



**IE4040**

**Information Assurance Auditing**

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

**Individual Mini Project**

Submitted to  
Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the  
Bachelor of Science Special Honors Degree in Information Technology

Shashangan J.S  
IT 16 5136 24

07-05-2020

# Table of Contents

Auditing. .... 3

Website Auditing..... 4

Audit Scope ..... 5

Audit Methodology ..... 6

Website Audit Checklist..... 8

References ..... 32

# Table of Figures

Figure 1 daraz.lk home page.....	5
Figure 2 Qualys SSL Labs SSL Server Test.....	9
Figure 3 SSL Checker .....	22
Figure 4 GTmetrix .....	24
Figure 5 Sitechecker.....	26
Figure 6 PageSpeed Insights.....	27
Figure 7 pentest tool.....	29

## **Auditing.**

An Information technology audit or information system audit is an inspection of management control within the information technology (IT) infrastructure. Assessing the evidence obtained can determine whether the information system protects assets, maintains data integrity, and effectively achieves the organization's goals. These checks can be conducted in conjunction with internal audits, financial statement audits, or any other form of certification participation [1].

With the widespread use of IT systems and the large amounts of data stored on such systems, it is important that IT systems and the data stored within are reliable and secure, because of these reasons IT audits are very important to the business.

The most important reasons to be conduct an IT audit:

- Ascertain whether IT systems are adequately protected.
- Ascertain whether IT systems provide reliable information
- Evaluate the risk of data tampering and/or data loss.
- Ascertain whether IT systems are managed to achieve their intended benefits.

We can divide IT audits in to five categories.

1. Systems and Applications: Audits to verify that the systems and applications are appropriate, effective, and fully controlled to ensure that they are valid, reliable, timely, and securely entered, processed, and exited at all levels of system activity. Process and system assurance review is a sub-type that focuses on enterprise IT systems for business processes. These audits are designed to assist financial auditors.
2. Information Processing Facilities: Audit to verify that the processing facility is monitored to ensure that the request is processed quickly, accurately and efficiently under normal and potentially destructive conditions.
3. Systems Development: Audit to verify that the system being developed meets the organization's goals and to ensure that the system is developed in accordance with recognized system development standards.
4. Management of IT and Enterprise Architecture: Conduct audits to verify whether the IT department has developed organizational structures and procedures to ensure a controlled and effective environment to process information.
5. Client/Server, Telecommunications, Intranets, and Extranets: Audit to verify whether there are telecom controls on the client (computer receiving service), server, and the network connecting the client and server.

The process of performing an IT audit is summarized in the five steps below:

1. Determine the objective and scope of the IT audit.
2. Develop an audit plan to achieve the audit objectives.
3. Gather information on relevant IT systems, operations and related controls.
4. Perform audit tests on key IT controls, using Computer-Assisted Audit Techniques (CAATs), where appropriate.
5. Report on the audit findings.

For this project I am going to audit a website.

## Website Auditing

Website audit is a comprehensive analysis of all content related to the search visibility level of a website. A complete and detailed questionnaire will give you a better understanding of why your website is not generating the traffic you think it should be, or why your sales and conversions are not improving.

A comprehensive audit service will provide you with all feedback from technical issues to content. This type of website inspector will help you provide the best user experience for visitors and the best crawling experience for search engines.

Conducting a website review can benefit any business to increase its online influence. Site audits can identify problems with the website architecture. Therefore, the site will learn where to improve the technical performance of the site.

The website auditing process includes:

- User engagement
- User experience
- Traffic
- Functionality
- Site health
- Website performance

The website audit can be categorized into the following parts:

- **Site health audit:** Site status audits assess the site's architecture and usability. It also identifies possible gaps in content structure, technical gaps and website speed. In addition, discover new opportunities for key performance indicators
- **Website Security Audit:** One of the most important elements of website auditing is website security auditing. Identify the vulnerability as a security vulnerability. Security audits can avoid damaging the confidential information of the company or its visitors.

The company will receive a summary report that includes the differences found. It also provides a more effective correction method. Regular website reviews keep companies agile and consistent with Google's best practices.

Website review is an important measure to improve website efficiency and visibility. Auditing can improve Google's search rankings, while increasing website traffic and performance. Website auditing provides companies with rare online development opportunities.

I am going to audit Daraz.lk website in this project. Daraz.lk the premium online shopping site in Sri Lanka. Shop for trendy Clothes, Mobiles, Electronics & many more with great prices all across Sri Lanka.

