Information Assurance & Auditing

4nd Year - 1st Semester

Assignment

Registration No: IT 17 00 7634

Name: G.U.H Perera

Batch: CSN-WE

Abstract

IT audit is a “process of collecting, observing and evaluation of company or organization’s IT infrastructure.” Today’s technological world, it is possible to flatten any kind of organization by a click of a button. Information technology gives excellent advantages but also create immense risks. One of the primary way to ensure the data and maintain these risks is information technology audits.

Therefore any organization or company which use information system should follow an audit process.

CONTENT

What is Website auditing

Today's business world websites are the most trending platform. A website audit is an act of analyzing and providing a detailed report of everything related to the website's speed, level of search visibility, security and quality. It gives a complete picture of the site's performance and health. Website audit determines whether it is optimized in SET (Search Engine Traffic), has any security issues, loading delay and user-friendly state.

Steps to perform a website audit

This audit will cover security, performance and search engine optimization. To perform a website audit, we need following,

- Create a task list
- Audit tool to perform the security audit
- Detailed report

Burp Suite is a great tool that can perform automated and manual scans for websites. In the burp suite, there are two main scan types. One is the active scanning, and the other one is passive scanning. Passive scanning just going through the application or site intercepting and observing the traffic. Based on that, Burp will identify issues and vulnerabilities.

Perform a passive security audit using Burp Suite

In passive scan, you have the ability to select a temporary project, new project or existing project. After you select or create a new project, you can select the configuration that you would like to load this project and save it in a folder.

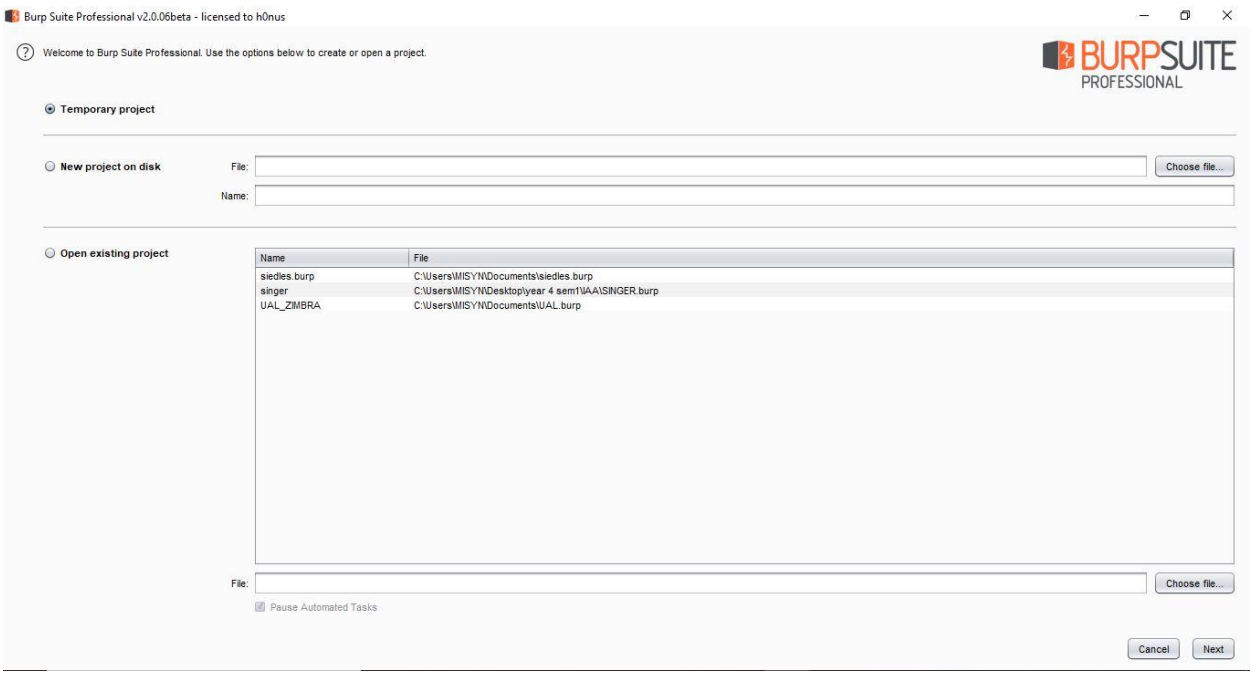


Figure 1

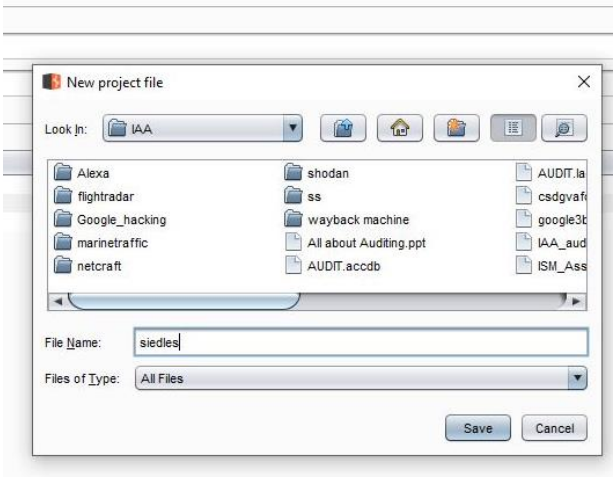


Figure 2

Now click on “New scan” button to perform a new site audit.

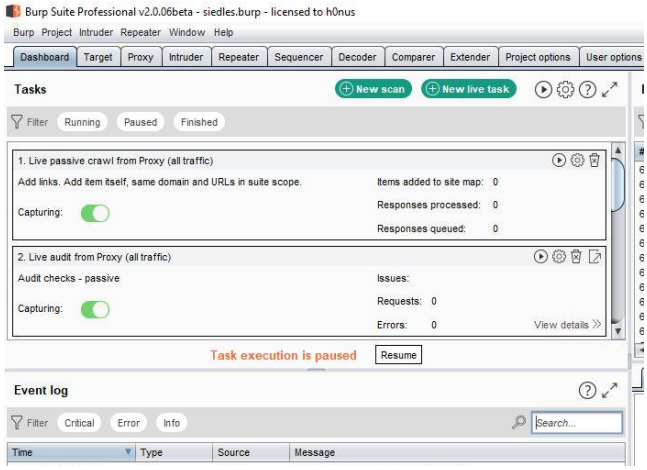


Figure 3

Then there are two main scan types to perform. Select the crawl and audit option in this section and define the URL that you want to scan, as shown in figure 4. Burp will begin crawling from these URLs, and by default will include everything beneath the specified URLs’ folders.

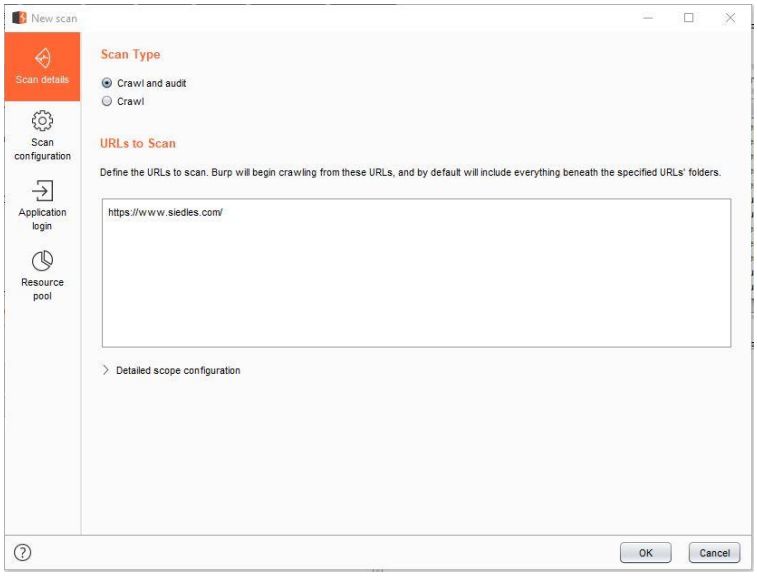


Figure 4

In this option, can select configurations to control how the scan carried out. You can select multiple configurations or preconfigure items from “Select from library” tab.

