysis of the all factors which affects the performance of the web site. It helps to identify the weak points of the procedure and thus it reveals the actions needed to be taken to improve search engine optimization (SEO) (1). Hence, website auditing is a very effective technique that can be used to determine the website’s visibility in search engines. Website audits can be divided into several types as site health audit, website security audit, social media presence audit, conversion rate optimization audit, negative SEO audit, competitor website audit, penalty and recovery audit and duplicate content audit (2). Among them, website security audit is one of the most important components in website auditing.

With the growing digitization of the businesses, cyber-attacks have become a major risk in the digital world. Hackers can attack at any time regardless of the size of the platform unless the platform is being secured completely (3). The main reason for facing such attacks is the poor security practices. Hence, securing the websites is very important to evade from such risks. Website security audits can be conducted to assess and secure the websites. It helps to identify the potential vulnerability issues and loopholes of the web system (4). The main purpose of the security audit is to evaluate the vulnerable areas of the web system while analyzing the security standards. A complete web security audit contains static and dynamic code analysis, business logic error testing etc (4). Thus, conducting website security audits should be a necessity in any business to ensure its security.

There are multiple tools or the scanners that can be used to conduct website security audits. Nikto, Nmap, Testssl, Nessus are some of scanners used to scan website security vulnerabilities (4). This report contains a thorough explanation about how to conduct a website security audit using Nessus professional security tool. It is one of a famous vulnerability assessment tool developed by Tenable, Inc. It uses a simple language called NASL (Nessus Attack Scripting Language) to describe potential vulnerability issues and threats (5). Nessus professional tool is rich with many features such as high-speed asset discovery, configuration auditing malware detection, sensitive data discovery, etc while setting the high standards for its speed and accuracy (6). Due to these features, Nessus professional tool is used for this website security audit. A detailed explanation about how to conduct a website security audit using Nessus professional tool is included in this report.

**Auditing a website using Nessus**

In present everyone is moving to the new technologies with the new area of technology. Website became more important to business as well as day today life. Having a website is easy for people to find certain things, read up about the companies and so on.

With the evolution of technology, society has been adapted to this modern technologies dramatically. With the use of this people’s day today life become simply. Because of heavy reliance on computers and internet, cyber-attacks, vulnerability attacks and security issues take place. Securing the information have become one of the biggest challenge in the world.

In computer security vulnerability is a weakness which can be exploited by an attacker to perform unauthorized actions within a computer system. To exploit a vulnerability an attacker must have at least one applicable tool or technique that can connect to a system weakness. Therefor there are so many vulnerability scanning tools, which is an automated technology that attempt to identify a vulnerability in the system. OpenVas, Nexpose Community, Nikto, Tripwire IP360, Wireshark, Aircrack, Nessus professional are some of the examples for vulnerability scanning tools. Within these tools Nessus is the most popular tool used in the world.

Nessus is open source network vulnerability scanner that uses the common vulnerabilities and rises an alert if it discovers any vulnerability that malicious hacker could use to gain access to any computer you have connected to network. Some of the main features of Nessus are remote and local security, up-to-date security vulnerability database, plug-ins, Scalable, Multiple services, full SSL Supports and proven maturity.

We can download the nessus in tenable site(figure 01). Download and after the installation we can use as a scanner.



Figure 01

After the installation, we can use nessus through web browser. Open the web browser and we enter “local host:8834/#/”(figure 2) to get nessus tool. we should configure this as our localhost.(figure 3)

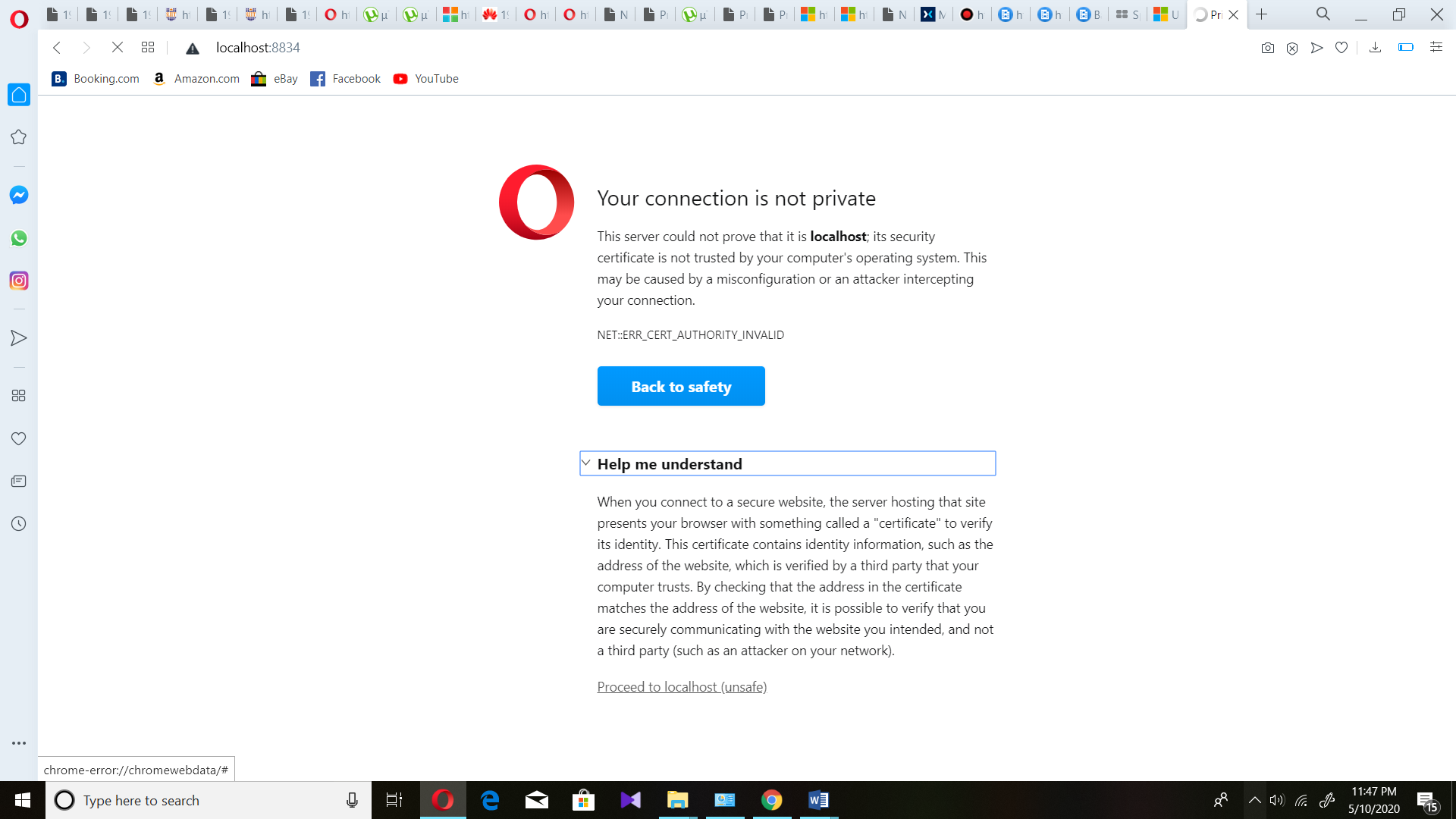
 

Figure 2 Figure 3

After the configuration we have to create a new account for nessus. Then we can log in to the nessus tool using user name and password.