## Audit Scope

Daraz is based on a marketplace model where all local sellers from top brands to SMEs, manufacturers and household entrepreneurs can set up their online shop, start building it and sell. 'Daraz.lk' is an e-commerce industry which has been in business for over 8 years in our country. 'Daraz.lk' is running successfully in the past eight years and achieved the success in its business performance and have a good reputation in market. Security is play a major role in the business in various ways in the success of the business. As the systems administrator of the 'Daraz.lk', it is my responsibility to make sure this company secure and preventing from the threats and vulnerabilities. As it is an e commerce industry, website is the most important thing in this business. We have to maintain the website well and with the better performance. Because all the local sellers and customers will access the website and they will do the transaction via the website. So website's security is very important and we have to make sure that often. So doing the website audit is helpful to make sure the security and the performance of the website and we can find the vulnerabilities and threats if there any. And the website audit ensures the proper user experience of the website visitors and the quality of the website. Moreover a proper website audit helps finding the tags, functionalities and navigations, and it should ensures the data protection also.

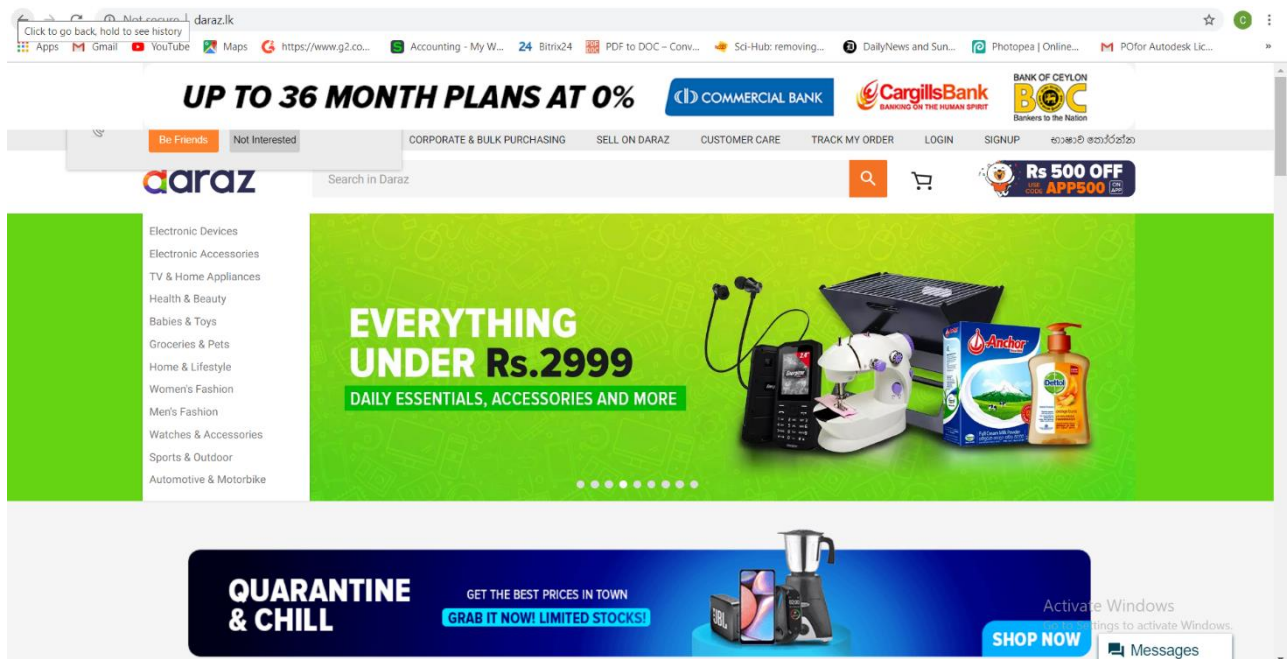


Figure 1 daraz.lk home page

## Audit Methodology

A good website audit takes into account all the factors that can influence your website's success: From your perspective and your customer's. Basically, a website audit helps you identify if your site is optimized in a way that helps you achieve goals associated with traffic and what areas you can improve upon to boost performance to hit those goals. I am going to use the online free tools to analyze and scan the website. And I am going to do this website audit in five parts.