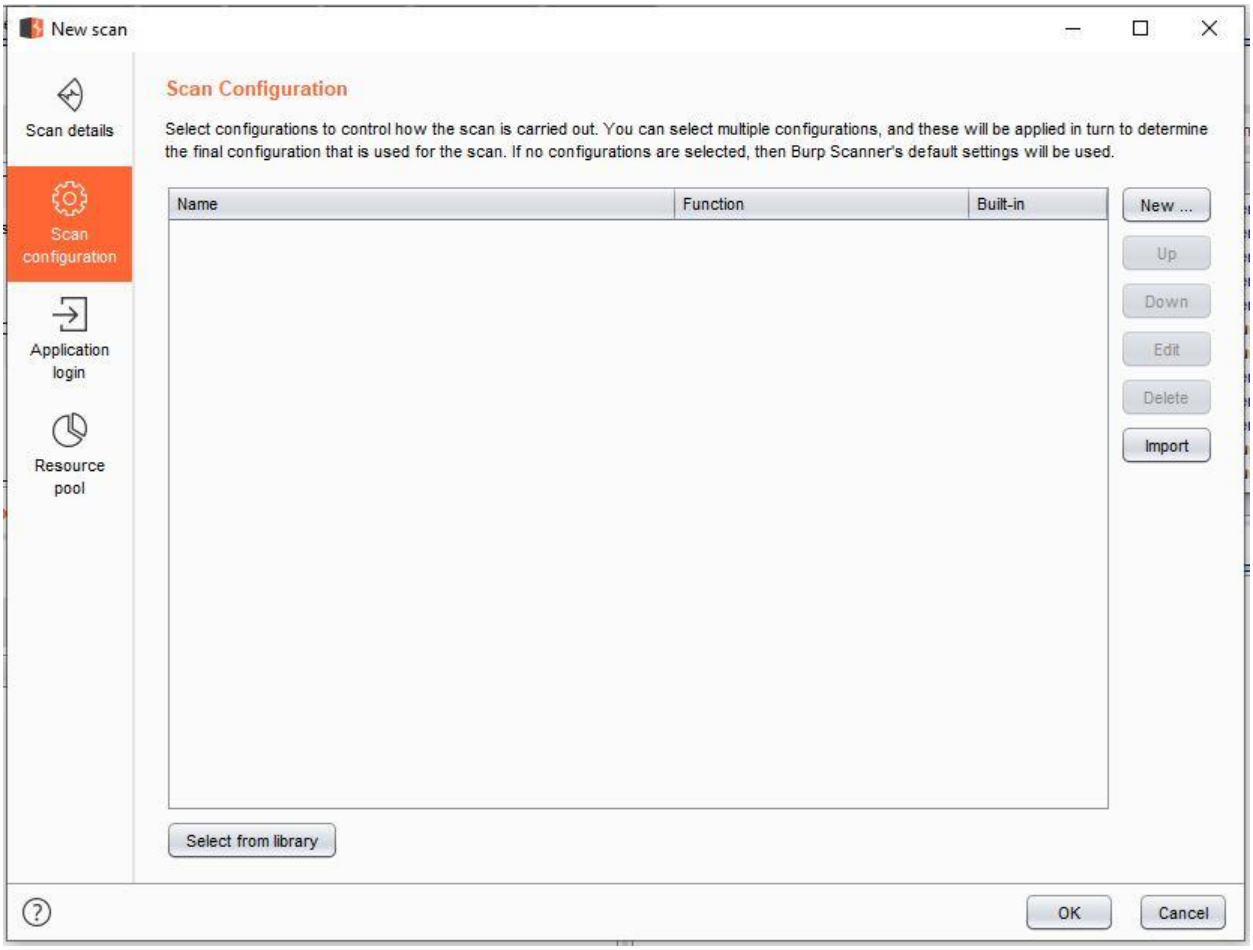


Figure 5

To create a new scanning configuration, click on the “New” tab. In this section can control the behaviour of the audit logic to reflect the audit and the nature of the target application. Then check only passive scan type in “Issues Reported” section.

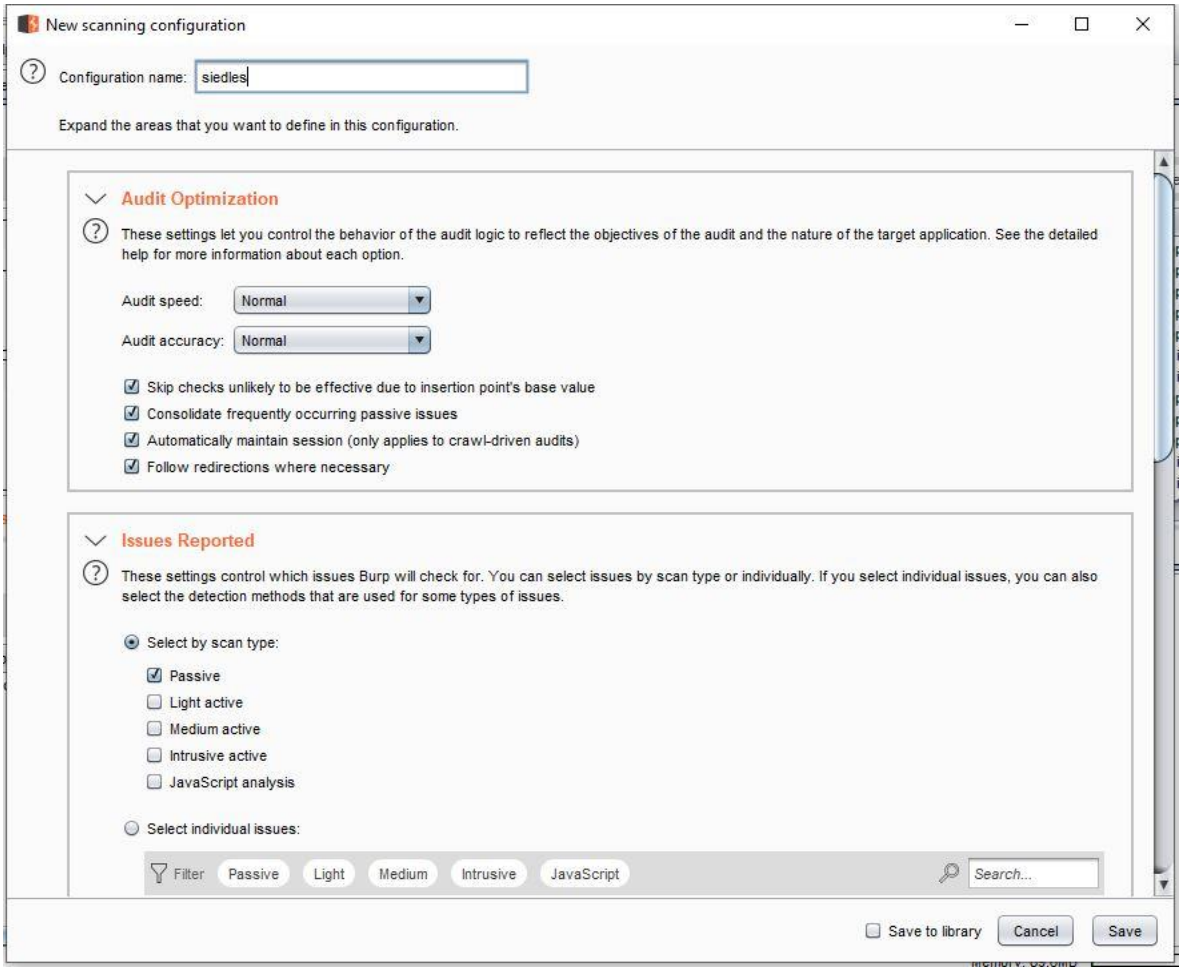


Figure 6

If have any login function in the site, can specify the account credentials and Burp crawler will use these to discover authenticated content behind login functions.

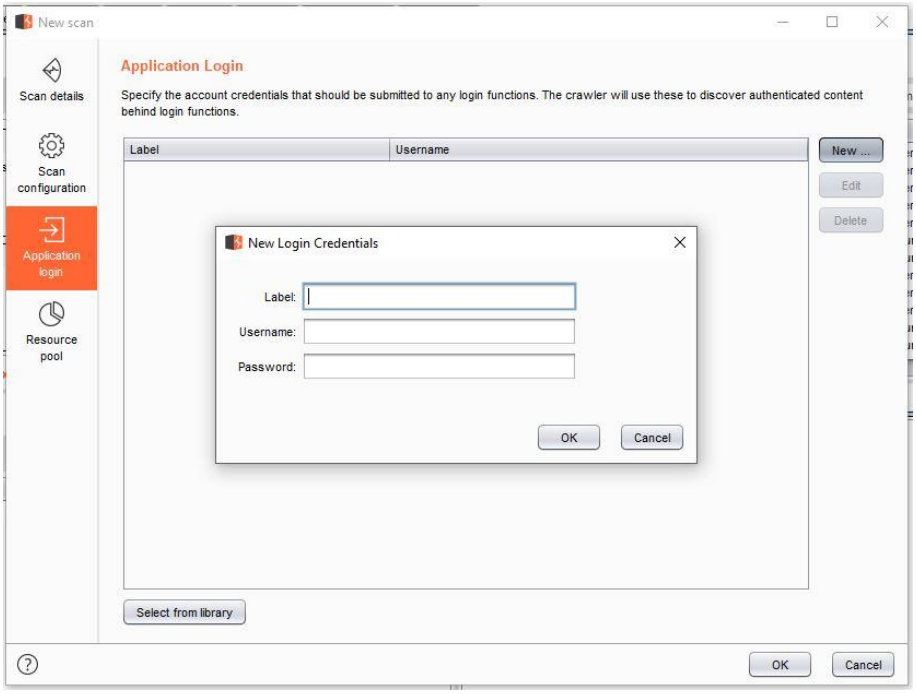


Figure 7

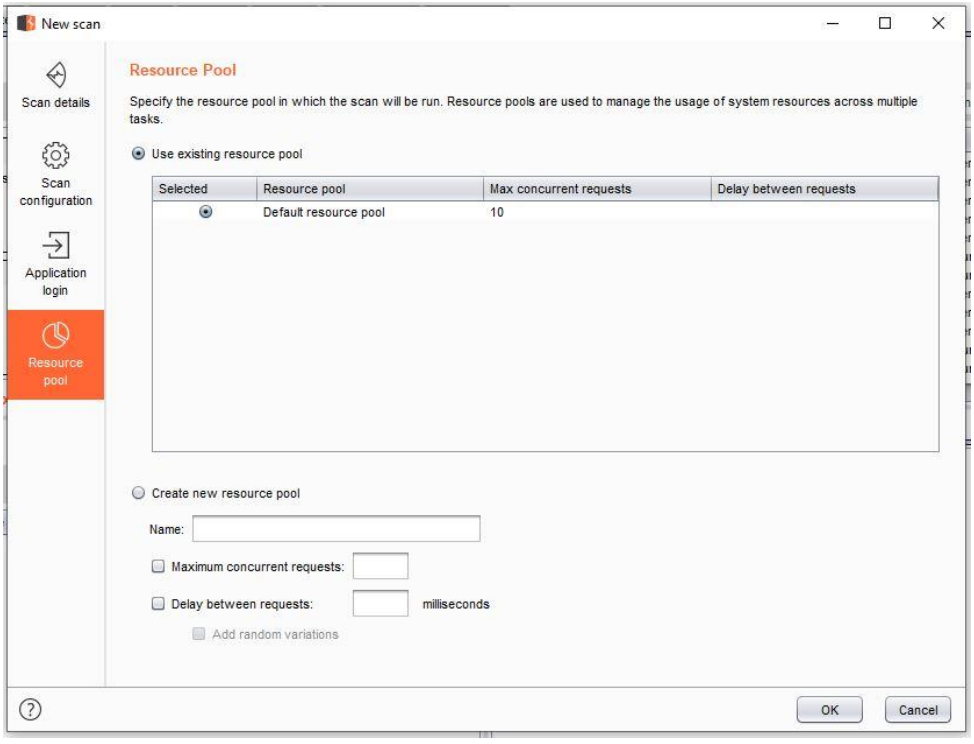


Figure 8

After click on “OK” button, you will have a new running process in Burp Suite Dashboard.