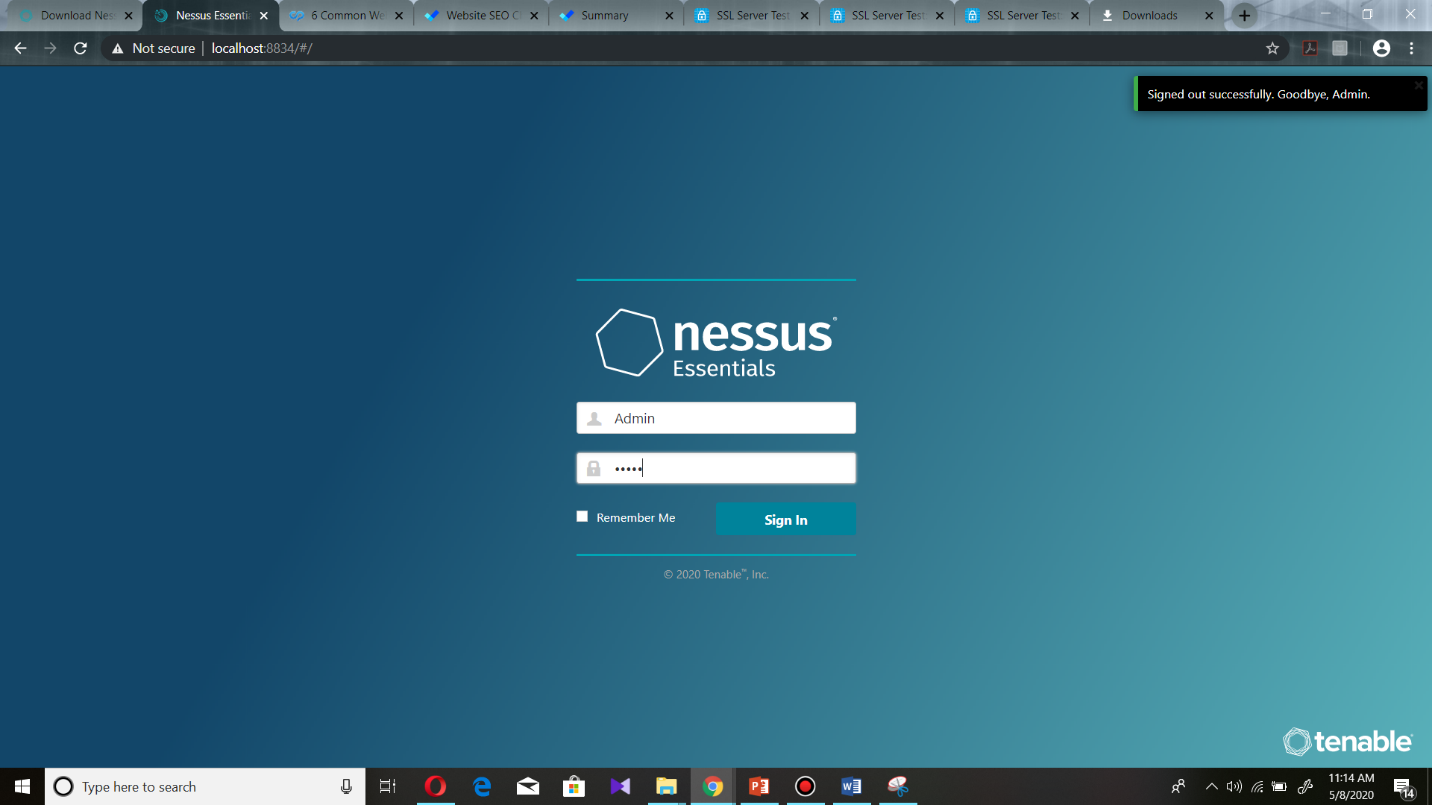


Figure 4

This is the interface which is inside the nessus. There are two tabs. Scan and Setting are them. In scan tab, here we can see few scans and also create groups properly by using folders. If we want to scan new website we should click “new scan” in top right.

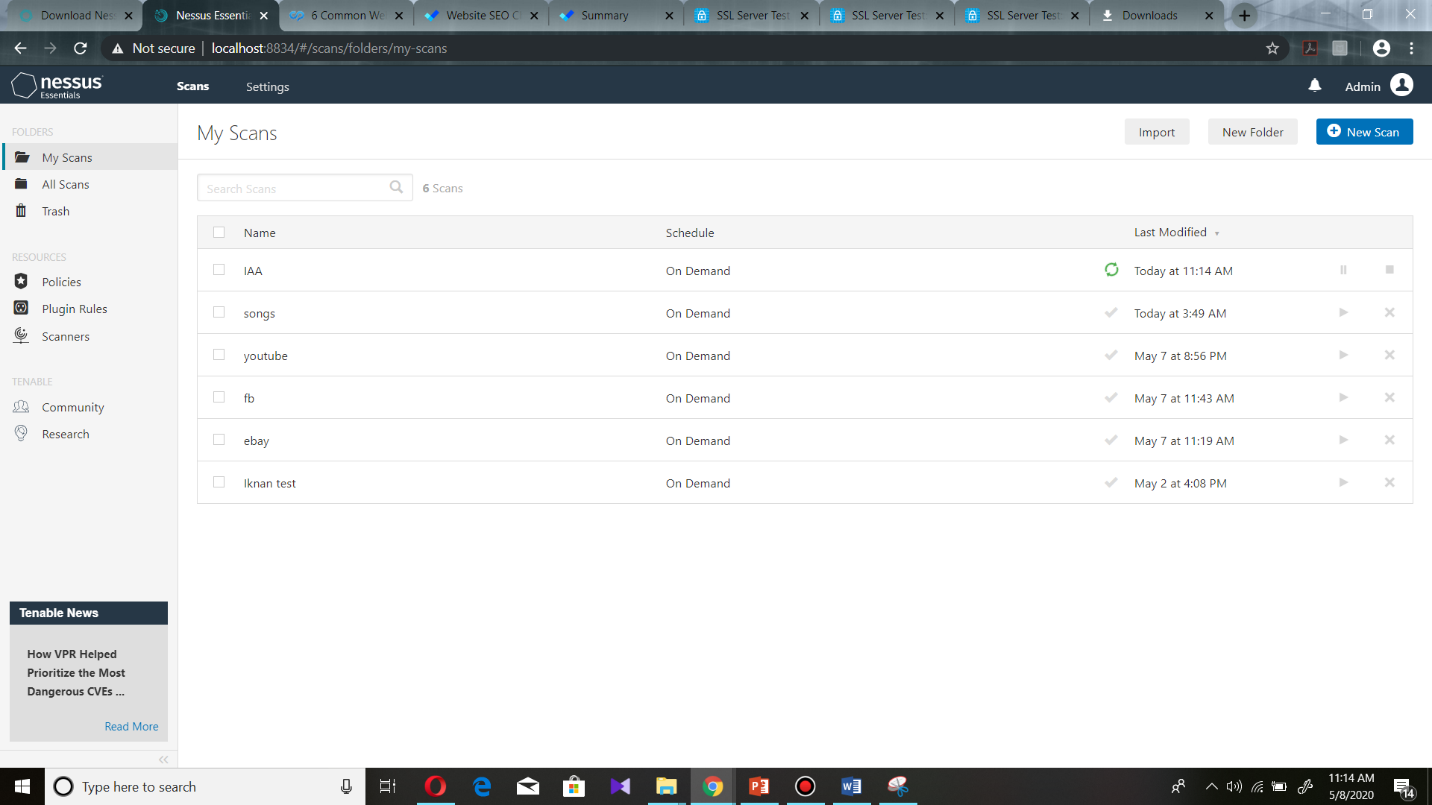


Figure 5

In setting tab, there are more sub tabs. In about tab, we can see Overview , License Utilization , Software Update and Master Password. In overview it shows version of the nessus and licensed hosts and also all details about plugins.