1. Technical Audit
2. On-page SEO Audit
3. Off-page SEO Audit
4. User experience Audit
5. Content and Funnel Audit.

Technical audit of the website will provide with the information on how the ongoing technology is performing or not performing and how it is effects the other aspects of the site and how people use it. In this technical audit we have to check the SSL certificate and we have to check whether it is properly implemented and consistently implemented. And we need to check we are using the content management system to make the updates easy and consistent. And want to check the CMS settings whether it is changed or obscured all default settings, including the login page location. We want to make sure that our site use the best security practices, like denying access after several failed logins. And our site render right on all major browsers and mobile platforms and have we done the cross-browser testing and have we used Google mobile friendly test. We can check the recently updated software plugins and modules on our site. We can check the website logins. Contact forms and social media integrations are working as expected. And the website performs the regular backups correctly.

Next one is on-page SEO audit, when it comes to technology it uses and endorses, an enterprise can take months to make changes but on page SEO can be radically improved in as little as one day. On-page SEO consists all the factors on our website that influence our search placement. Every page on our site have the keyword optimized title tag and a Meta description and website have relevancy indicators including its business address, phone number, trust indicators including privacy policy and terms. We have to check the website us an XML sitemap to improve our pages indexing and crawl ability. Are we using readable, keyword enriched url structures and avoid the dynamic urls. And the content pages and images are optimized and usability using alt text and file names.

Off-page SEO audit is the most challenging part. There are many factors where you have only limited, indirect control, so it can be harder to move the needle on off-page SEO. Counting all the backlinks that point to a site remains one of the biggest problems in digital marketing. No matter what tools you use or how diligent you are, it's impossible to get the same view of your link portfolio that Google has. Off page SEO audit includes, how many total referring link to our website and how many backlinks do our content and landing pages have. Is our backlink portfolio is growing or shrinking over time.

Next is user experience audit, it refers to the ability of each user to find what they need on our website,

make use of it in the way we expect to, and develop positive associations with our site along the way. User experience is the place where design, technology and internet intersect to facilitate activity on our site. We have to make sure that our website pages are loading in less than three seconds on the average internet connection and does our site use minimal advertising that might interfere with content viewing, minimal obnoxious lead capture methods like 'eye-busters' and minimal JavaScript or at least load it asynchronously. And do us using the lossless compression to ensure that large graphics load more readily.

Finally will do the content and funnel audit. Quality content has become one of the most powerful forces for improving online visibility and building trust relationships with potential customers. As the core of the inbound marketing concept, the content is how you show your will and ability to add value to the prospective customer's life. We have to check that fully optimized landing pages with one page per product and service and all the major content pages include the relevant, engaging visual elements and attractive social sharing buttons and do content pages use personalization whenever appropriate.



## Website Audit Checklist

Category	Grade (A-F)	Priority Level (High, Medium, Low)
Marketing		
Strategies and goals are established.	A	High
Plan for measuring success is in place	C	Medium
Overall performance is growing	B	High
Audience has been defined	C	Low
Service level agreement indicates number of leads needed for sales.	A	High
Website Usability		
Site is responsive.	B	Medium
Page load speed is excellent.	A	High
Navigation is simple.	A	High
Website Effectiveness	B	High
Landing pages are built with relevant offers.	B	High
Current marketing strategies are generating enough traffic.	C	Medium
CTAs are placed on each page.	D	High
Lists are organized in the CRM.	C	High
Email marketing is effectively driving traffic.	B	High
Website Design		
Pages are consistent in format.	F	High
Content is easy to find.	D	Low
Content is easily digestible.	E	High
Design aligns with branding.	B	Medium
Images and text have continuity.	F	Medium
Conversion paths are clear to visitors.	B	Medium
Website Content		
Homepage describes your products and services.	C	High
Landing page content is enticing.	B	Medium
Headlines are creative and engaging.	B	Low
Blog content is educational and informative.	A	High
Site is free of duplicate content.	B	Medium
Content is free of errors.	C	Medium
Content is broken up with lists.	D	Medium
Serve resources from a consistent URL	F	High
Content includes relevant links	B	High
Serve scaled images	F	High
Leverage browser caching	F	High

Specify a cache validator	E	High
Defer parsing of JavaScript	B	High
Minimize redirects	B	High
Optimize images	B	High
Minify CSS	A	High
Website Security		
Site has a SSL certificate.	A	Medium
Software is updated, running on its latest version.	B	High
Vulnerabilities in server side software	A	High
Security issues regarding HTTP cookies	A	High
Client access policies	A	High
Secure Communication	A	High

I am going to use the online tools to audit the website. Here I attached the part of the analyze reports and results from the online tools.