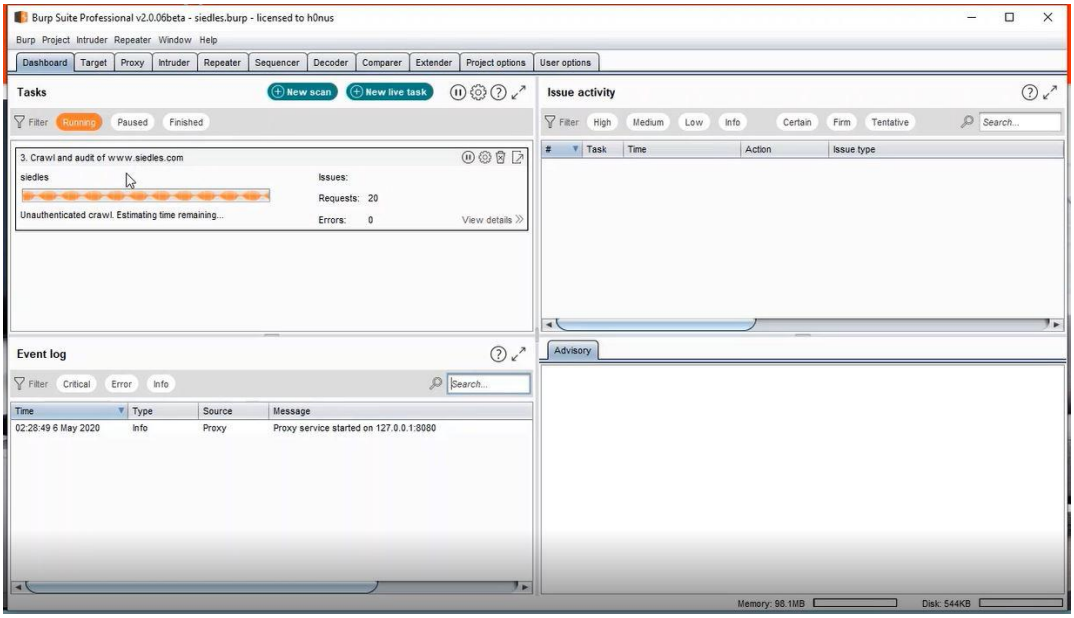


Figure 9

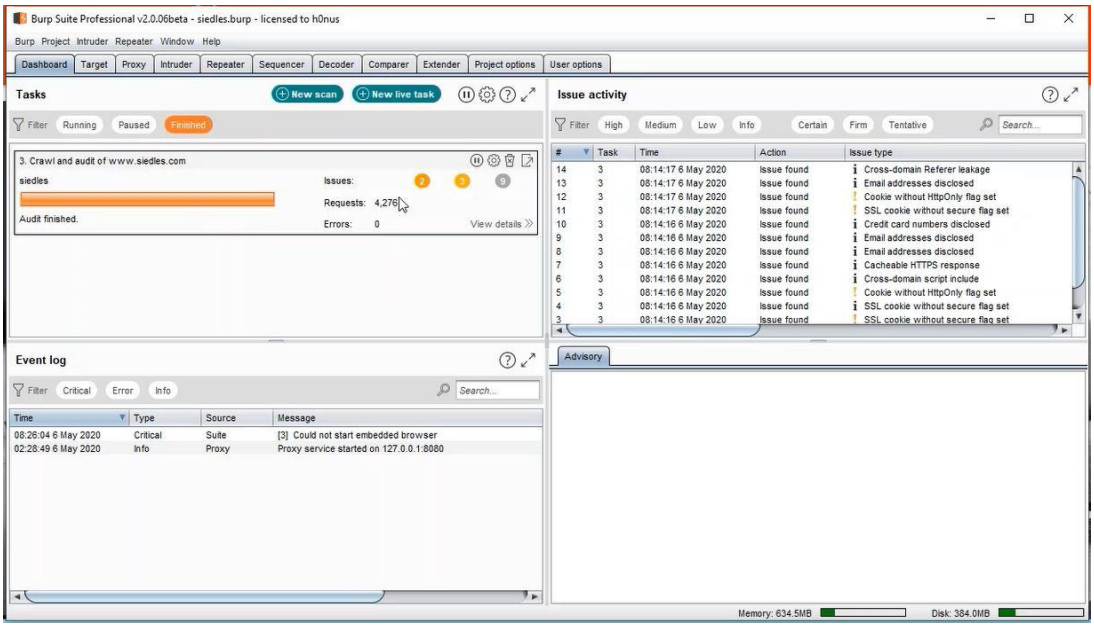


Figure 10

Perform an active security audit using Burp Suite

In order to perform an active scan, go to the target tab in Burp Suite window and right-click on URL that you want to scan. Then select scan > open scan launcher.

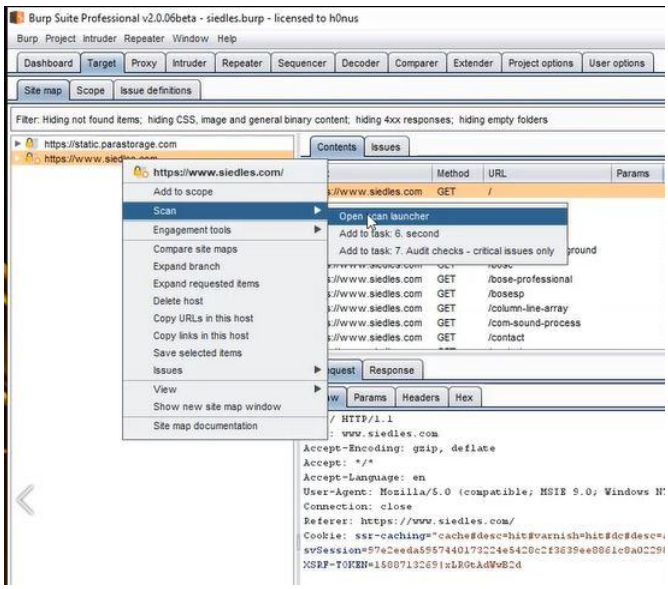


Figure 11

In this option, select audit selected item “check the create a new task.” And hit on “OK”

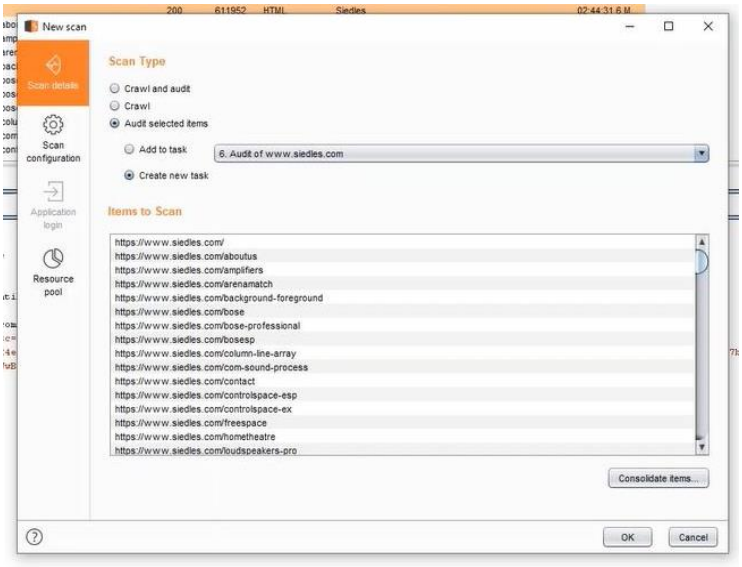


Figure 12

Then provide new scanning configuration with all the active scan types without “intrusive active” and “JavaScript analysis”. If you select intrusive active and JavaScript analysis option as well, it will take much more time but will provide a highly accurate and detailed report. And also you can run a scan just for audit specific individual errors using “Select individual analysis.” option

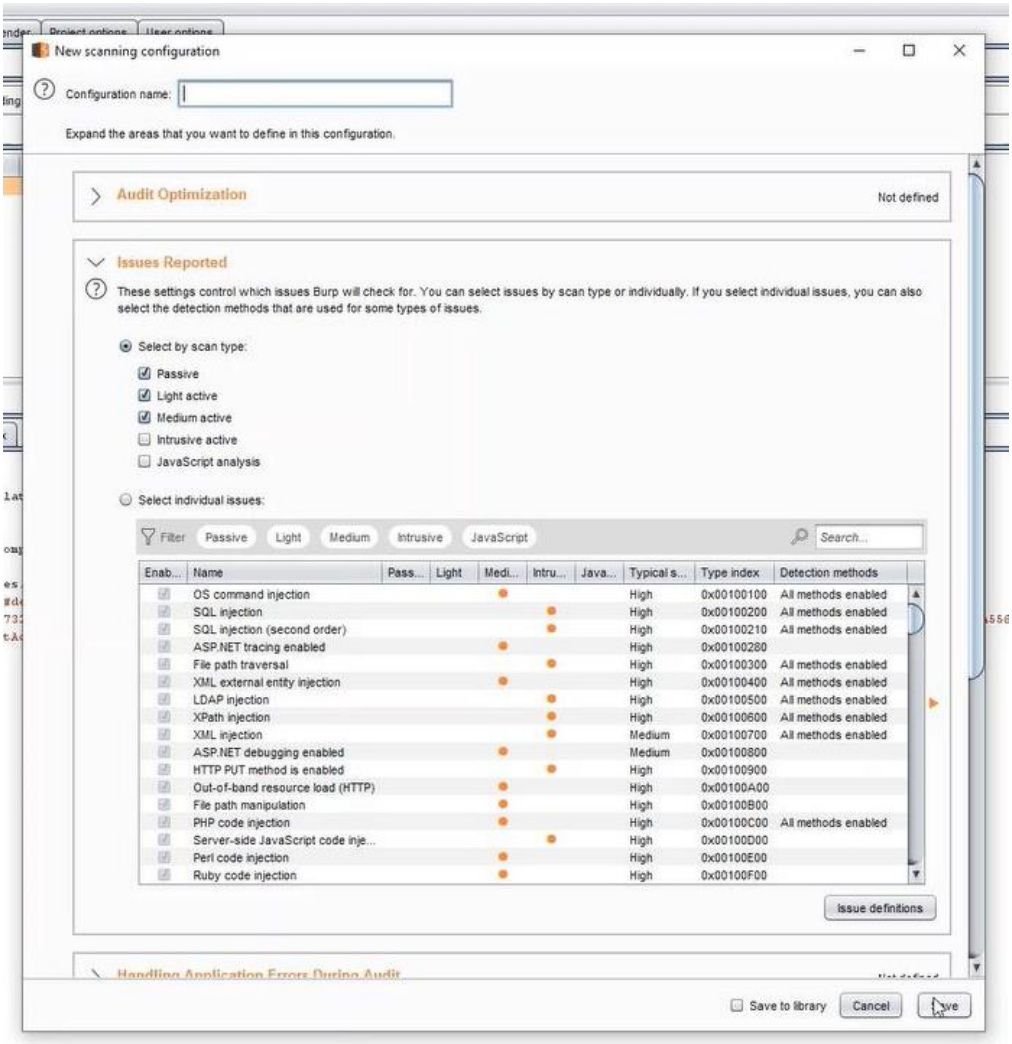


Figure 13

Clicking on “Issue definitions” tab which is under the target tab will provide the list of definitions of all issues that can be detected by Burp Scanner.

