



# **Information Assurance & Auditing**

**4<sup>nd</sup> Year - 1<sup>st</sup> 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**

<b>Abstract .....</b>	<b>i</b>
<b>What is Website auditing.....</b>	<b>1</b>
<b>Steps to perform a website audit .....</b>	<b>1</b>
<b>Perform a passive security audit using Burp Suite .....</b>	<b>2</b>
<b>Perform an active security audit using Burp Suite .....</b>	<b>8</b>
<b>Audit SSL implementation .....</b>	<b>15</b>
<b>Audit website performance, speed and device compatibility .....</b>	<b>17</b>
<b>SEO audit .....</b>	<b>19</b>
<b>Summary of the website audit .....</b>	<b>22</b>
<b>Conclusion .....</b>	<b>24</b>
<b>References .....</b>	<b>25</b>

## **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.

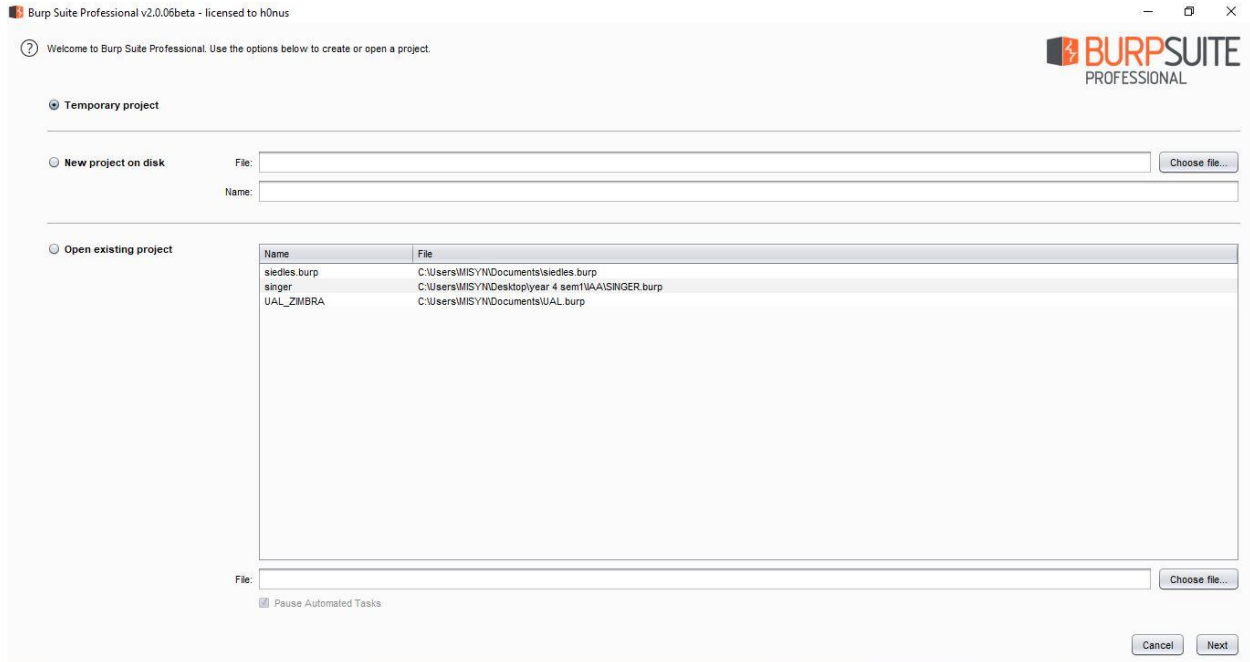


Figure 1

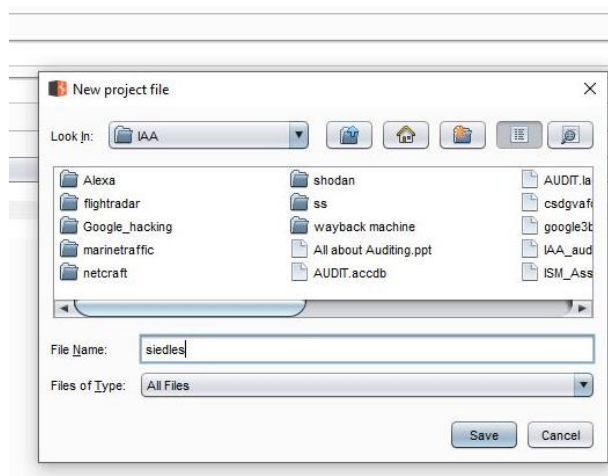


Figure 2

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

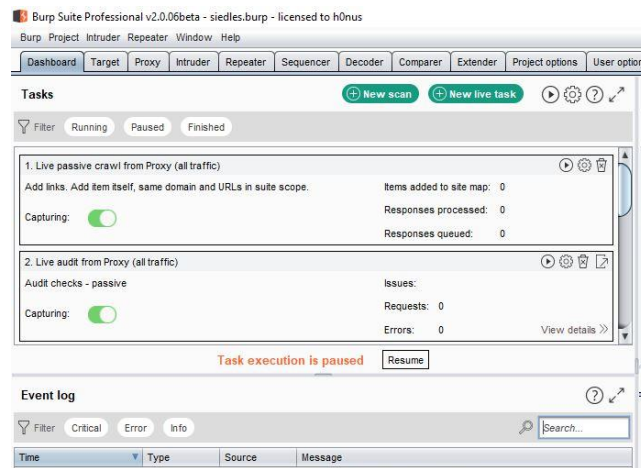


Figure 3

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.

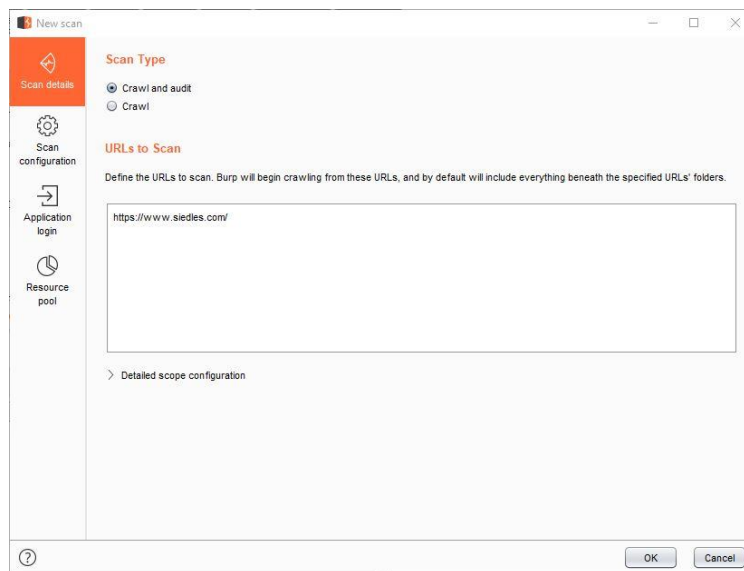


Figure 4

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.