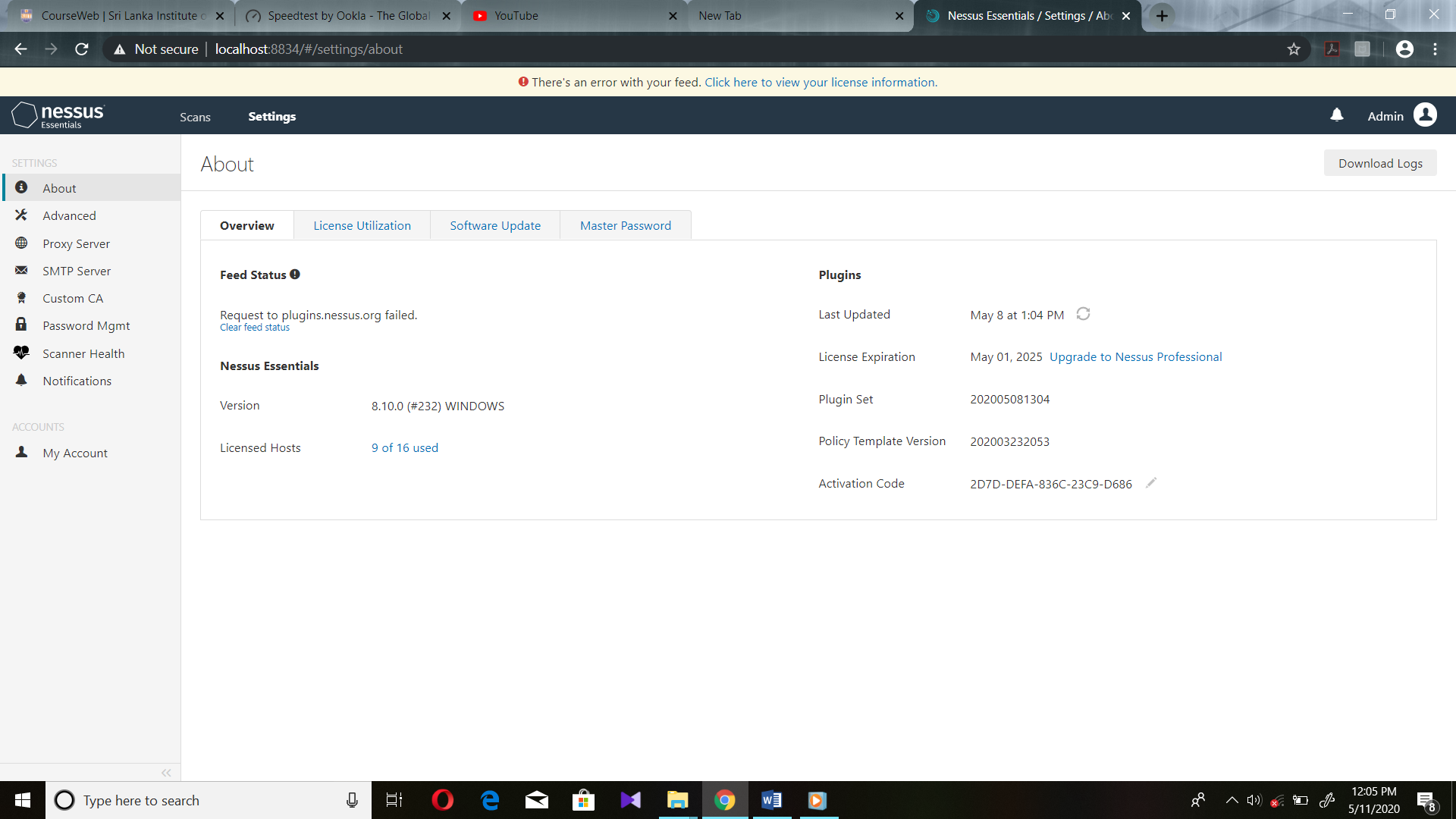


Figure 6

In license Utilization it shows what are the licensed ip addresses.