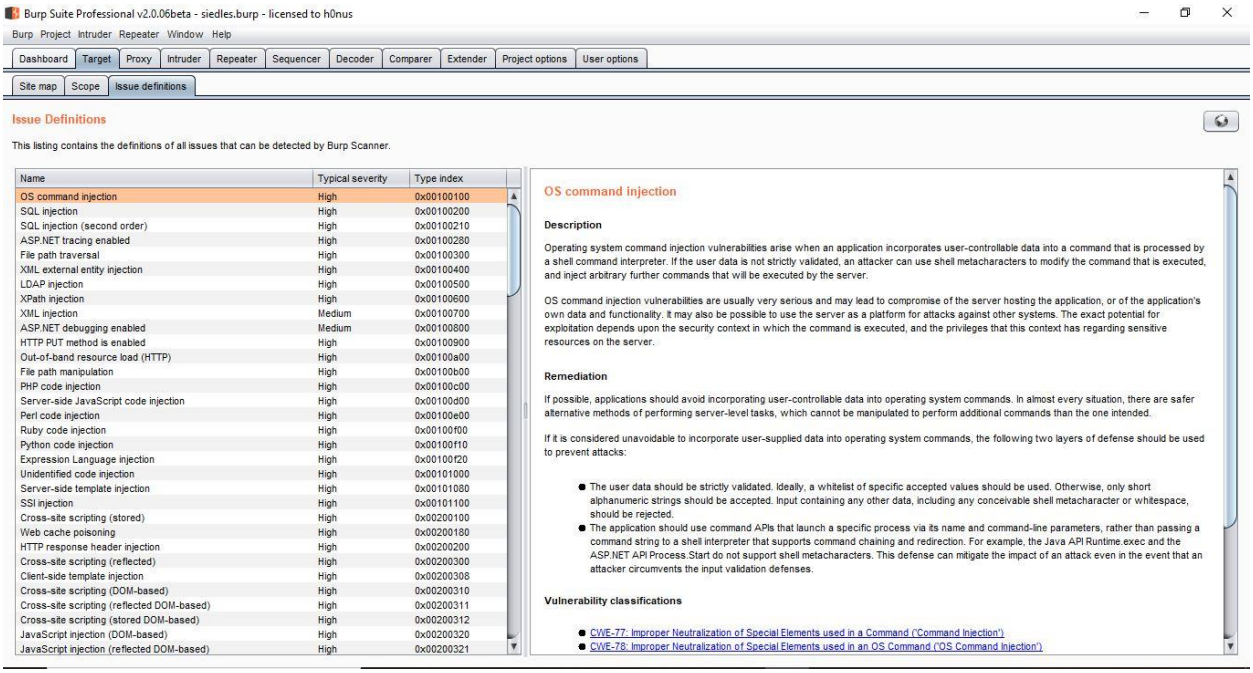


Figure 15

In Burp Suite, we can export a detailed report. In order to do that right-click on the URL under target tab and select “Report issues for this host” option.

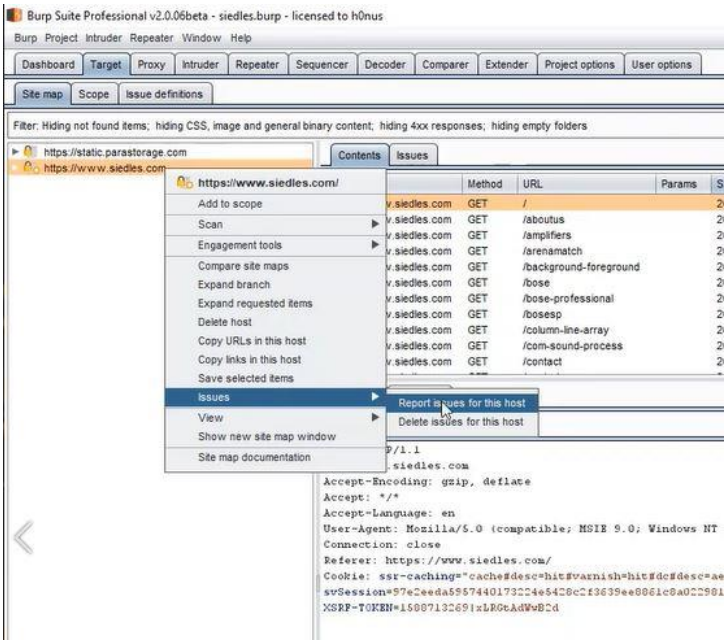


Figure 16

Then choose the format for the report.

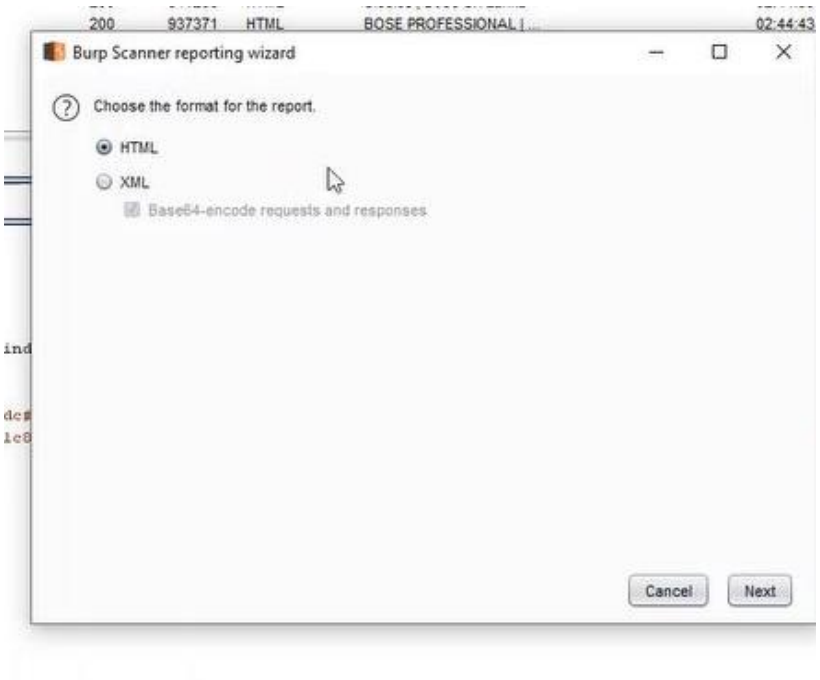


Figure 17

Select the types of details and the type of issues to include the report.

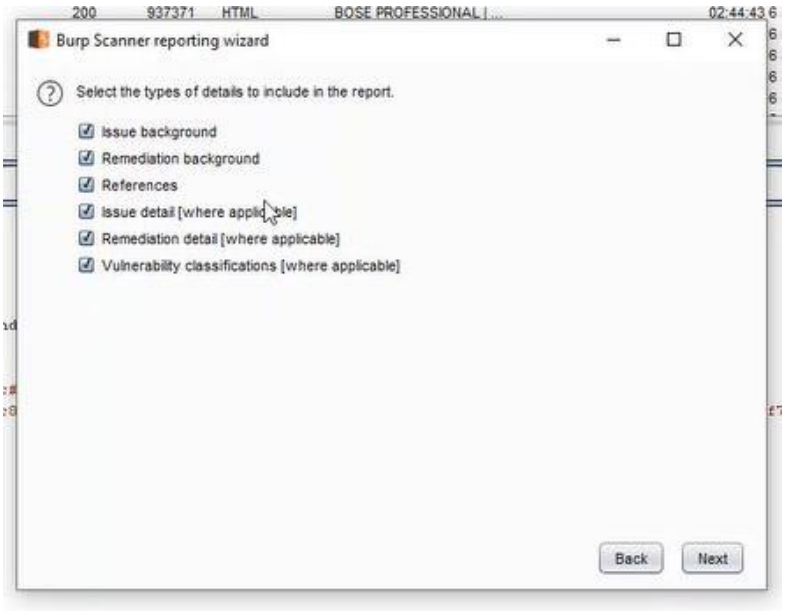


Figure18

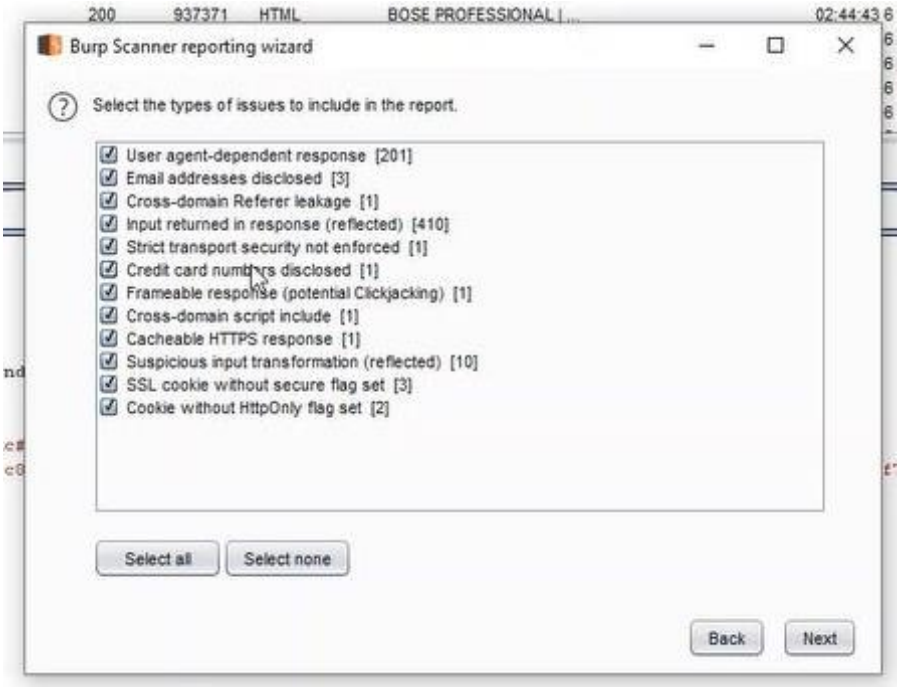


Figure 19

Provide file location to save the report and report title.