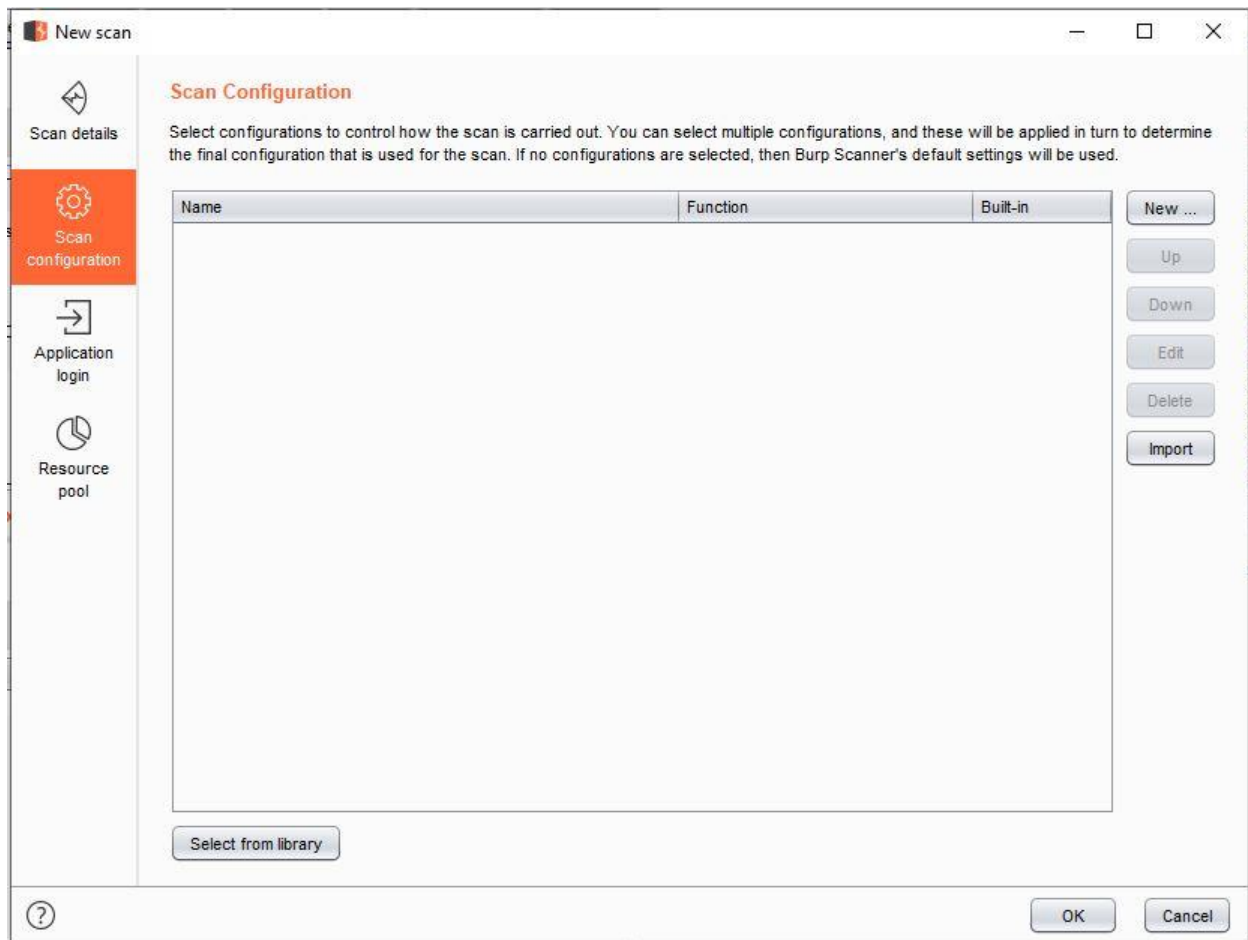


Figure 5

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.

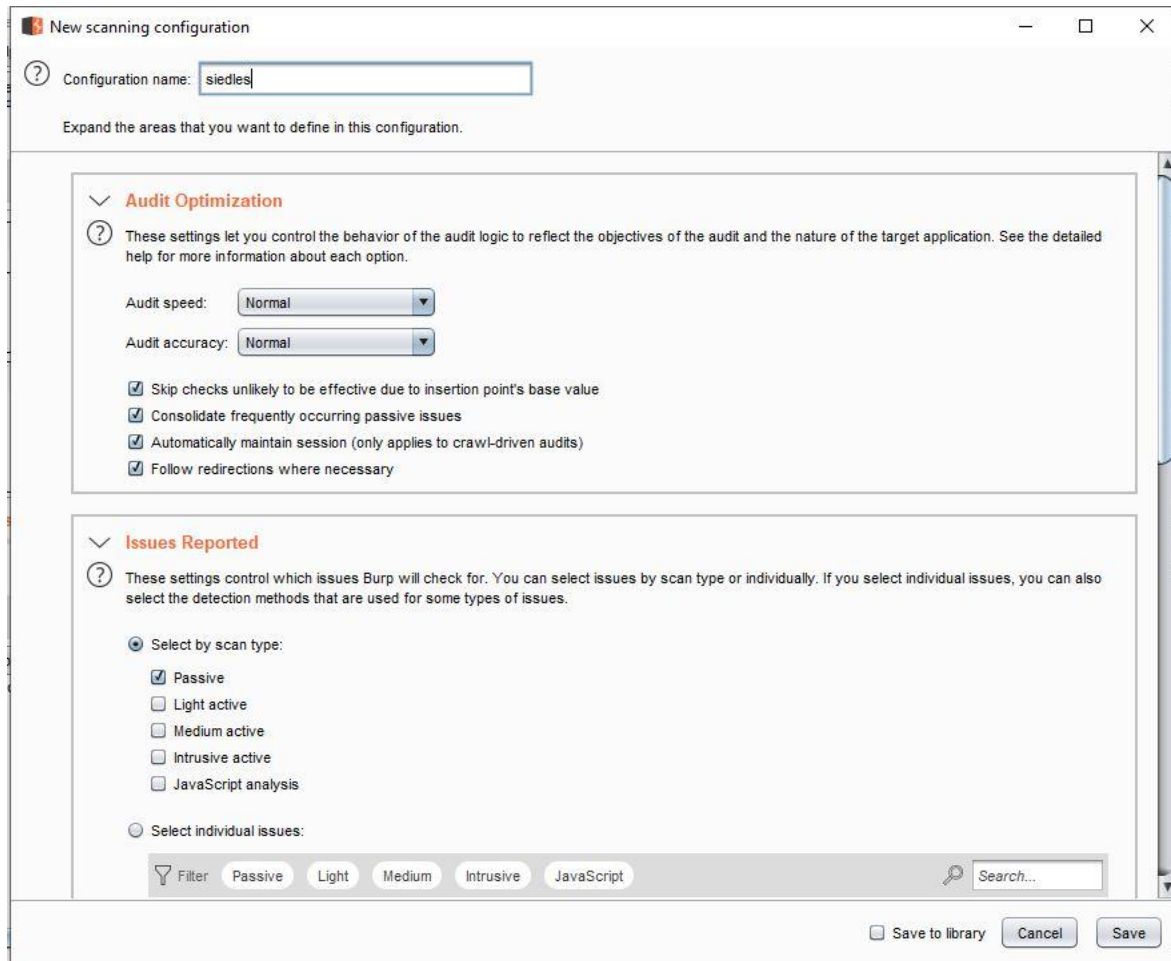


Figure 6

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.