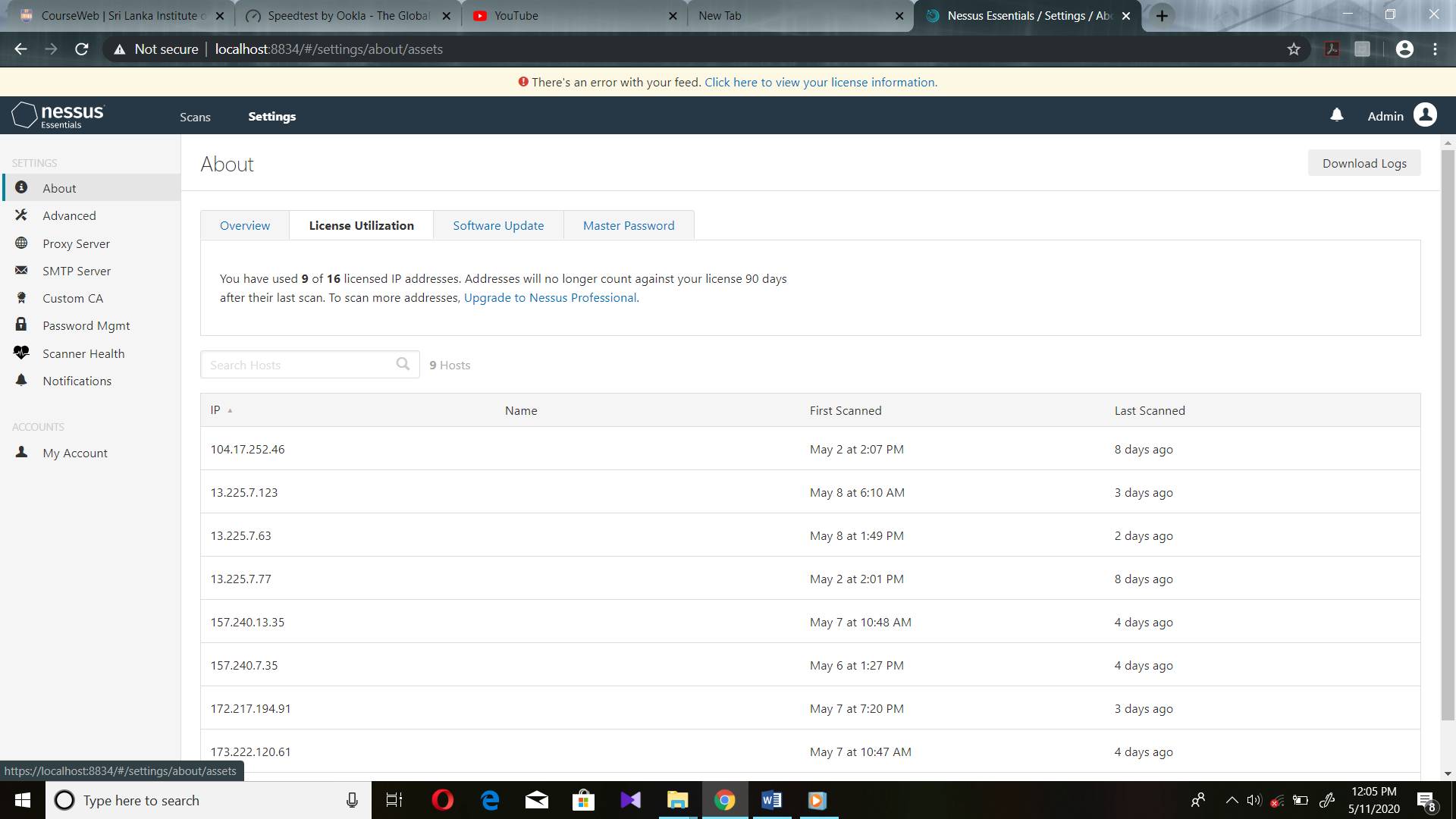


Figure 7

Here shows about software updates.

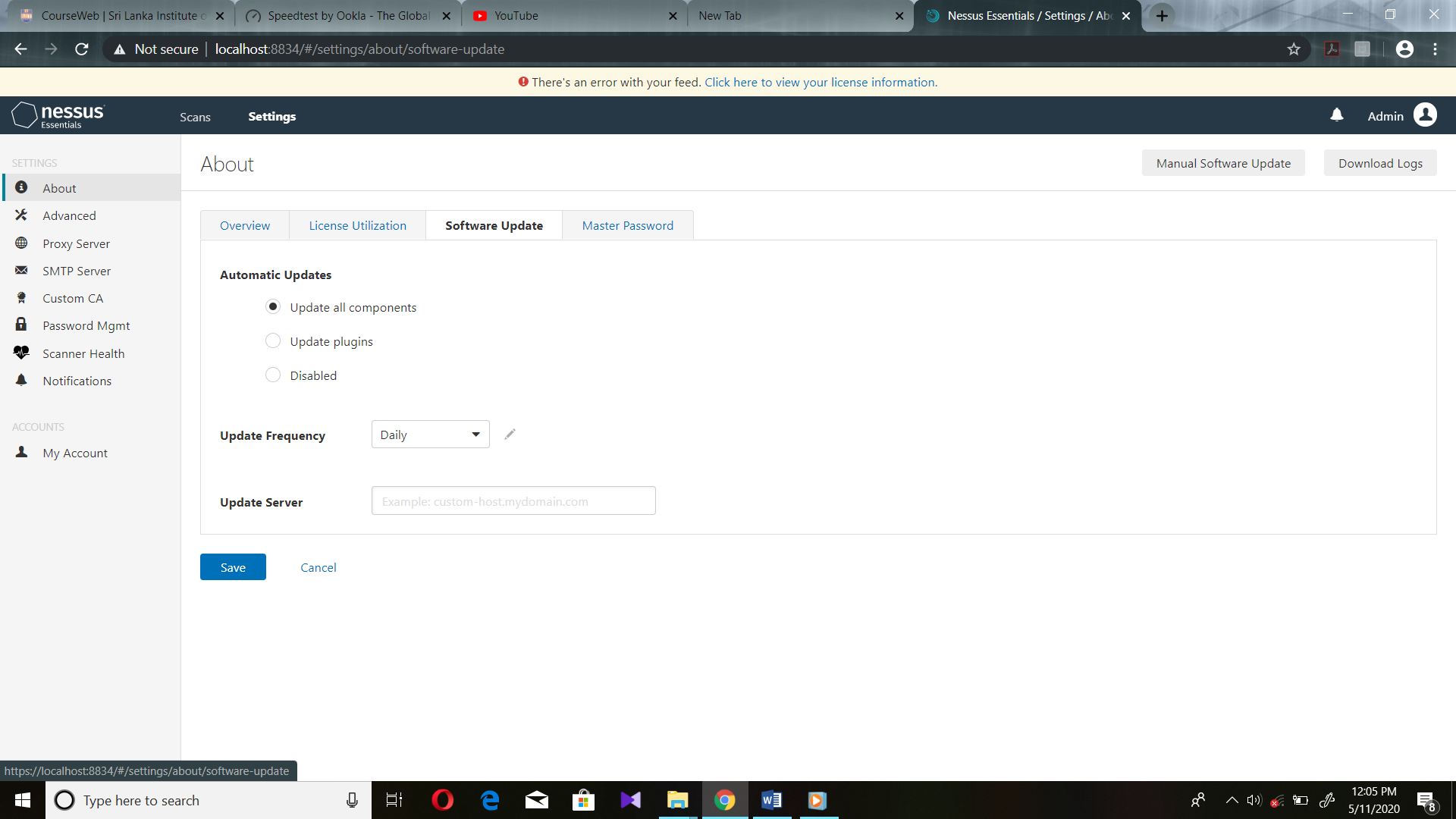


Figure 8

Here we can setting a master password to protect the encryption key for al policies and also configurations.