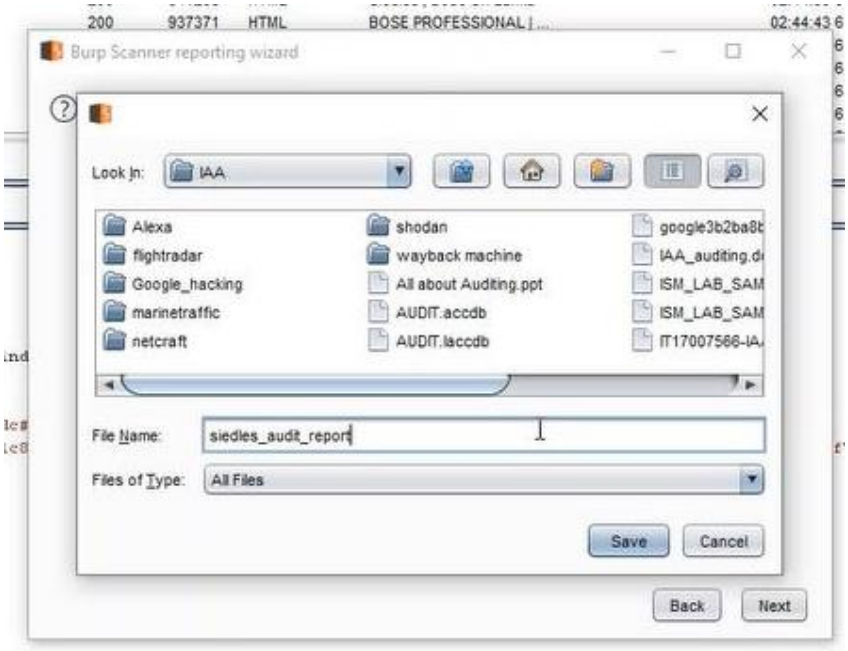


Figure 20

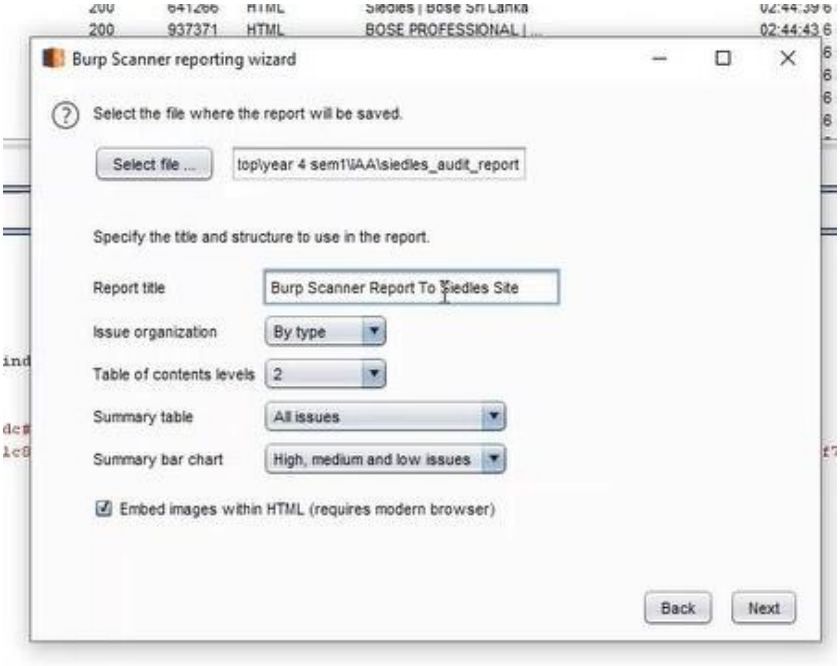
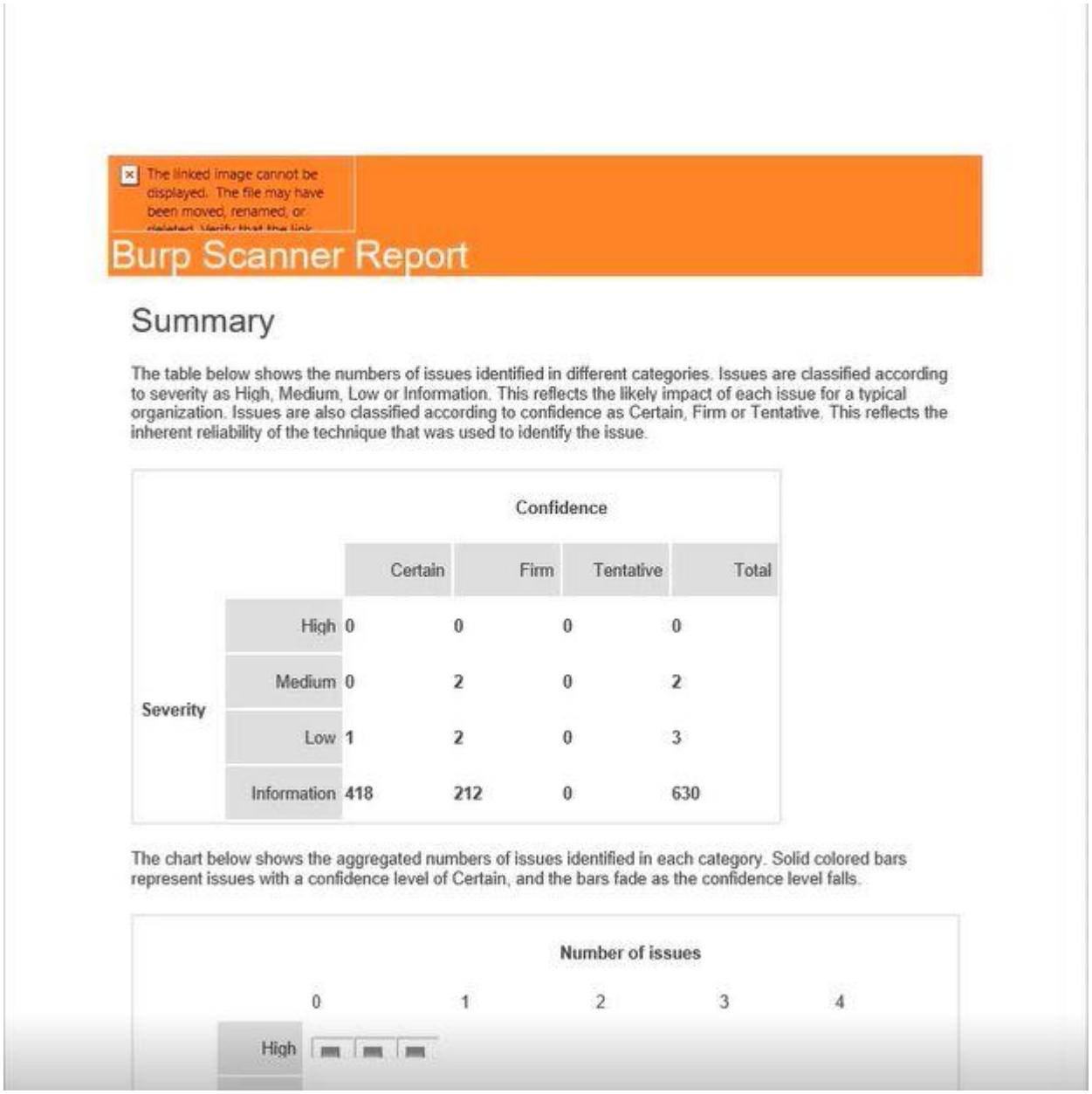


Figure 21

The Scanner Report will look like as shown below.


The linked image cannot be displayed. The file may have been moved, renamed, or

Burp Scanner Report

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	2	0	2
	Low	1	2	0	3
	Information	418	212	0	630

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

Figure 22

Audit SSL implementation

To perform SSL checkup “Qualys SSL Labs” is a great online tool. You can paste the URL in the appropriate section and start the process by click in on the “Submit” button.