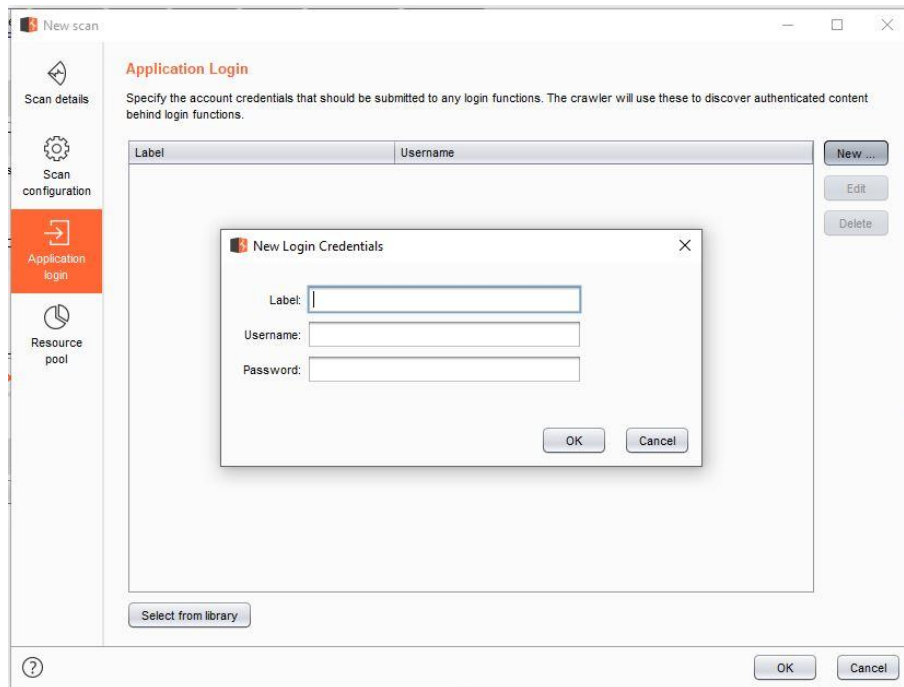


Figure 7

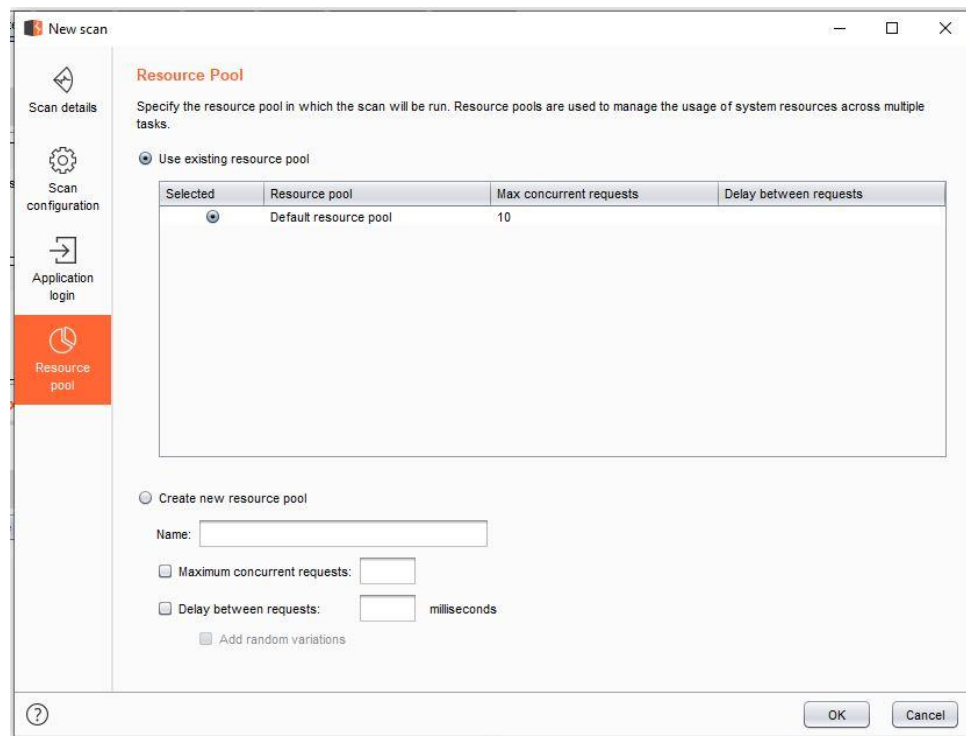


Figure 8

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

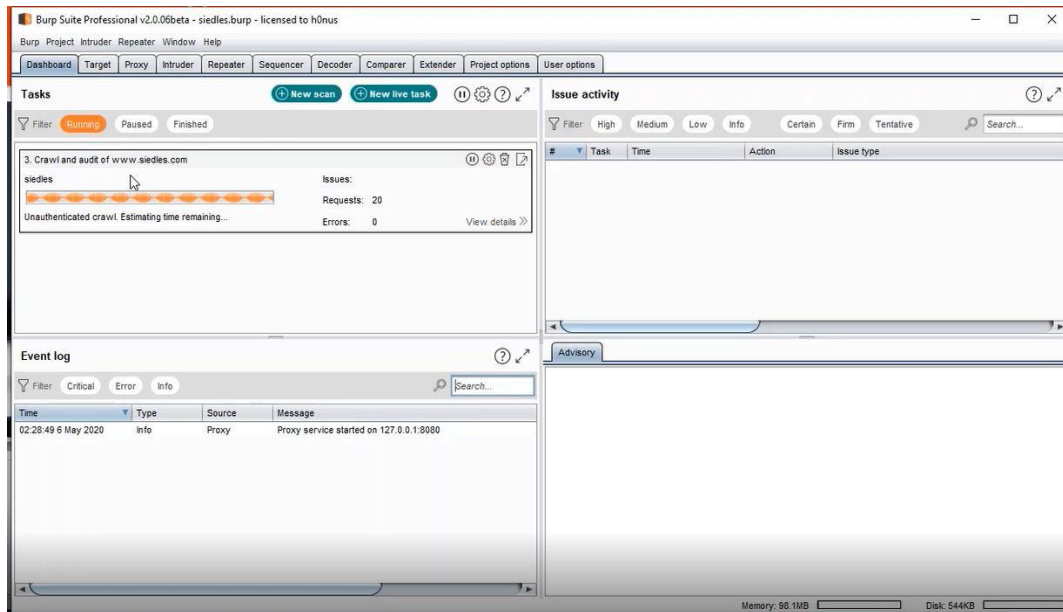


Figure 9

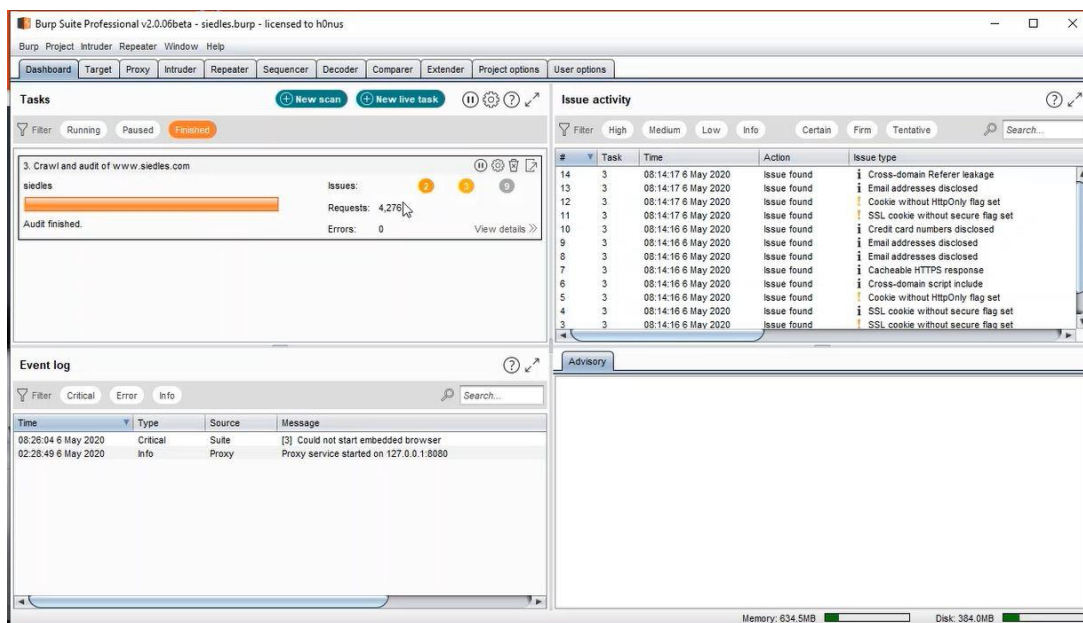


Figure 10

## 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.

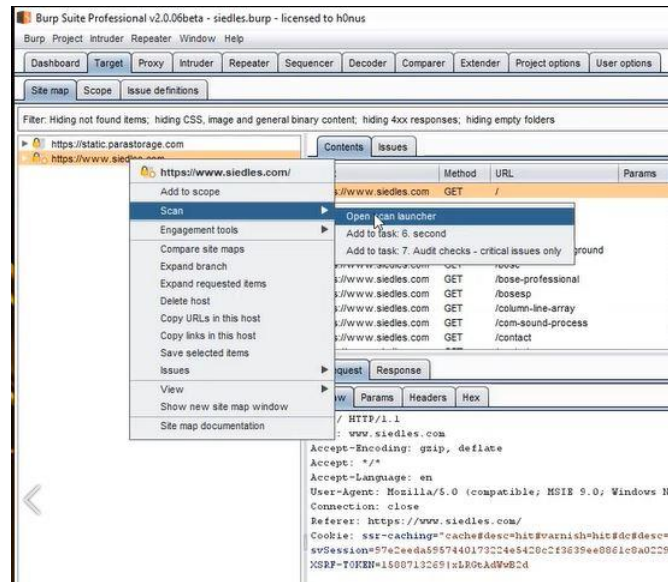


Figure 11

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

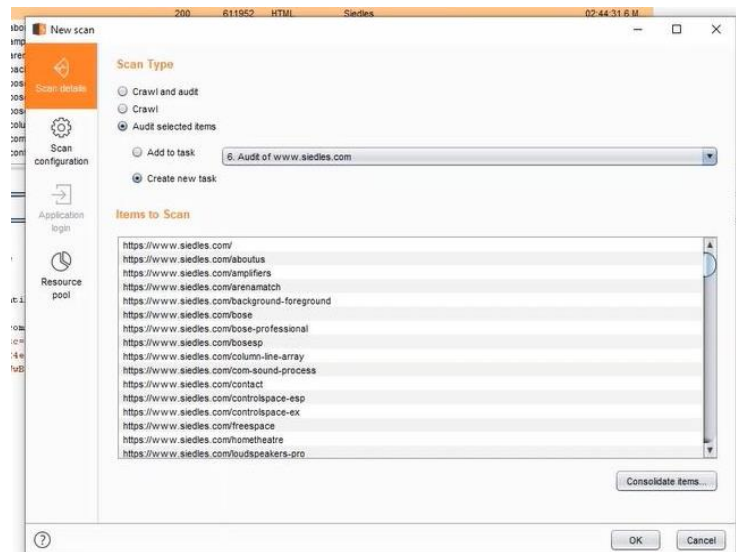


Figure 12

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

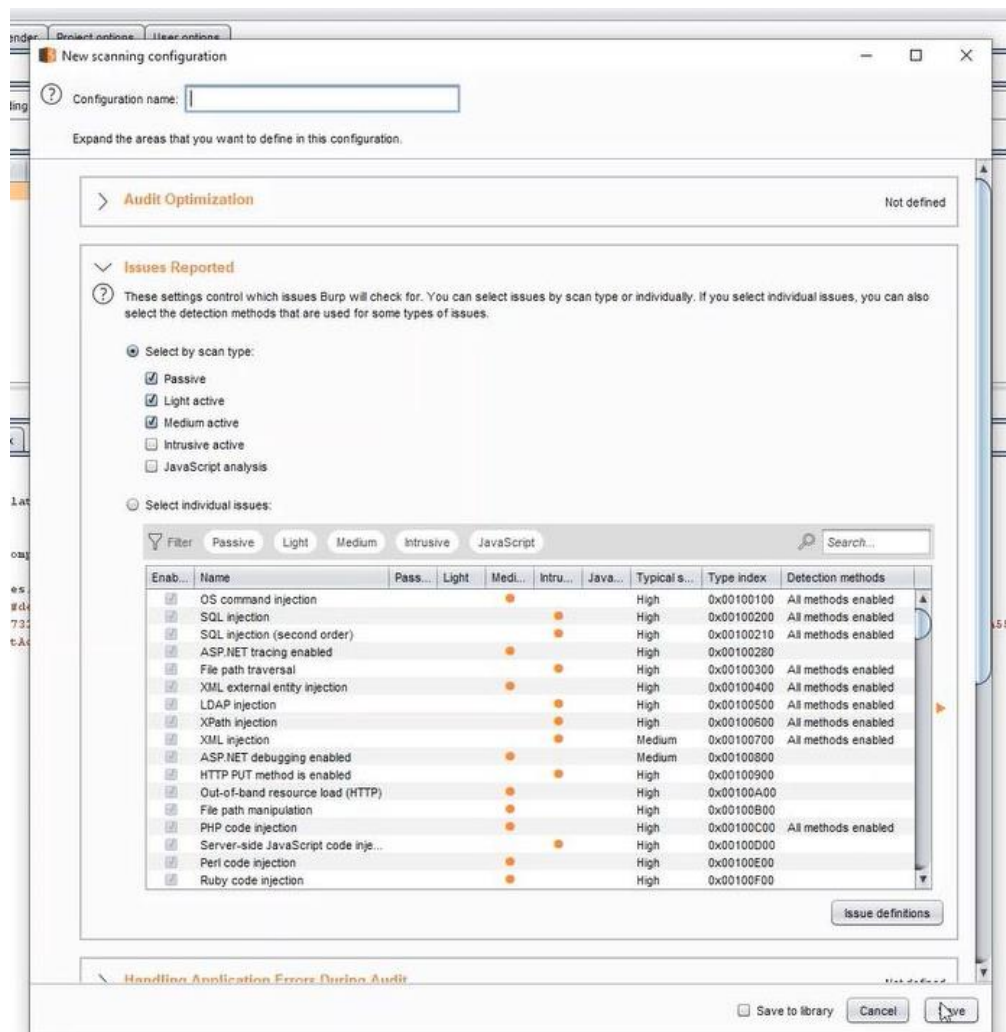


Figure 13

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.

**Issue Definitions**

This listing contains the definitions of all issues that can be detected by Burp Scanner.

Name	Typical severity	Type index
OS command injection	High	0x00100100
SQL injection	High	0x00100200
SQL injection (second order)	High	0x00100210
ASP.NET tracing enabled	High	0x00100280
File path traversal	High	0x00100300
XML external entity injection	High	0x00100400
LDAP injection	High	0x00100500
XPath injection	High	0x00100600
XML injection	Medium	0x00100700
ASP.NET debugging enabled	Medium	0x00100800
HTTP PUT method is enabled	High	0x00100900
Out-of-band resource load (HTTP)	High	0x00100a00
File path manipulation	High	0x00100b00
PHP code injection	High	0x00100c00
Server-side JavaScript code injection	High	0x00100d00
Perl code injection	High	0x00100e00
Ruby code injection	High	0x00100f00
Python code injection	High	0x00100f10
Expression Language injection	High	0x00100f20
Unidentified code injection	High	0x00101000
Server-side template injection	High	0x00101080
SSI injection	High	0x00101100
Cross-site scripting (stored)	High	0x00200100
Web cache poisoning	High	0x00200180
HTTP response header injection	High	0x00200200
Cross-site scripting (reflected)	High	0x00200300
Client-side template injection	High	0x00200308
Cross-site scripting (DOM-based)	High	0x00200310
Cross-site scripting (reflected DOM-based)	High	0x00200311
Cross-site scripting (stored DOM-based)	High	0x00200312
JavaScript injection (DOM-based)	High	0x00200320
JavaScript injection (reflected DOM-based)	High	0x00200321