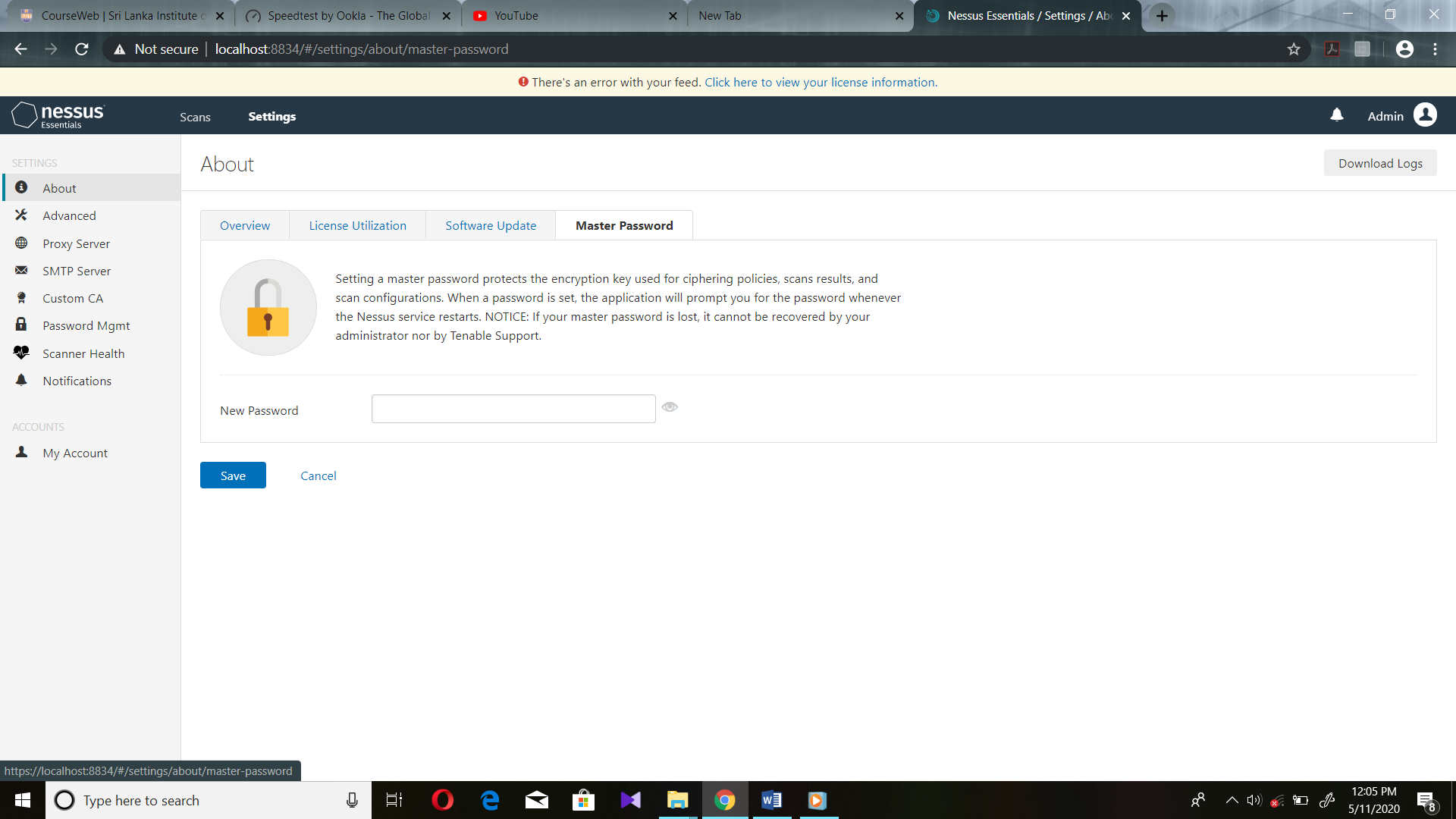


Figure 9

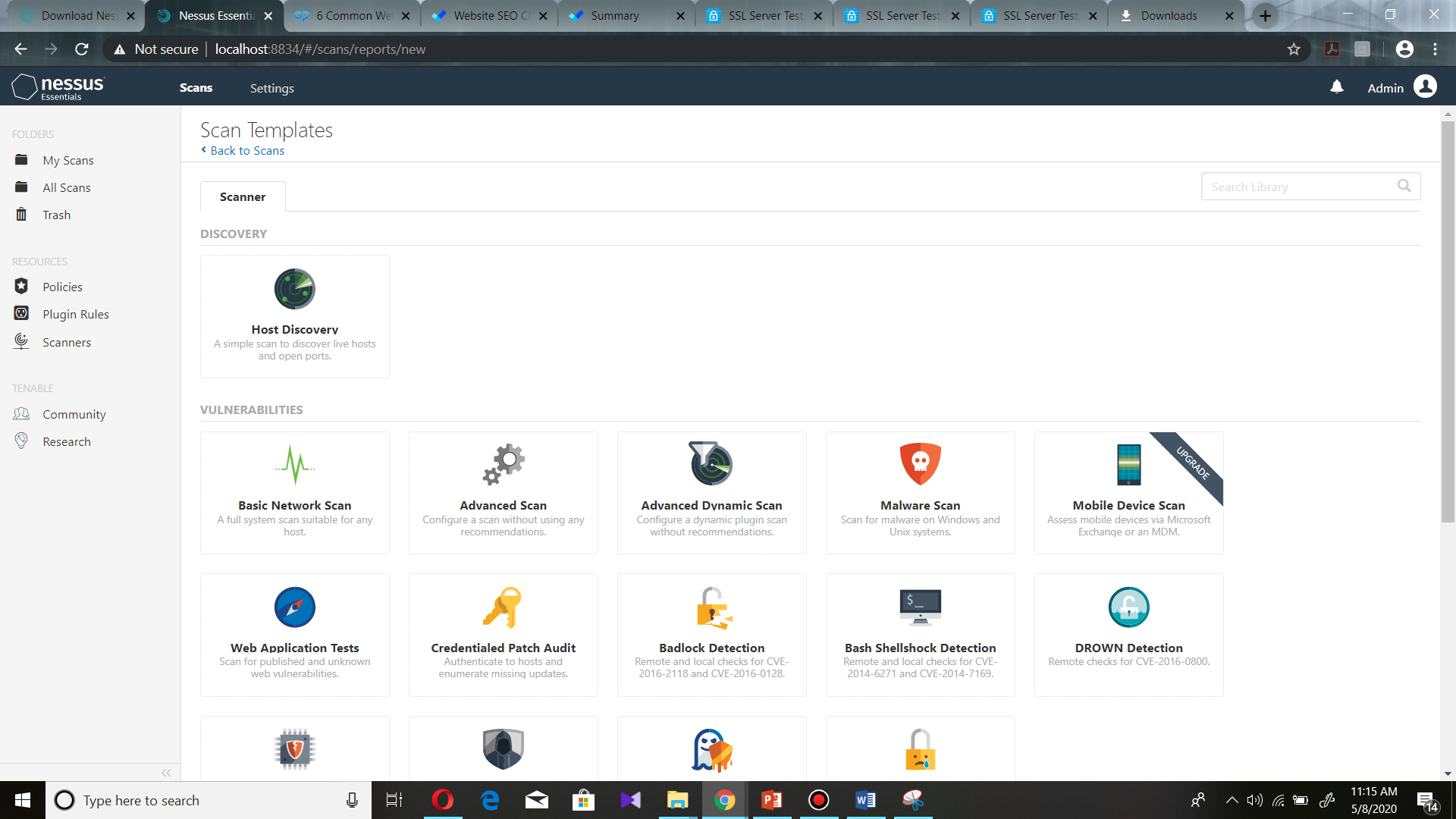
Now Let see how to scan a website to identify vulnerabilities. In Scan tab, After click the “new scan” we can see many scan templates. One discovery scan template and more vulnerability scan templates. But we want to scan a website. Therefore, we should click “Web Application Test” to continue. 

Figure 10

After select the “Web Application Tests”, we can see this interface to give inputs about website which is we want to scan. We can Schedule the scan which is at what time want to scan using Schedule tab and also we can make configurations about notifications using notification tab.

In here we can give any name to “Name”. Because it use to identify the scan only. It is not depend on scan. If we want, we can give description. It also not compulsory. We should select the folder because it is store location. After that in “Target”, we should enter the domain name which is want to scan. Then we should save and go back.