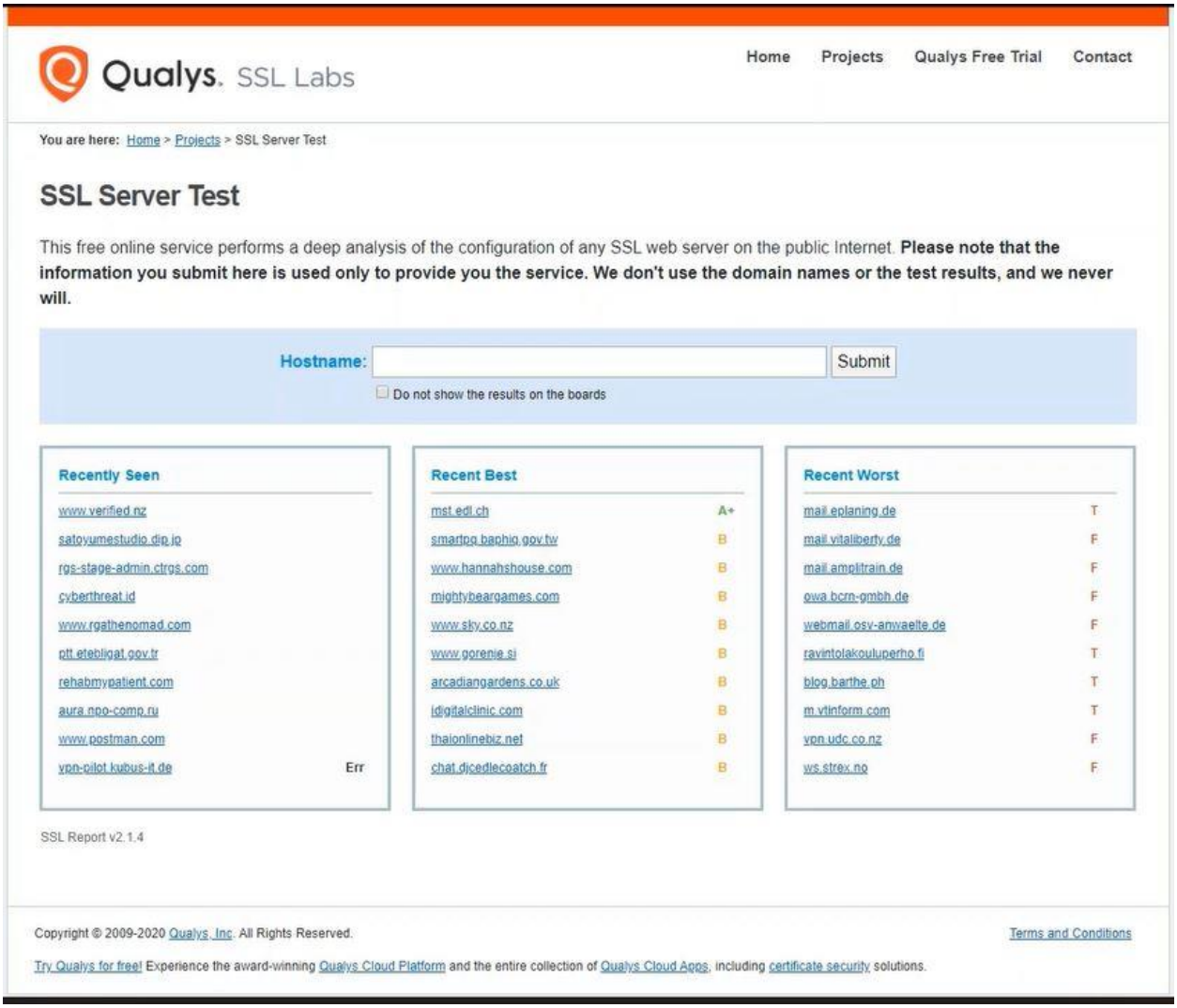


Figure 23

Results of the SSL checkup will looks like the below figure.

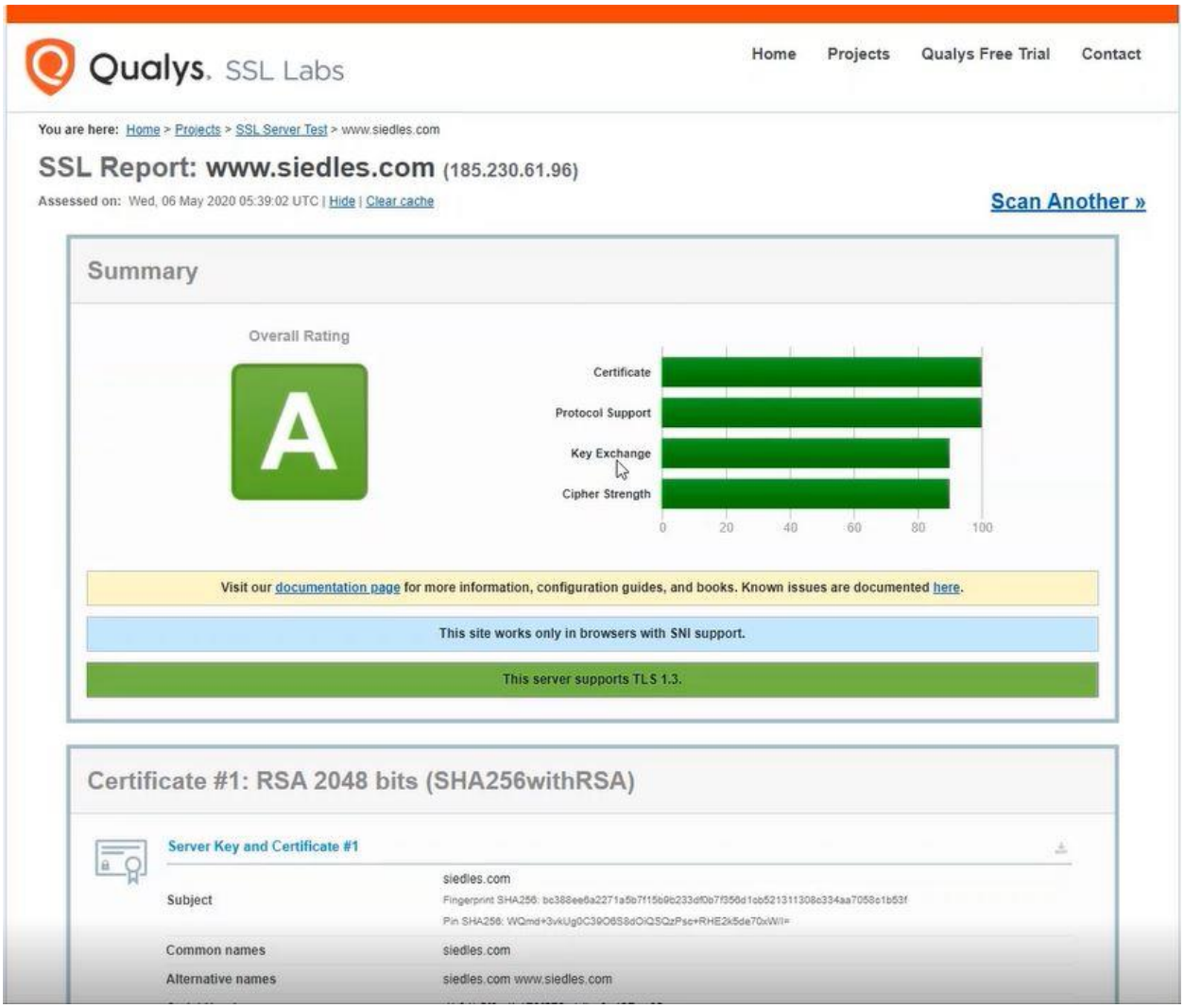


Figure 24

Audit website performance, speed and device compatibility

To check website performance, speed and device Compatibility, we can use google developer tools.

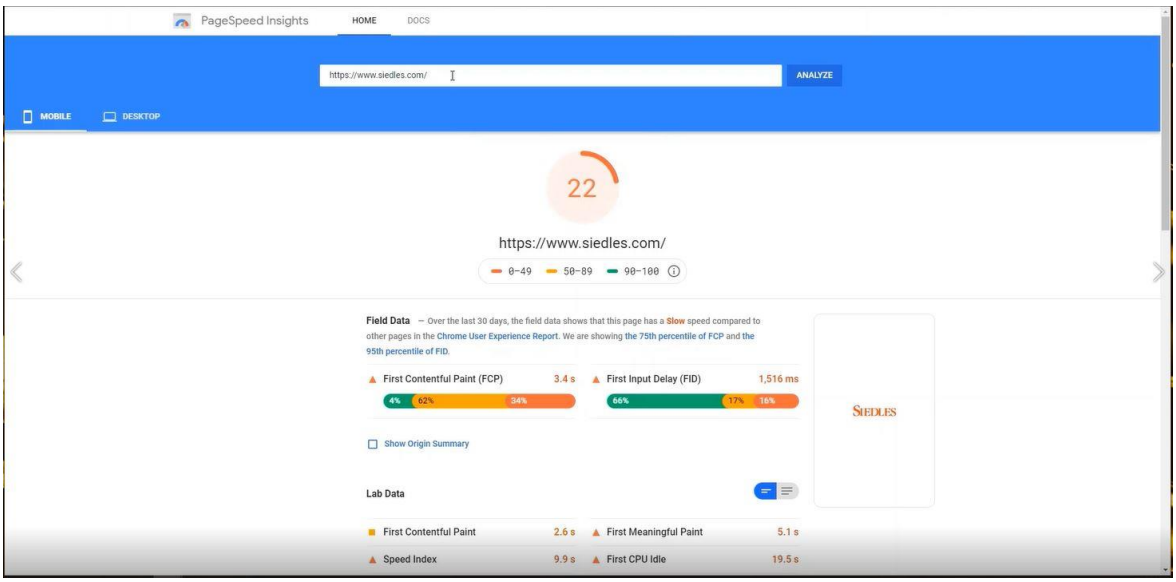


Figure 26

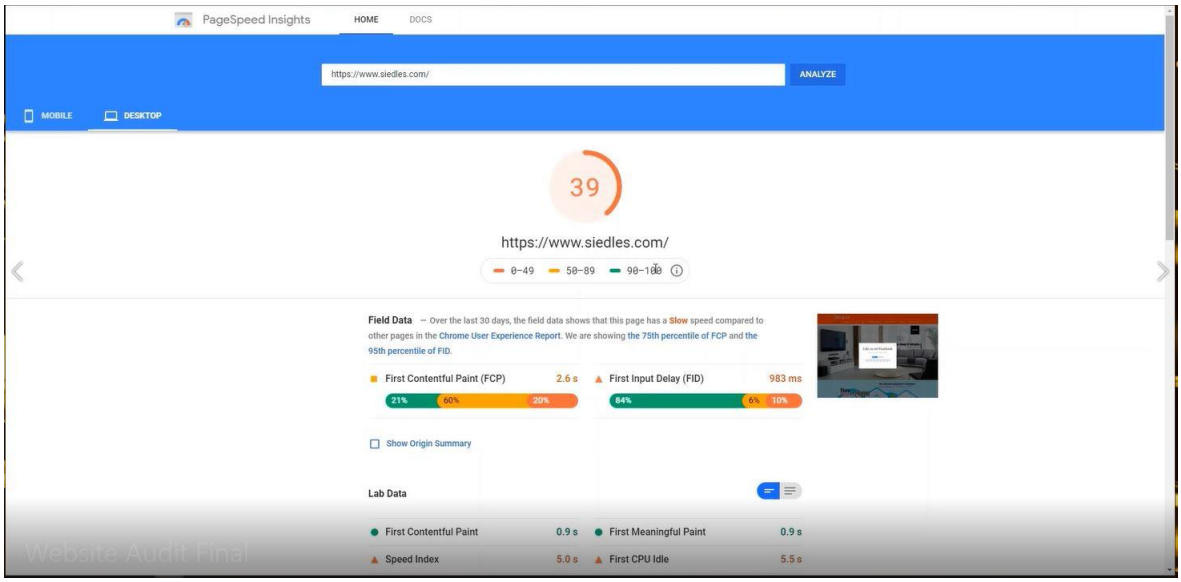


Figure 27

As well as GTmetrix is another tool for check speed of the website. It will provide a complete detail report according to the performance of the website that you need to audit.