**OS command injection**

**Description**

Operating system command injection vulnerabilities arise when an application incorporates user-controllable data into a command that is processed by a shell command interpreter. If the user data is not strictly validated, an attacker can use shell metacharacters to modify the command that is executed, and inject arbitrary further commands that will be executed by the server.

OS command injection vulnerabilities are usually very serious and may lead to compromise of the server hosting the application, or of the application's own data and functionality. It may also be possible to use the server as a platform for attacks against other systems. The exact potential for exploitation depends upon the security context in which the command is executed, and the privileges that this context has regarding sensitive resources on the server.

**Remediation**

If possible, applications should avoid incorporating user-controllable data into operating system commands. In almost every situation, there are safer alternative methods of performing server-level tasks, which cannot be manipulated to perform additional commands than the one intended.

If it is considered unavoidable to incorporate user-supplied data into operating system commands, the following two layers of defense should be used to prevent attacks:

- The user data should be strictly validated. Ideally, a whitelist of specific accepted values should be used. Otherwise, only short alphanumeric strings should be accepted. Input containing any other data, including any conceivable shell metacharacter or whitespace, should be rejected.
- The application should use command APIs that launch a specific process via its name and command-line parameters, rather than passing a command string to a shell interpreter that supports command chaining and redirection. For example, the Java API Runtime.exec and the ASP.NET API Process.Start do not support shell metacharacters. This defense can mitigate the impact of an attack even in the event that an attacker circumvents the input validation defenses.

**Vulnerability classifications**

- [CWE-77: Improper Neutralization of Special Elements used in a Command \('Command Injection'\)](#)
- [CWE-78: Improper Neutralization of Special Elements used in an OS Command \('OS Command Injection'\)](#)

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.

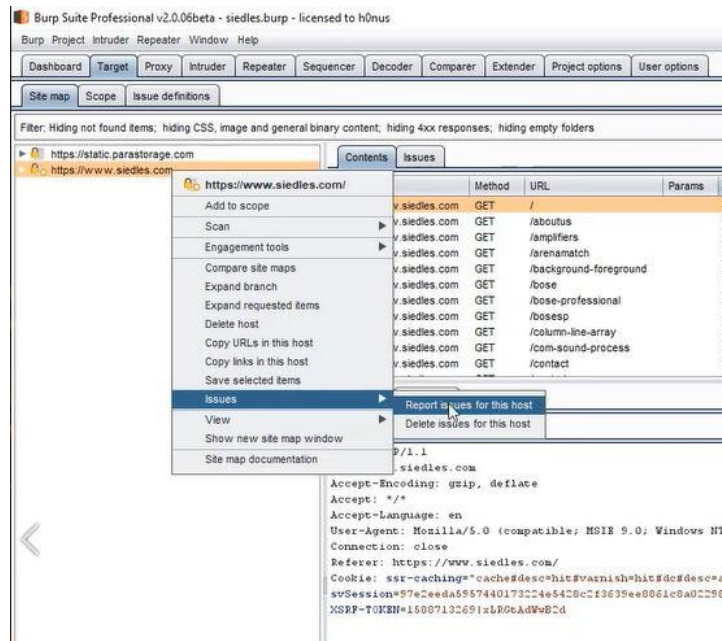


Figure 16

Then choose the format for the report.