First I am using the Qualys SSL labs Server test. This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet [2].

*Figure 2 Qualys SSL Labs SSL Server Test*

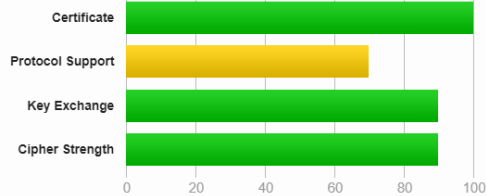
## SSL Report: www.daraz.lk (47.246.75.103)

Assessed on: Fri, 08 May 2020 04:11:02 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

## Certificate #1: RSA 2048 bits (SHA256withRSA)




### Server Key and Certificate #1

Subject	*.daraz.com
	Fingerprint SHA256: fa12290e8638c1f9f429da6c2d907bfb4b156cc97d7debbbc83dc07b6f3785a
	Pin SHA256: kbzwJZaBzObyBhvQoZGwsYNEWCgw2xninC5QddzuyvY=
Common names	*.daraz.com
Alternative names	*.daraz.com *.daraz.lk *.education.daraz.lk *.education.daraz.com.bd
	*.education.daraz.com.np *.alimebot.daraz.com *.education.daraz.pk
	*.sellercenter-staging.shop.com.mm daraz.pk *.x-space.daraz.com daraz.lk
	*.alimebot.daraz.com.bd *.alimebot.daraz.com.np *.education.shop.com.mm
	*.alimebot.daraz.pk *.alimebot.shop.com.mm *.sellercenter-
	staging.daraz.com.bd *.sellercenter-staging.daraz.com.np
	www.university.daraz.com.bd www.university.daraz.com.np
	*.sellercener.daraz.lk *.shop.com.mm *.sellercenter.daraz.com.bd
	*.sellercenter.daraz.com.np *.alimebot.daraz.lk *.sellercenter-staging.daraz.lk
	www.university.shop.com.mm www.university.daraz.pk *.sellercenter-
	staging.daraz.pk daraz.com.bd daraz.com.np *.daraz.com.bd *.daraz.com.np

## Server Key and Certificate #1

	*.sellercenter.daraz.pk shop.com.mm *.daraz.pk *.sellercenter.shop.com.mm *.sellercenter.daraz.lk www.university.daraz.lk daraz.com
Serial Number	6c6967c4152cb293c5992ed5
Valid from	Tue, 07 Apr 2020 02:34:42 UTC
Valid until	Thu, 08 Apr 2021 02:34:42 UTC (expires in 10 months and 30 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GlobalSign Organization Validation CA - SHA256 - G2 AIA: <a href="http://secure.globalsign.com/cacert/gsignorganizationvalsha2g2r1.crt">http://secure.globalsign.com/cacert/gsignorganizationvalsha2g2r1.crt</a>
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: <a href="http://crl.globalsign.com/gsignorganizationvalsha2g2.crl">http://crl.globalsign.com/gsignorganizationvalsha2g2.crl</a> OCSP: <a href="http://ocsp2.globalsign.com/gsignorganizationvalsha2g2">http://ocsp2.globalsign.com/gsignorganizationvalsha2g2</a>
Revocation status	Good (not revoked)
DNS CAA	No ( <a href="#">more info</a> )
Trusted	Yes Mozilla Apple Android Java Windows




## Additional Certificates (if supplied)

Certificates provided	2 (3648 bytes)
Chain issues	None

### #2

Subject	GlobalSign Organization Validation CA - SHA256 - G2 Fingerprint SHA256: 74ef335e5e18788307fb9d89cb704bec112abd23487dbff41c4ded5070f241d9 Pin SHA256: IQBnNBEiFuhj+8x6X8XLgh01V9Ic5/V3IRQLNFFc7v4=
Valid until	Tue, 20 Feb 2024 10:00:00 UTC (expires in 3 years and 9 months)
Key	RSA 2048 bits (e 65537)