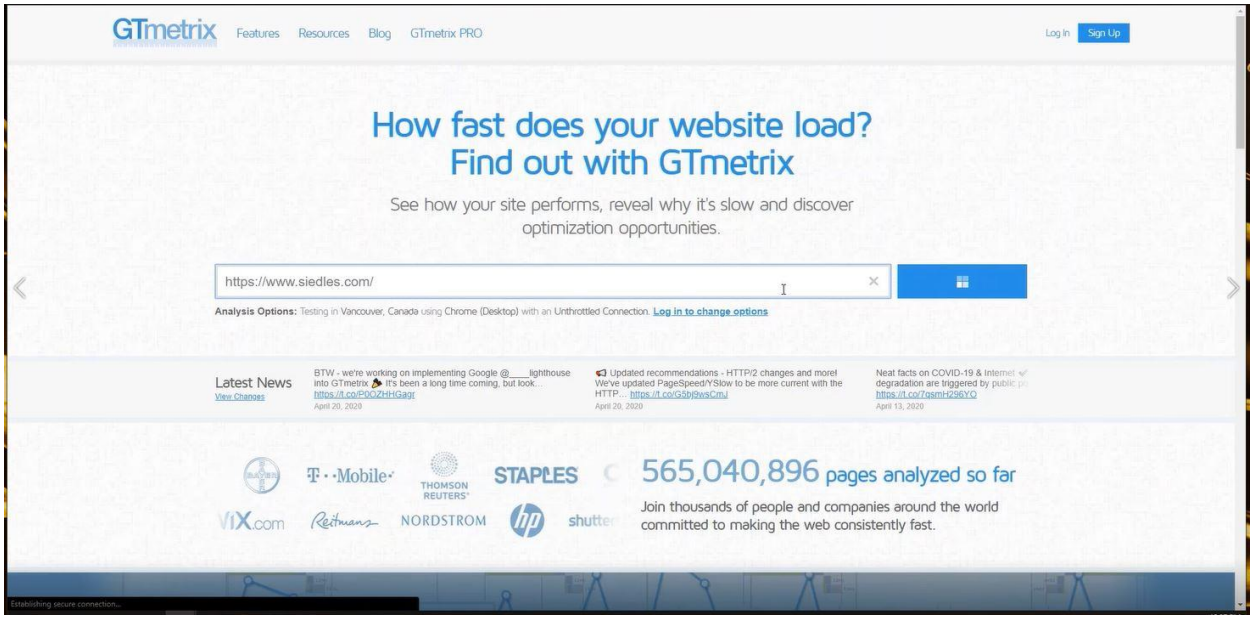


Figure 28

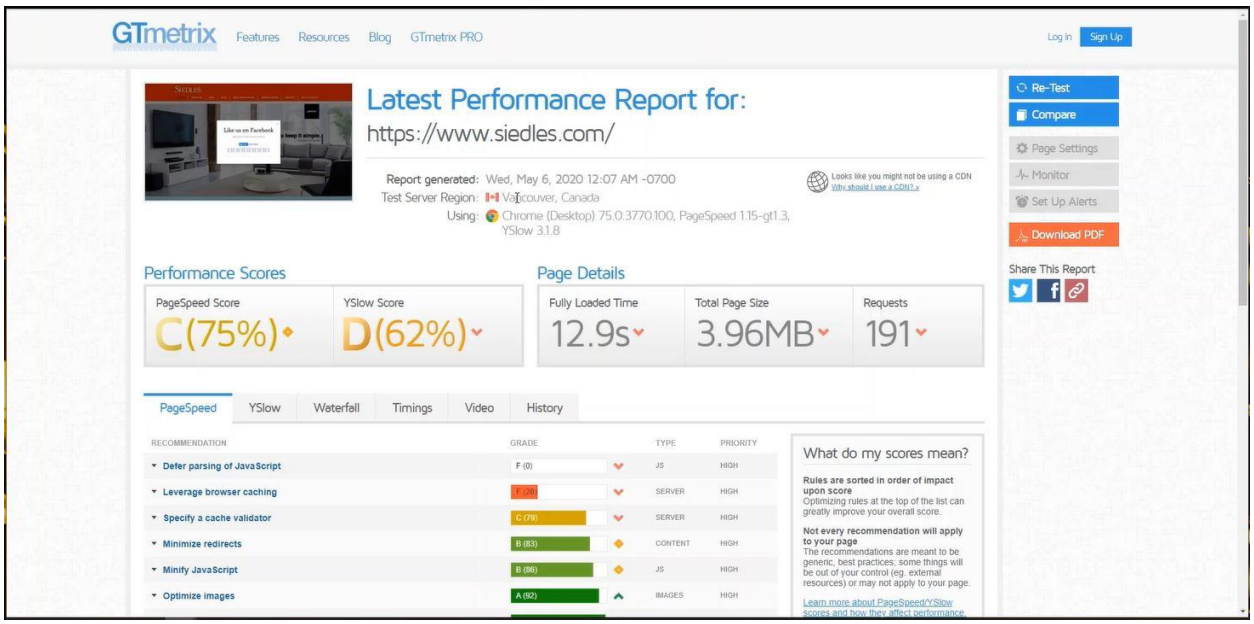


Figure 29

SEO audit

There are plenty of online tools to perform an SEO audit. In this, we use an SEO audit tool built by NEIL PATEL.

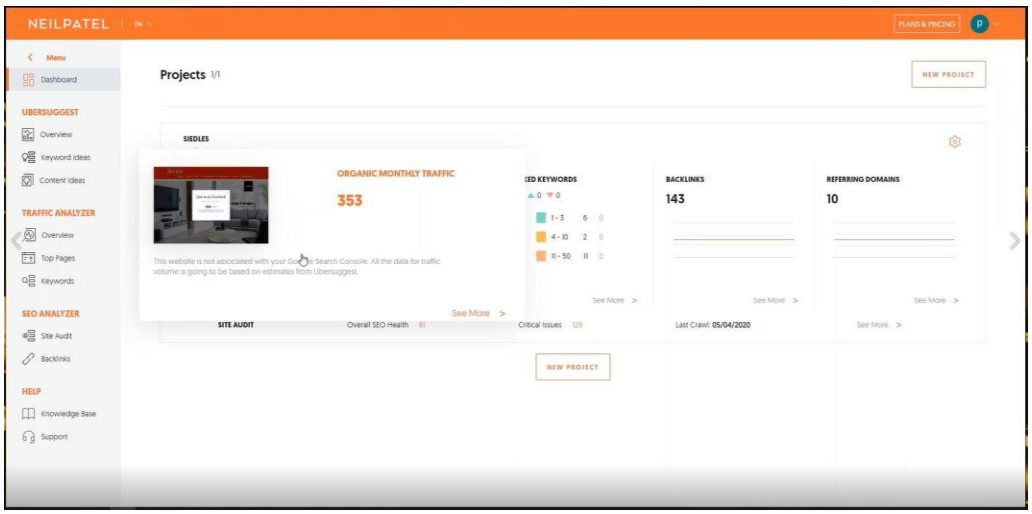


Figure 30

In the overview tab, we can see organic keywords, domain score and backlink overview.