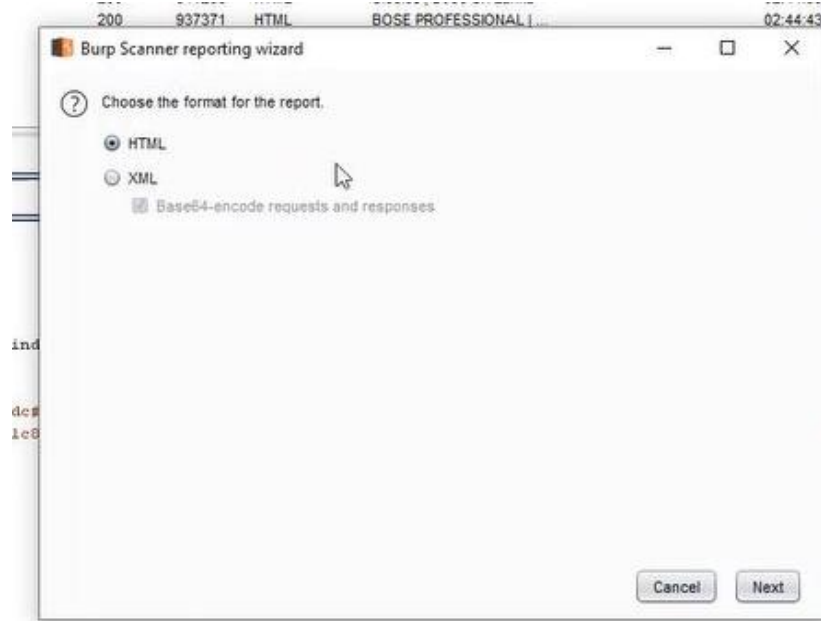


Figure 17

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

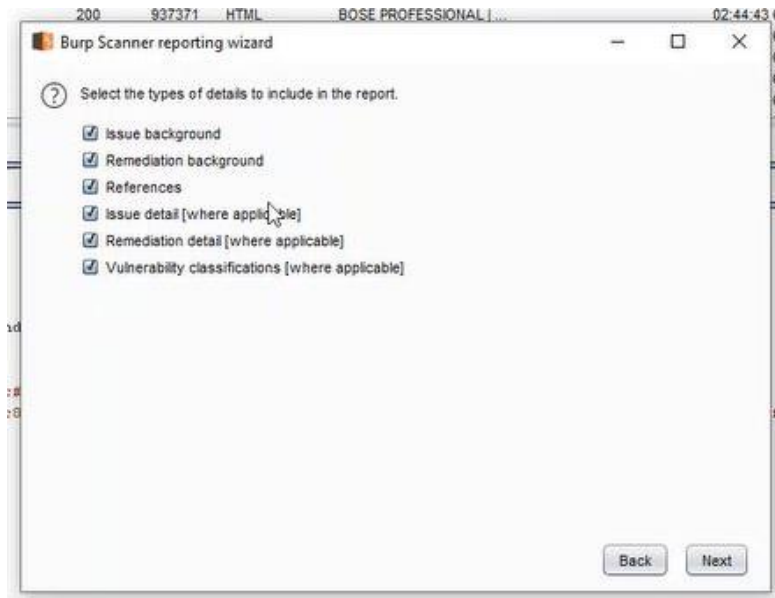


Figure18



Figure 19



Provide file location to save the report and report title.

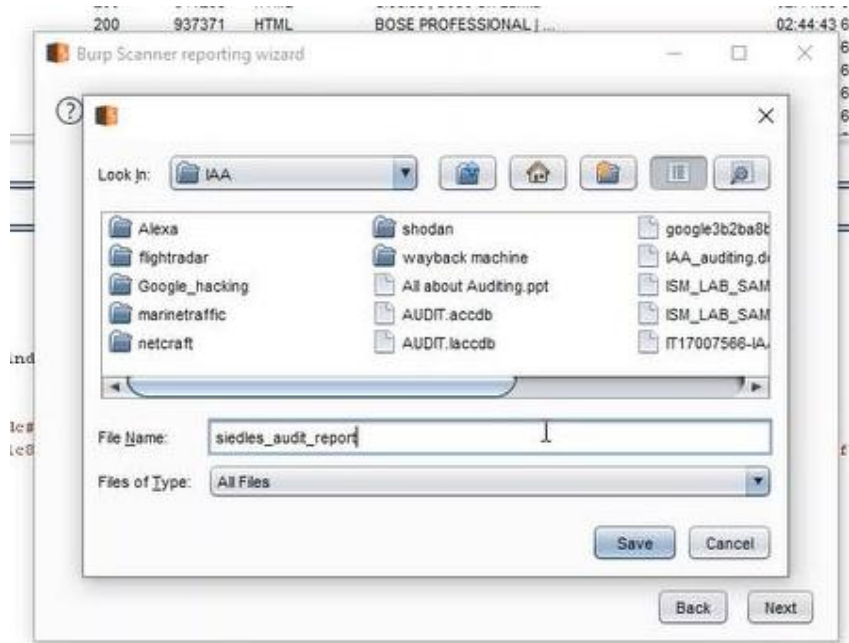


Figure 20



Figure 21



The Scanner Report will look like as shown below.

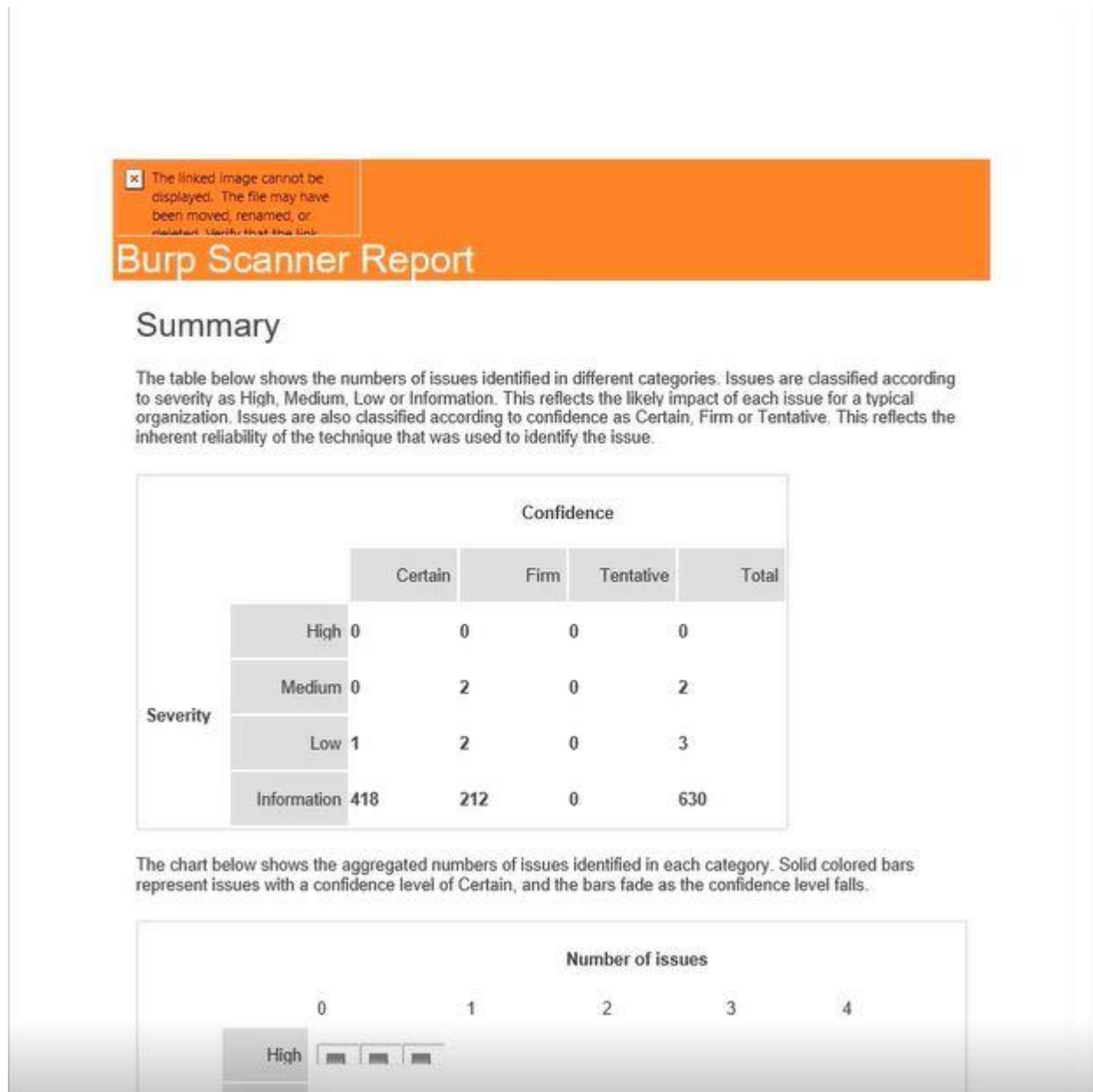


Figure 22

## 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.

The screenshot displays the Qualys SSL Labs website. At the top, there is a navigation bar with links for Home, Projects, Qualys Free Trial, and Contact. Below this, a breadcrumb trail indicates the current location: Home > Projects > SSL Server Test. The main heading is "SSL Server Test". A descriptive paragraph explains that the service performs a deep analysis of SSL web server configurations and includes a privacy notice. A form for testing is provided with a "Hostname:" label, a text input field, and a "Submit" button. A checkbox option "Do not show the results on the boards" is located below the input field. The results section is divided into three columns: "Recently Seen", "Recent Best", and "Recent Worst". Each column lists domain names with their corresponding SSL grades. The "Recently Seen" column includes domains like www.verified.nz and satoyamestudio.dig.jp. The "Recent Best" column shows domains like mst.edi.ch with an A+ grade. The "Recent Worst" column lists domains like mail.eplaning.de with a T grade. At the bottom, there is a footer with copyright information and a link to the Terms and Conditions.