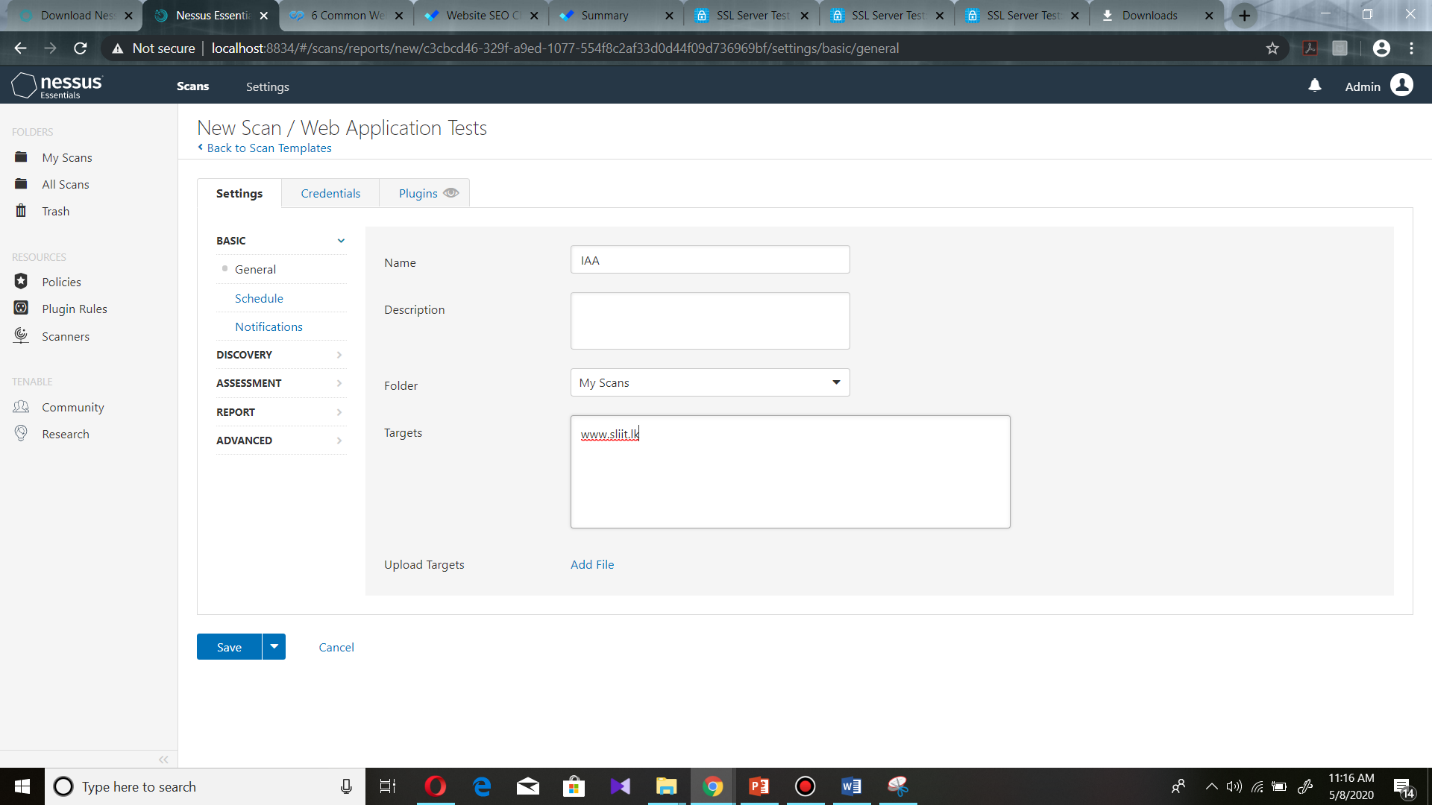


Figure 11

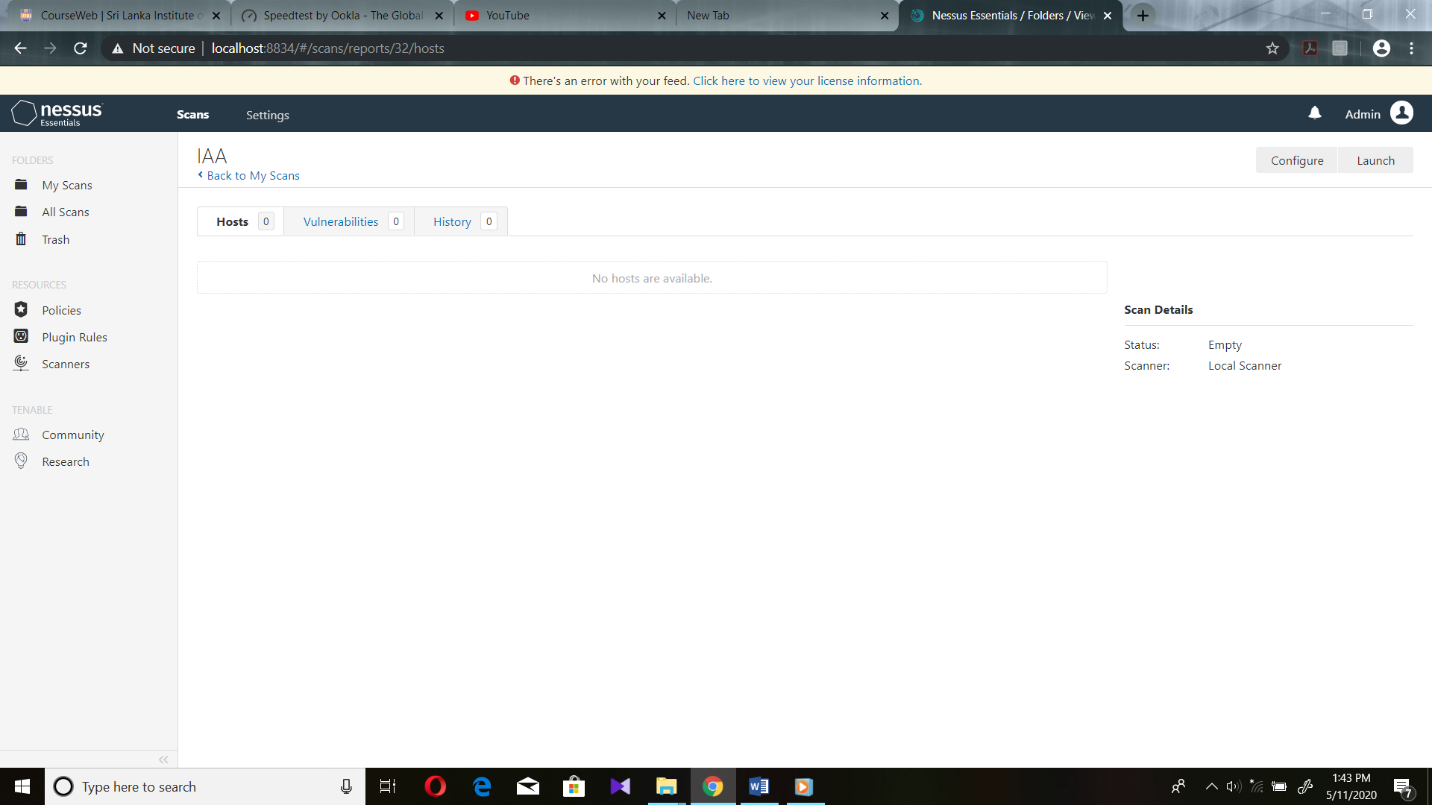
After the save if we want to do any change, we can change by clicking that scan name. Then come to this interface (figure 12). Then here we can see “Configure” on top right. We can do any changes after clicking that and after the changes it should save again. Then we have to launch. It will get more time nearly two hours. 