Domain Overview

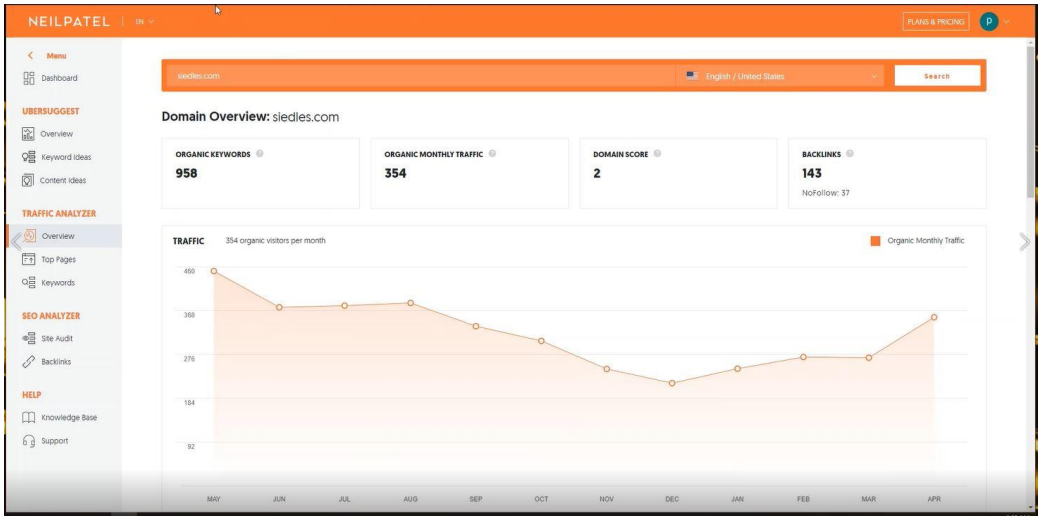


Figure 31

SEO keywords ranking

Figure 32

Backlinks

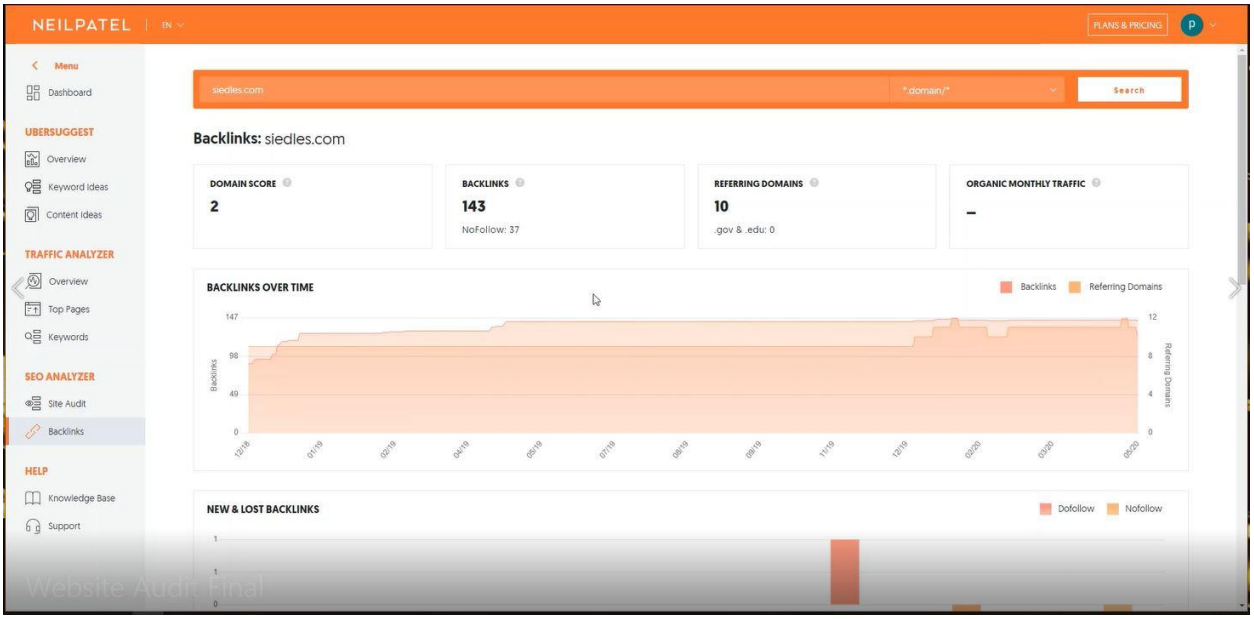


Figure 33

Keywords

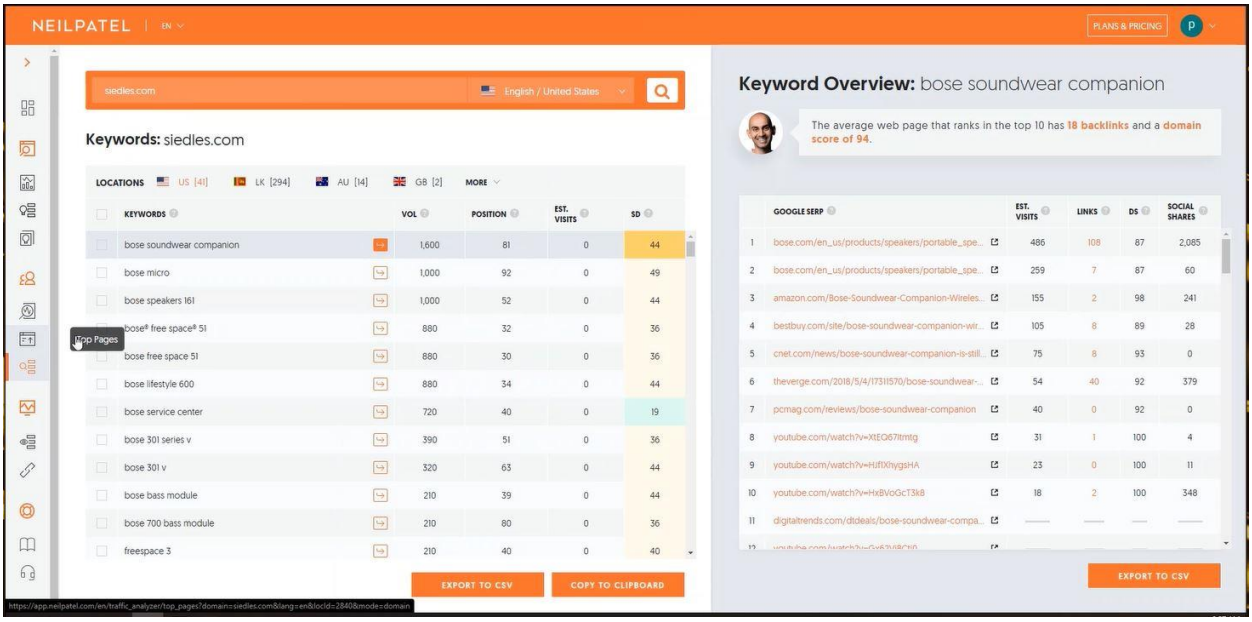


Figure 34

Summary of the SEO audit

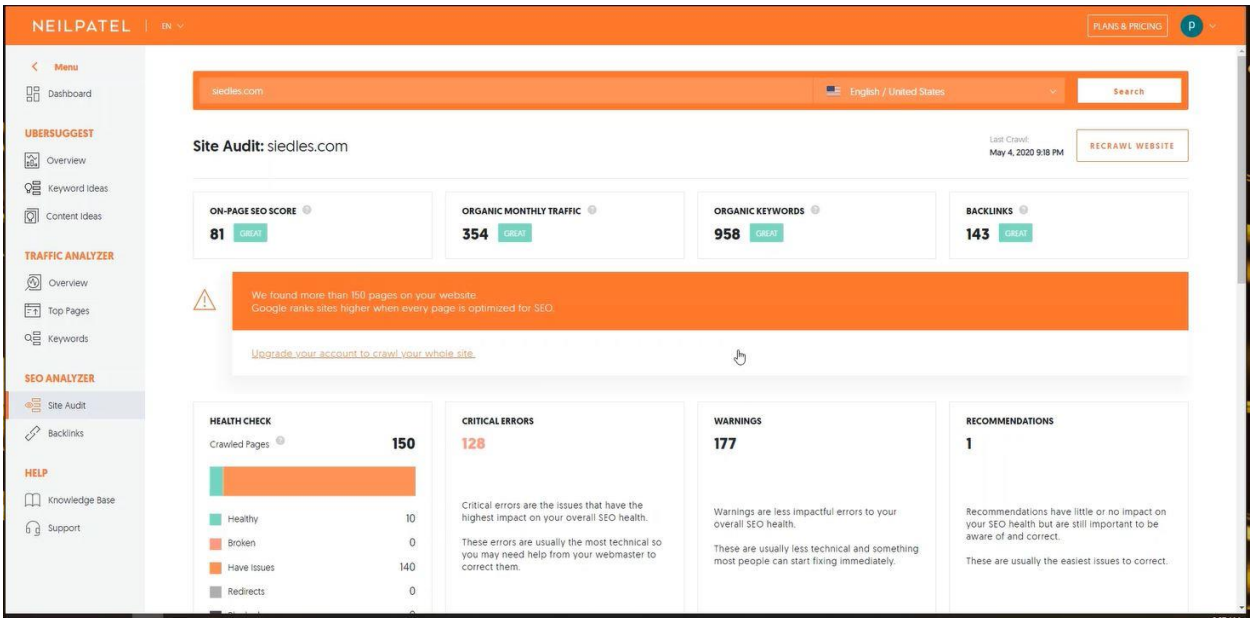


Figure 35

Summary of the website audit

Security

In this site, we could not spot any critical vulnerability issues. There are only two medium issues and several issues that have an only small impact on the site. These are the issues and recommendation given by Burp Suite to address those medium issues,

1. SSL cookie without secure flag set

1.1. https://www.siedles.com/
1.2. https://www.siedles.com/
1.3. https://www.siedles.com/

2. Cookie without HttpOnly flag set

2.1. https://www.siedles.com/
2.2. https://www.siedles.com/

3. Strict transport security not enforced

4. Suspicious input transformation (reflected)

4.1. https://www.siedles.com/product-page/10-series-v-home-theater-speaker-system [URL path filename]
4.2. https://www.siedles.com/product-page/151-speaker-system [URL path filename]
4.3. https://www.siedles.com/product-page/161-speaker-system [URL path filename]
4.4. https://www.siedles.com/product-page/201-series-v-speaker-system [URL path filename]
4.5. https://www.siedles.com/product-page/251-environmental-speakers [URL path filename]
4.6. https://www.siedles.com/product-page/301-series-v-speaker-system [URL path filename]
4.7. https://www.siedles.com/product-page/acoustimass-5-series-v [URL path filename]
4.8. https://www.siedles.com/product-page/arenamatch-am10 [URL path filename]
4.9. https://www.siedles.com/product-page/arenamatch-am20 [URL path filename]
4.10. https://www.siedles.com/product-page/arenamatch-am40 [URL path filename]

5. Cross-domain Referer leakage

6. Cross-domain script include

7. Frameable response (potential Clickjacking)

8. Email addresses disclosed

8.1. https://www.siedles.com/
8.2. https://www.siedles.com/
8.3. https://www.siedles.com/repairs-upgrades

SSL cookie without secure flag set

The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

Cookie without HttpOnly flag set

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

Credit card numbers disclosed

Issue detail

The following credit card number was disclosed in the response:

- **5127704720193543**

This issue was found in multiple locations under the reported path.

Issue background

Applications sometimes disclose sensitive financial information such as credit card numbers. Responses containing credit card numbers may not represent any security vulnerability - for example, a number may belong to the logged-in user to whom it is displayed. If a credit card number is identified during a security assessment it should be verified, then application logic reviewed to identify whether its disclosure within the application is necessary and appropriate.

Website performance

When considering the performance of the website, mobile performance score is about 22% and Desktop performance is about 39% in PageSpeedInsights.

SEO

There are 300 – 400 visitors normally visit this site acroding to SEO audit. Most of the keywords are in SEO ranking, therefore this site will appear 1st page of the google search most of the time. We can find 143 backlinks to the home page of this site. More backlinks is good. Generally site take great scores in organic monthly traffic, organic keywords, and backlinks as well as on-page SEO scores.

Conclusion

Overall site security, and SEO ratings are good in this website, but need to improve performance and speed of the site. Also mitigate above mentioned medium and low risk issues is necessary to reduce and prevent future security threats.

References

- ssllabs.com.2020.SSL Server Test (Powered by Qualys SSL Labs). [Online] Available at:
- < https://www.ssllabs.com/ssltest/analyze.html?d=www.siedles.com&latest> [Accessed 4 May 2020]

- portswigger.net. 2020. Download Burp Suite [online] Available at: < **https://portswigger.net/burp**> [Accessed 4 May 2020]

- gtmetrix.com 2020. Gtmetrix Site performance. [Online] Available at: <**https://gtmetrix.com/**> [Accessed 4 May 2020]
- developers.google.com. 2020. PageSpeed Insights. [Online] Available at: < **https://developers.google.com/speed/pagespeed/insights/** > [Accessed 4 May 2020]
- neilpatel.com. 2020. SEO auditing. [Online] Available at: <**https://app.neilpatel.com/en/dashboard**> [Accessed 4 May 2020]