Qualys SSL Labs

Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > SSL Server Test

### SSL Server Test

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.**

Hostname:  Submit

☐ Do not show the results on the boards

Recently Seen	Recent Best	Recent Worst
<a href="#">www.verified.nz</a>	<a href="#">mst.edi.ch</a> A+	<a href="#">mail.eplaning.de</a> T
<a href="#">satoyamestudio.dig.jp</a>	<a href="#">smartop.bahqin.gov.tw</a> B	<a href="#">mail.vitaliberty.de</a> F
<a href="#">rqs-stage-admin.ctqrs.com</a>	<a href="#">www.hannahshouse.com</a> B	<a href="#">mail.amplitrain.de</a> F
<a href="#">cyberthreat.id</a>	<a href="#">mightybeargames.com</a> B	<a href="#">owa.bcm-gmbh.de</a> F
<a href="#">www.rgathenomad.com</a>	<a href="#">www.sky.co.nz</a> B	<a href="#">webmail.osv-anwaelle.de</a> F
<a href="#">pft.stebilogat.gov.tr</a>	<a href="#">www.goreme.si</a> B	<a href="#">ravintolakouluperho.fi</a> T
<a href="#">rehabmypatient.com</a>	<a href="#">arcadiangardens.co.uk</a> B	<a href="#">blog.barthe.ch</a> T
<a href="#">aura.nno-como.ru</a>	<a href="#">idig@alclinic.com</a> B	<a href="#">m.vtinform.com</a> T
<a href="#">www.postman.com</a>	<a href="#">thalonlinebiz.net</a> B	<a href="#">vpn.udc.co.nz</a> F
<a href="#">vpn-pilot.kubus-it.de</a>	<a href="#">chat.dicedlecoatch.fr</a> B	<a href="#">ws.strex.no</a> F

SSL Report v2.1.4

Copyright © 2009-2020 Qualys, Inc. All Rights Reserved. [Terms and Conditions](#)

Try Qualys for free! Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.

Figure 23

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

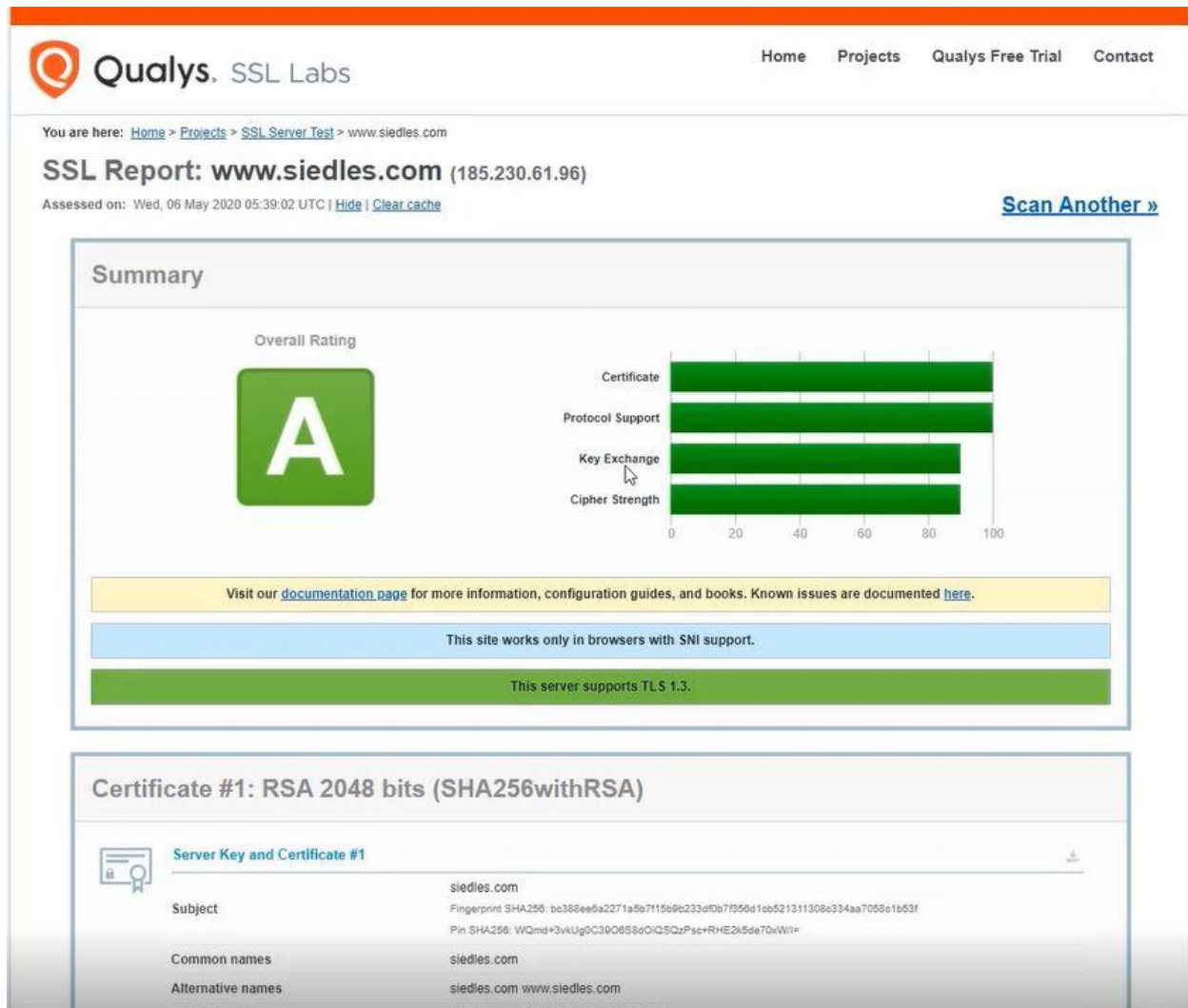


Figure 24

## Audit website performance, speed and device compatibility

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

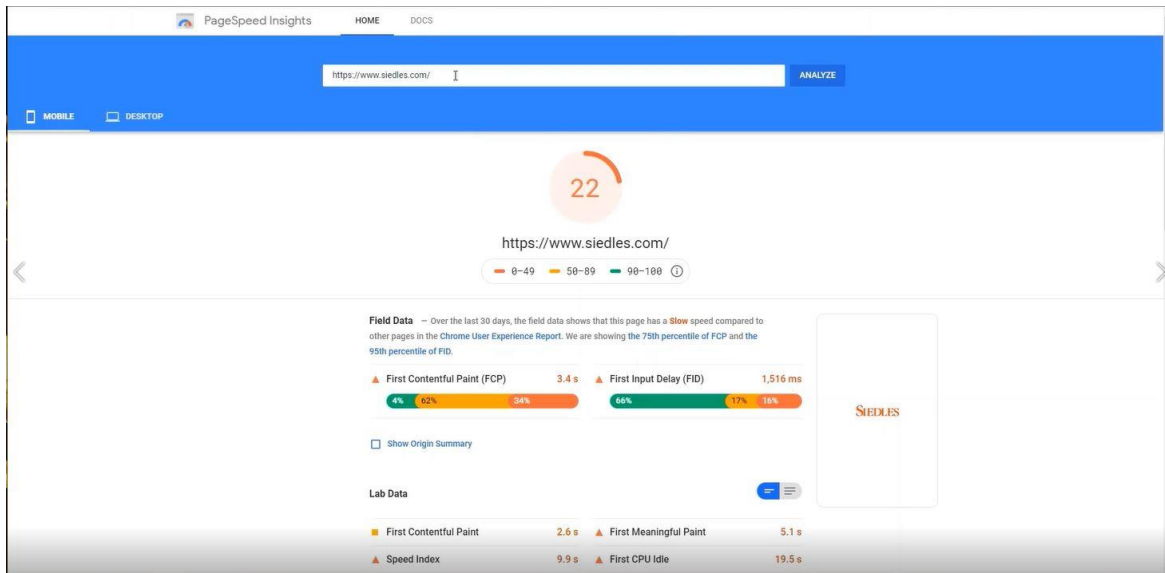


Figure 26

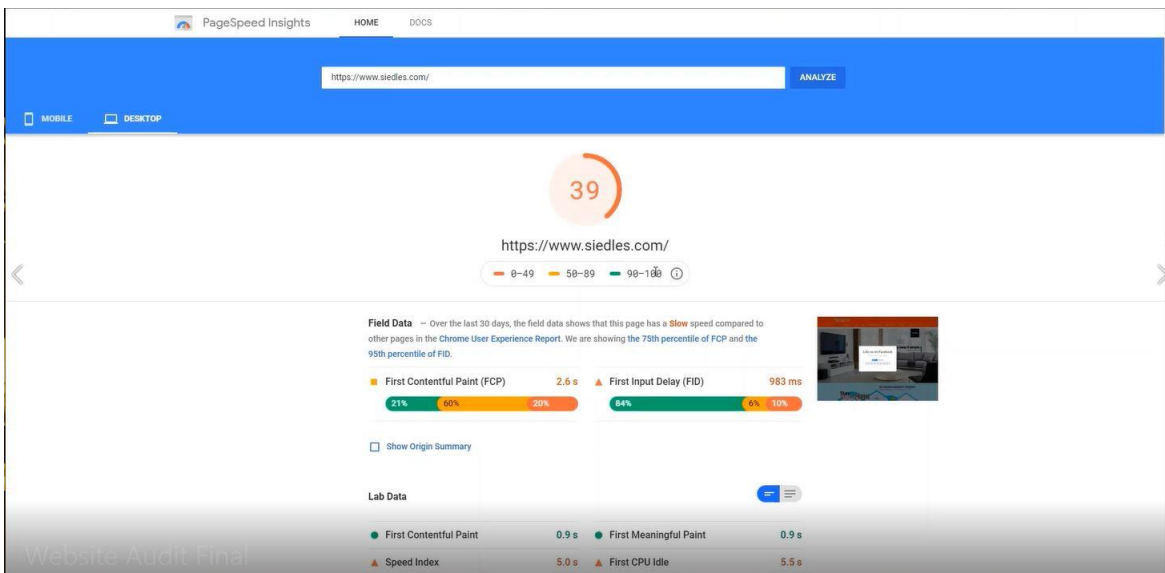


Figure 27

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.