Figure 12

After the scan, we can get those details. It shows few colors. If it gets blue color it shows Info. If it gets green color it shows law risk. If it gets yellow color it shows medium risk. If it gets orange color it shows high risk. If it gets gray color it shows critical risk.

This scan shows how many vulnerabilities are available. If we click any vulnerability, it shows it’s description, solutions, out put and also port number. Then we can get whole details using this.

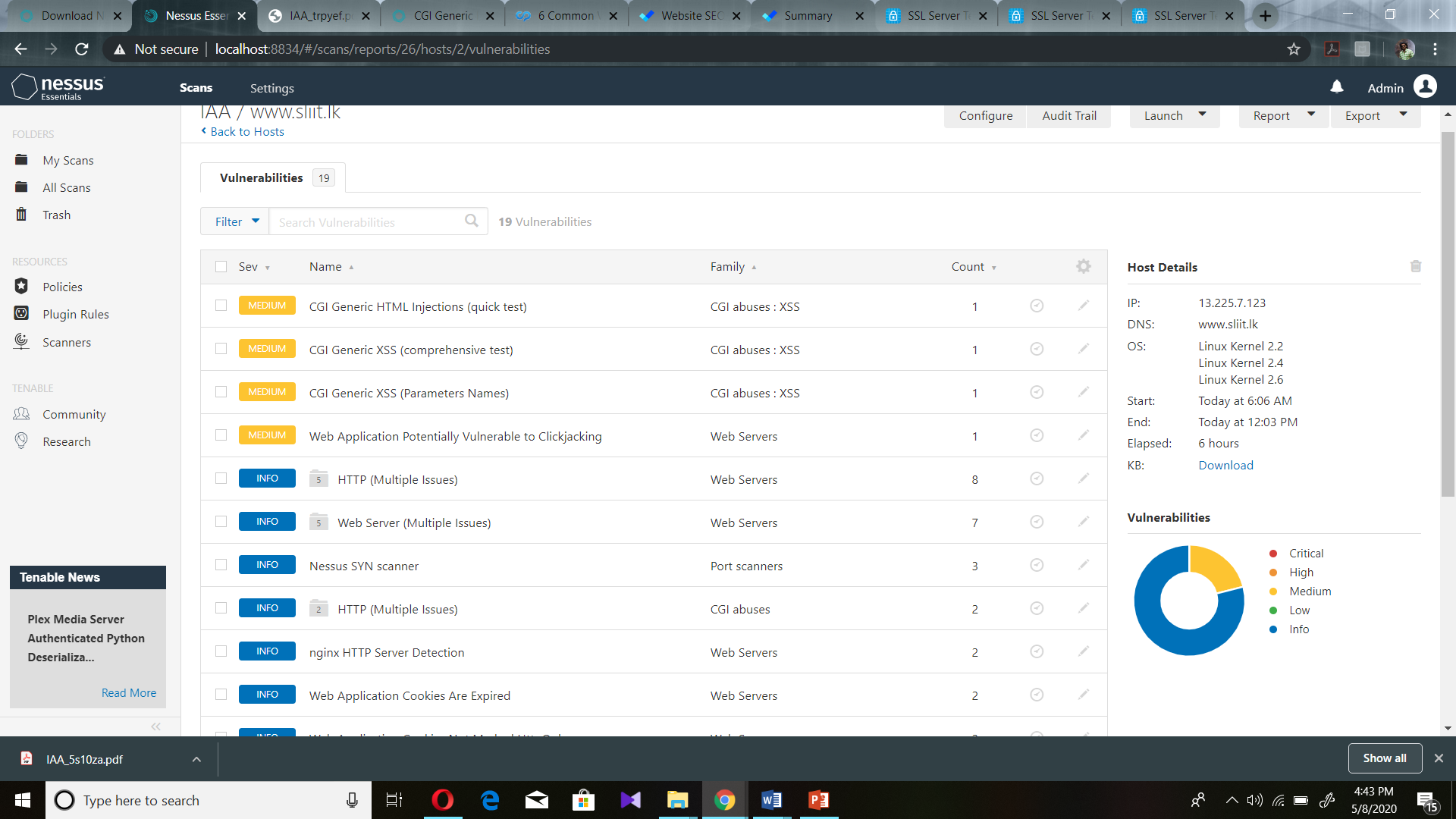


Figure 13

After the scan if we want, it provide a final report of this scan. We can get that report as a pdf , HTML or CSV. This I select pdf and after that it will download.