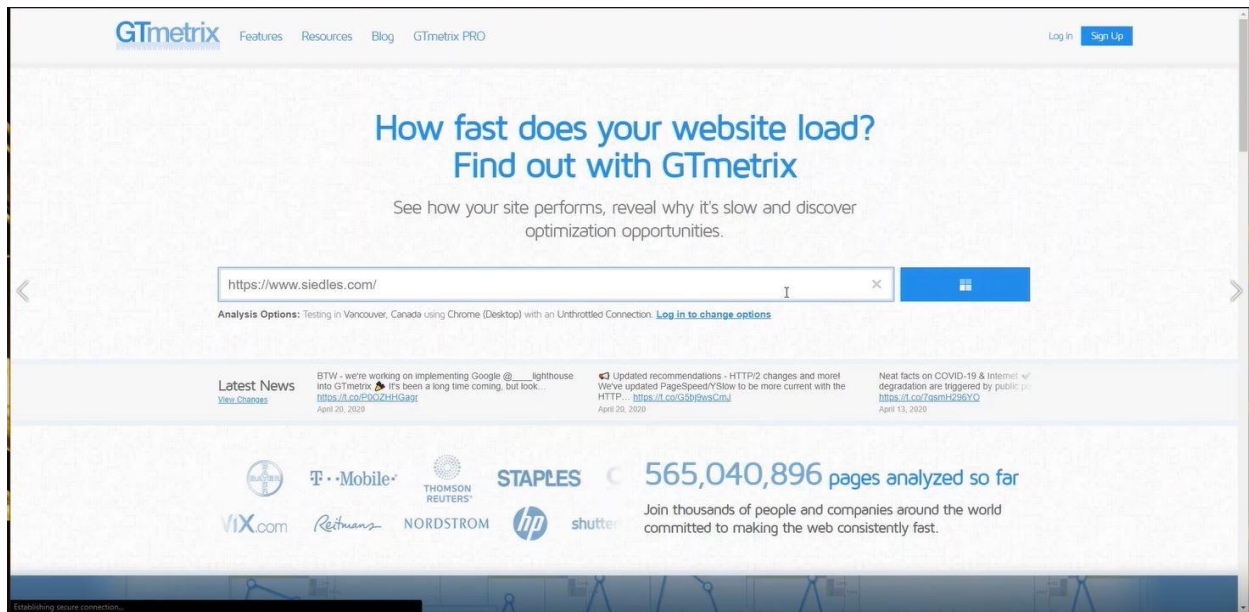


Figure 28

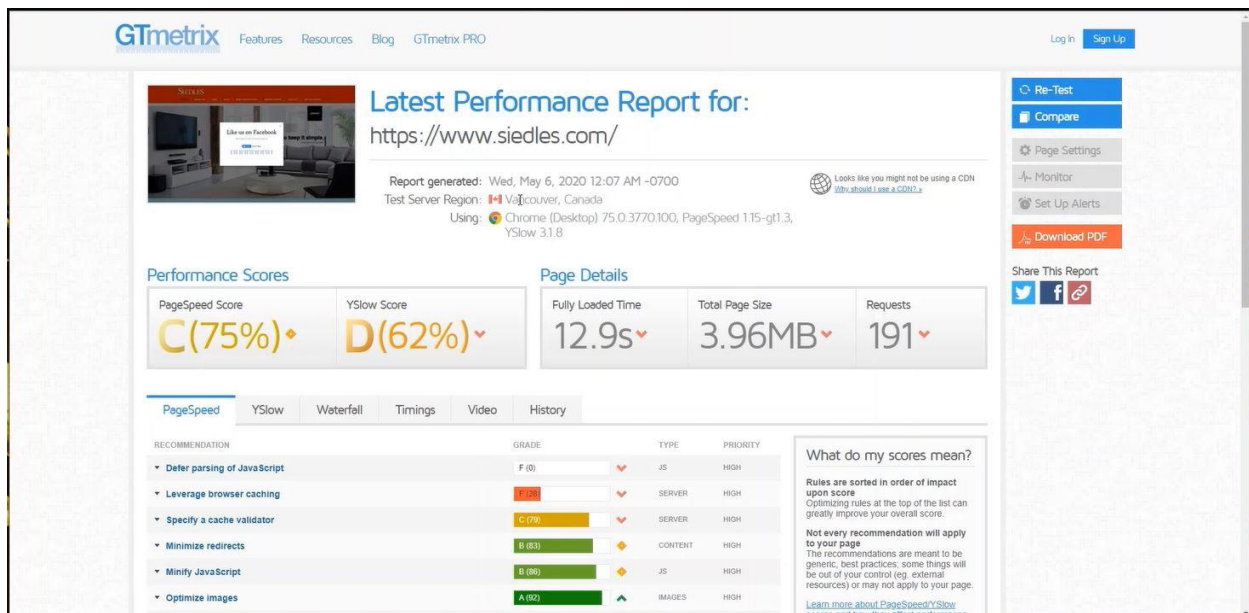


Figure 29

## 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.

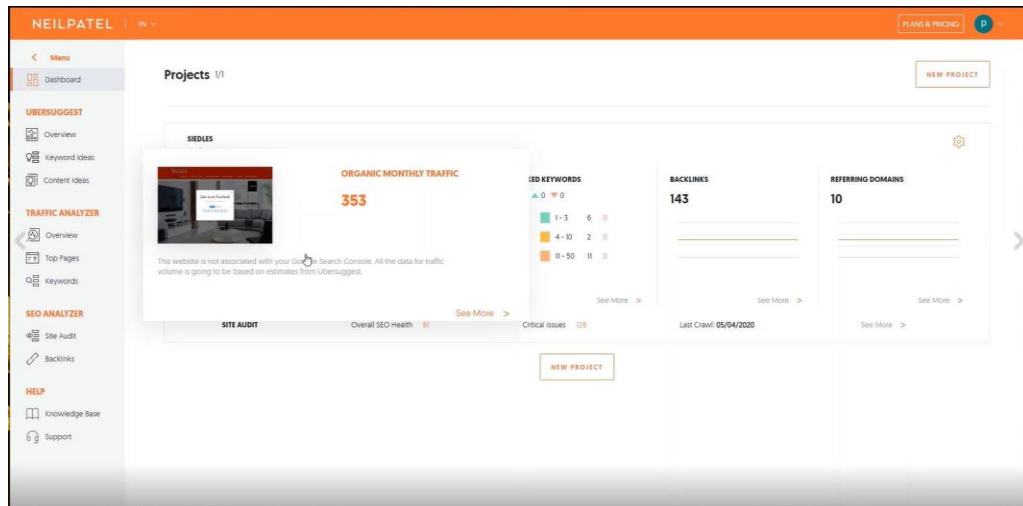


Figure 30

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

## Domain Overview

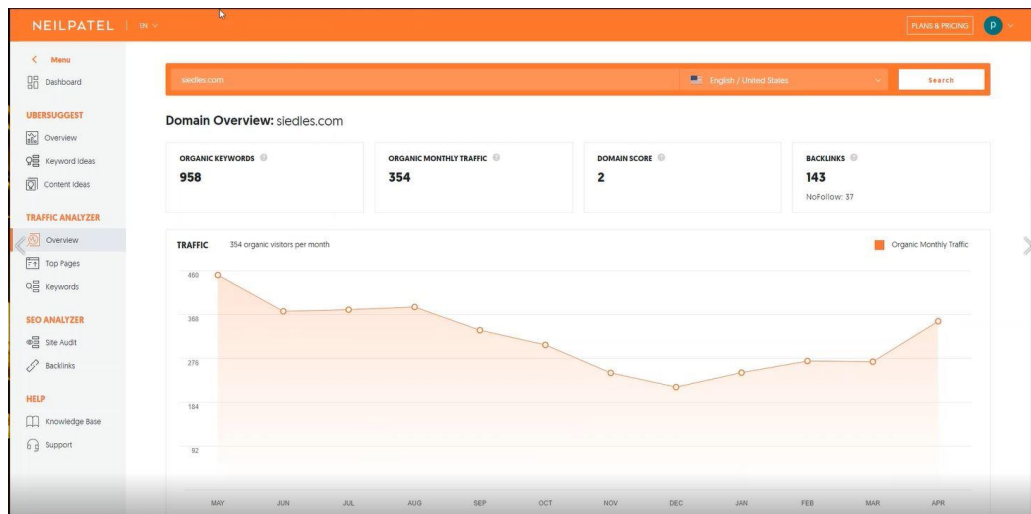


Figure 31

## SEO keywords ranking



Figure 32

## Backlinks

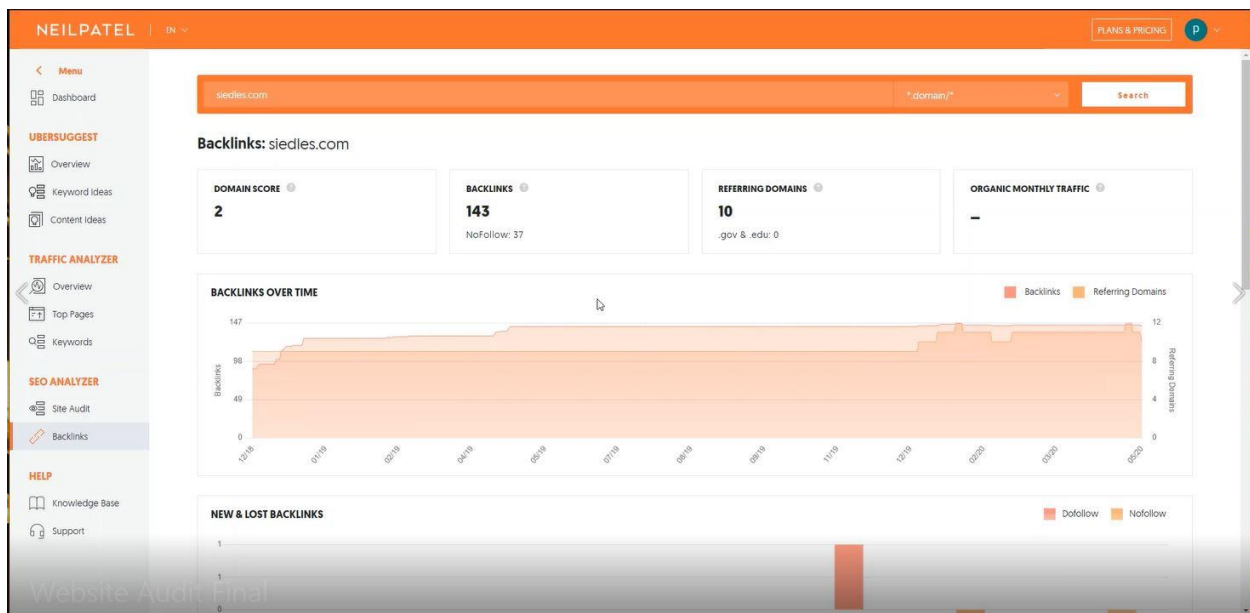


Figure 33



## Keywords

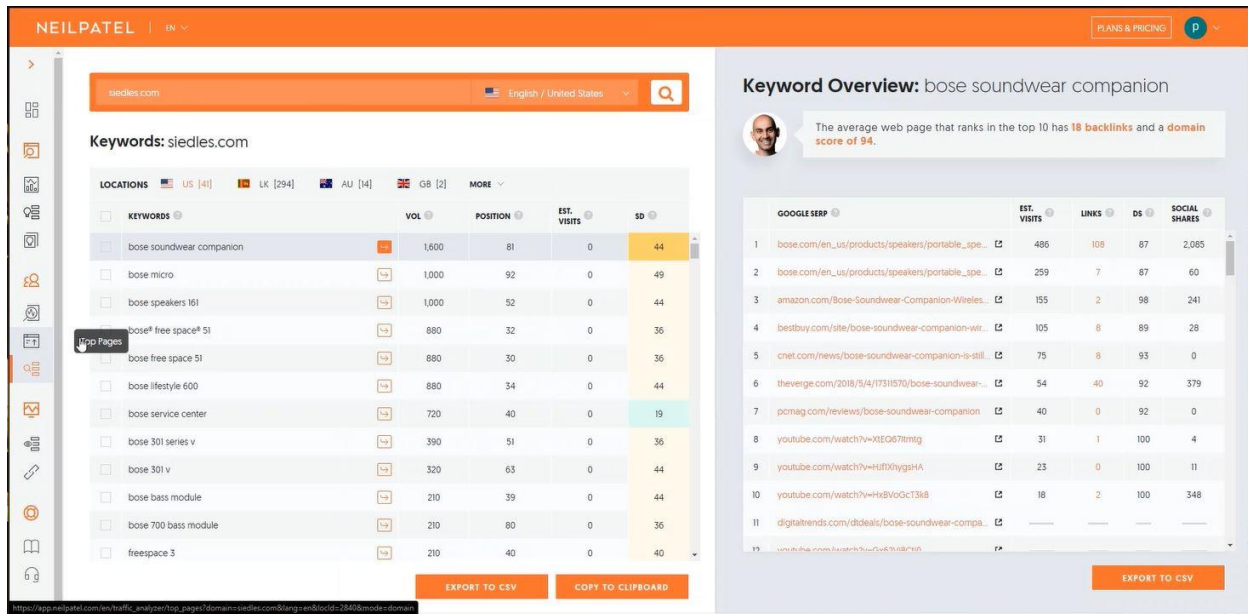


Figure 34

## Summary of the SEO audit

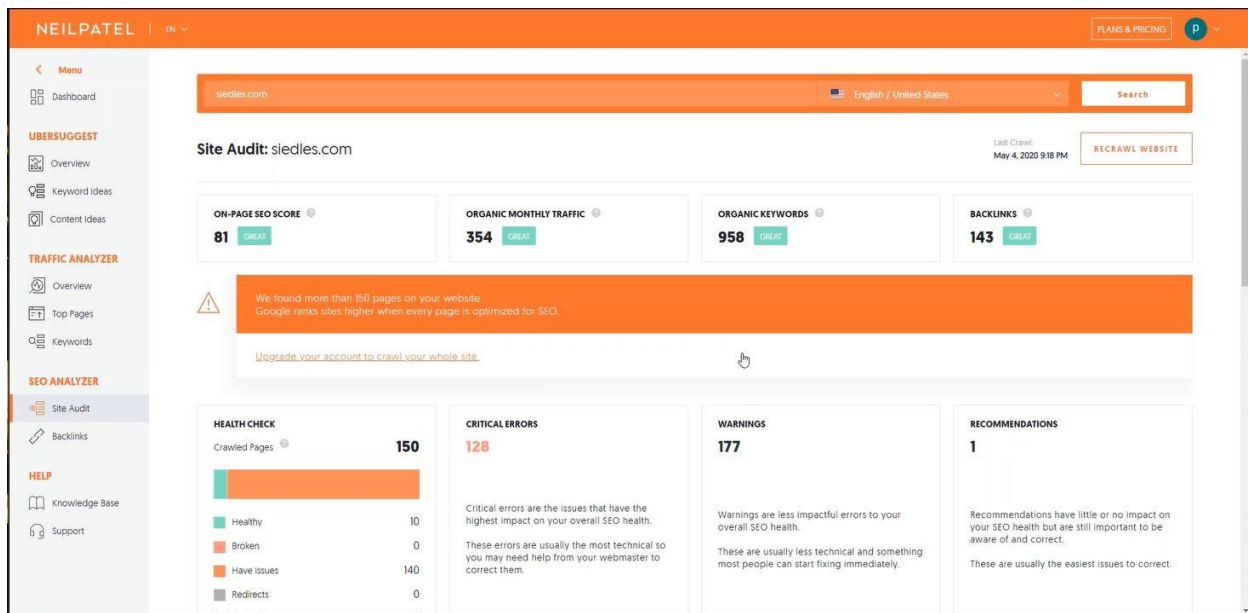


Figure 35



## 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>

## 9. Credit card numbers disclosed

## 10. Cacheable HTTPS response

### 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 according to SEO audit. Most of the keywords are in SEO ranking, therefore this site will appear 1<sup>st</sup> 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

- sslabs.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]
- gtmatrix.com 2020. Gtmatrix Site performance. [Online] Available at: <<https://gtmatrix.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]