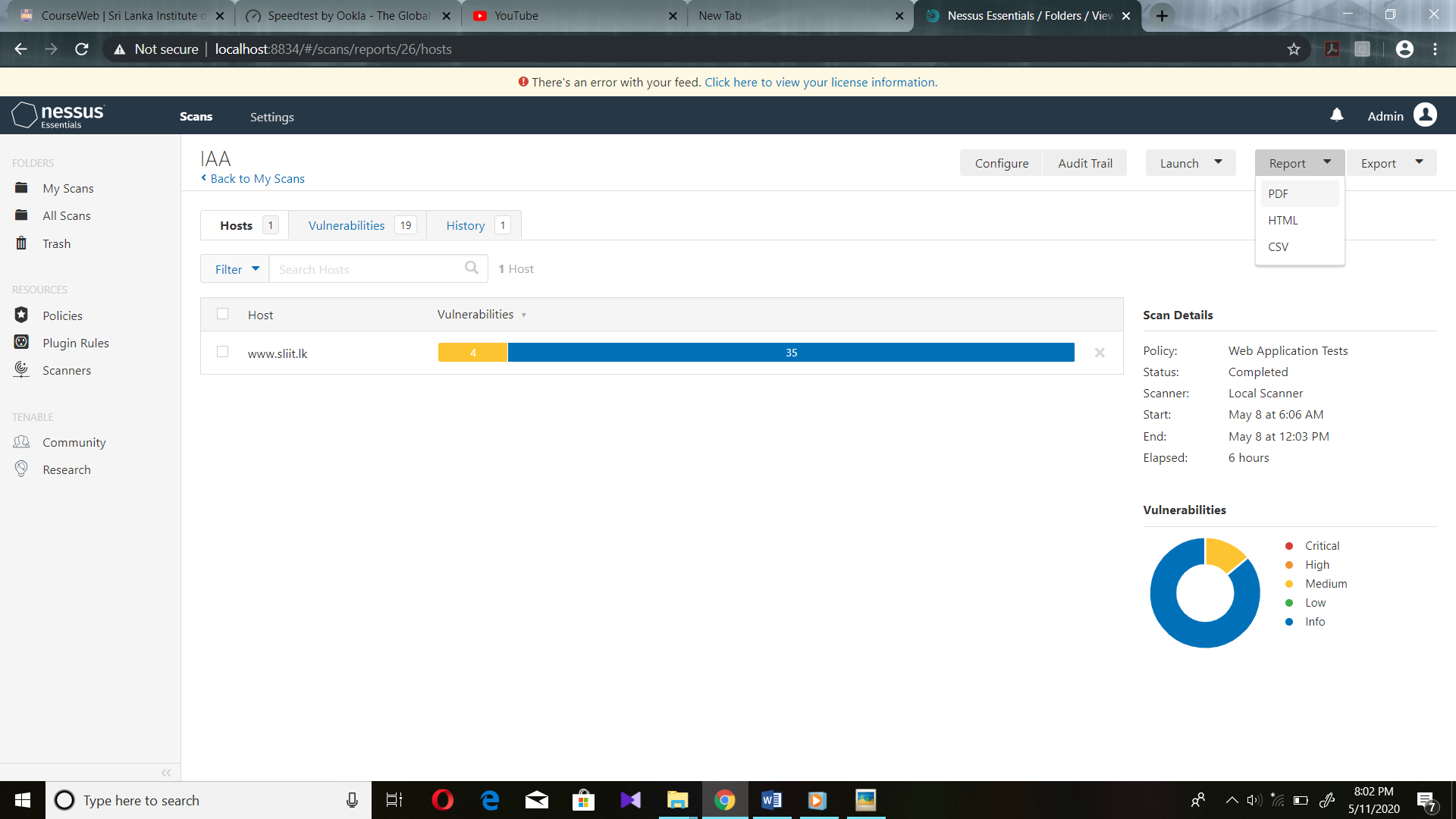


Figure 14

This is the pdf of final report. In here there are few separate plugins. If we click any plugin, tenable website provides more details about vulnerability which is related plugin.

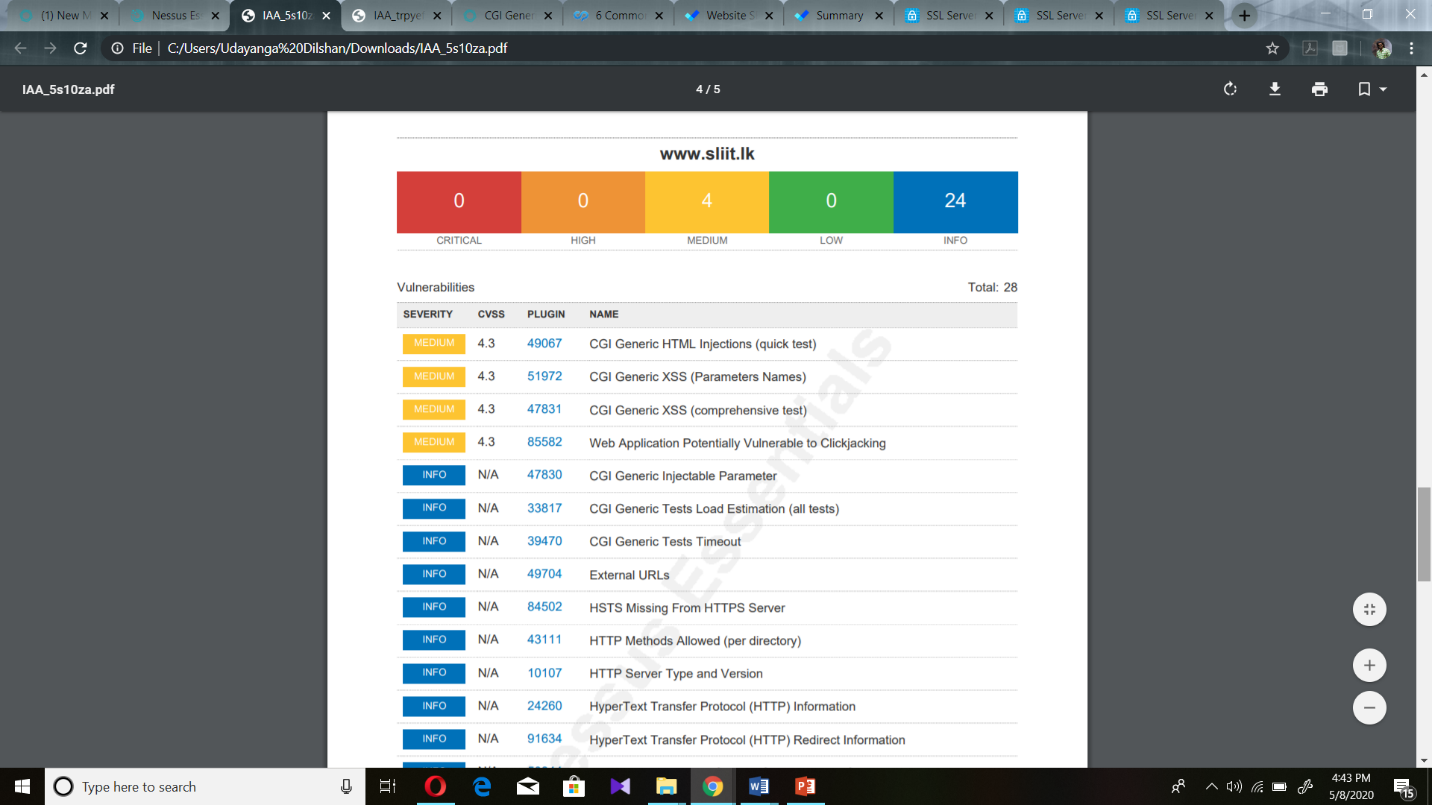


Figure 14

**References**

[1] Churt, R., 2020. *How To Audit Your Website For Improved SEO And Conversions*. [online] Blog.hubspot.com. Available at: <https://blog.hubspot.com/marketing/website-audit> [Accessed 10 May 2020].

[2] Pedestal. 2020. *What Is A Website Audit And Why Is It Necessary In 2019?*. [online] Available at: <https://pedestalsearch.com/what-is-website-audit-why-necessary/> [Accessed 10 May 2020].

[3] Customers, S., Community, C., Loyalty, B., Strategies, A., Operations, A., Online, D., Remote, W., Healthy, S., Services, C., Services, F., Wellness, H., Organizations, N., Services, P., Estate, R., Services, T., Developers, W., Business, S., Ideas, U., Startups, O., Business, N., Investing, D., Estate, S., Restaurant, S., Business, S., Website, C., Blog, S., Brand, B., Security, I., Tools, W., Security, W., Marketing, E., Business, S., Marketing, S., Business, F., 365, U., Auctions, D., Investing, D., Office, M., Email, P., Bookkeeping, O., Hosting, W., Hosting, B., Hosting, W., Social, G., Marketing, E., Listings, L., Pro, G., Program, R., Hosting, R., Certificates, S., Security, W., Removal, E., Backup, W., Marketing, W., Ecommerce, W., Websites, W. and Design, W., 2020. *How To Do Your Own Website Security Audit*. [online] GoDaddy Blog. Available at: <https://www.godaddy.com/garage/how-to-do-your-own-website-security-audit/> [Accessed 10 May 2020].

[4] Astra Security Blog. 2020. *Website Security Audit: Your Topmost Concern*. [online] Available at: <https://www.getastra.com/blog/security-audit/website-security-audit/> [Accessed 10 May 2020].

[5] SearchNetworking. 2020. *What Is Nessus? - Definition From Whatis.Com*. [online] Available at: <https://searchnetworking.techtarget.com/definition/Nessus> [Accessed 10 May 2020].

[6] Community.tenable.com. 2020. *Tenable Community*. [online] Available at: <https://community.tenable.com/s/article/About-Nessus-Professional> [Accessed 10 May 2020].

[7] Tenable®. 2020. *Nessus Product Family*. [online] Available at: <https://www.tenable.com/products/nessus> [Accessed 10 May 2020].