### Additional Certificates (if supplied)

Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA
	

### Certification Paths

Mozilla

#### Path #1: Trusted

1	Sent by server	<p>*.daraz.com</p> <p>Fingerprint SHA256: fa12290e8638c1f9f429da6c2d907bfb4b156cc97d7debbec83dc07b6f3785a</p> <p>Pin SHA256: kbzwJZaBzObyBhvQoZGwsYNEWCgw2xninC5QddzuyvY=</p> <p>RSA 2048 bits (e 65537) / SHA256withRSA</p>
2	Sent by server	<p>GlobalSign Organization Validation CA - SHA256 - G2</p> <p>Fingerprint SHA256: 74ef335e5e18788307fb9d89cb704bec112abd23487dbff41c4ded5070f241d9</p> <p>Pin SHA256: IQBnNBEiFuhj+8x6X8XLgh01V9lc5/V3IRQLNFFc7v4=</p> <p>RSA 2048 bits (e 65537) / SHA256withRSA</p>
3	In trust store	<p>GlobalSign Root CA Self-signed</p> <p>Fingerprint SHA256: ebd41040e4bb3ec742c9e381d31ef2a41a48b6685c96e7cef3c1df6cd4331c99</p> <p>Pin SHA256: K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q=</p> <p>RSA 2048 bits (e 65537) / SHA1withRSA</p> <p>Weak or insecure signature, but no impact on root certificate</p>

## Certificate #2: EC 256 bits (SHA256withRSA)



### Server Key and Certificate #1

Subject	<p>*.daraz.com</p> <p>Fingerprint SHA256:</p> <p>b60a0f985ffee1b8dcd04a45b2e72e80dc52dcb37f358988ed14aed4d94fb56</p> <p>Pin SHA256: 7apX8H2PMdFB4j3NoKKJLTmM7wORGgqThV2v/a5KzOg=</p>
---------	--

## Server Key and Certificate #1

<b>Common names</b>	*.daraz.com *.daraz.com *.alimebot.daraz.com *.alimebot.daraz.com.bd *.alimebot.daraz.com.np *.alimebot.daraz.lk *.alimebot.daraz.pk *.alimebot.shop.com.mm *.daraz.com.bd *.daraz.com.np *.daraz.lk *.daraz.pk *.education.daraz.com.bd *.education.daraz.com.np *.education.daraz.lk *.education.daraz.pk *.education.shop.com.mm *.sellercener.daraz.lk *.sellercenter-staging.daraz.com.bd *.sellercenter-staging.daraz.com.np *.sellercenter-staging.daraz.lk *.sellercenter-staging.daraz.pk *.sellercenter-staging.shop.com.mm *.sellercenter.daraz.com.bd *.sellercenter.daraz.com.np *.sellercenter.daraz.lk *.sellercenter.daraz.pk *.sellercenter.shop.com.mm *.shop.com.mm *.x-space.daraz.com daraz.com.bd daraz.com.np daraz.lk daraz.pk shop.com.mm www.university.daraz.com.bd www.university.daraz.com.np www.university.daraz.lk www.university.daraz.pk www.university.shop.com.mm daraz.com
<b>Alternative names</b>	
<b>Serial Number</b>	4975c6ad807bb6c3219e8b31
<b>Valid from</b>	Tue, 07 Apr 2020 02:37:01 UTC
<b>Valid until</b>	Thu, 08 Apr 2021 02:34:42 UTC (expires in 10 months and 30 days)
<b>Key</b>	EC 256 bits
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	GlobalSign Organization Validation CA - SHA256 - G2 AIA: <a href="http://secure.globalsign.com/cacert/gsignorganizationvalsha2g2r1.crt">http://secure.globalsign.com/cacert/gsignorganizationvalsha2g2r1.crt</a>
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	CRL, OCSP CRL: <a href="http://crl.globalsign.com/gsignorganizationvalsha2g2.crl">http://crl.globalsign.com/gsignorganizationvalsha2g2.crl</a> OCSP: <a href="http://ocsp2.globalsign.com/gsignorganizationvalsha2g2">http://ocsp2.globalsign.com/gsignorganizationvalsha2g2</a>
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows



## Additional Certificates (if supplied)

Certificates provided	2 (3445 bytes)
Chain issues	None

#2

Subject	GlobalSign Organization Validation CA - SHA256 - G2 Fingerprint SHA256: 74ef335e5e18788307fb9d89cb704bec112abd23487dbff41c4ded5070f241d9 Pin SHA256: IQBnNBEiFuhj+8x6X8XLgh01V9Ic5/V3IRQLNFFc7v4=
Valid until	Tue, 20 Feb 2024 10:00:00 UTC (expires in 3 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA



## Certification Paths

Mozilla

### Path #1: Trusted

1	Sent by server	*.daraz.com Fingerprint SHA256: b60a0f985ffee1b8dcd04a45b2e72e80dc52dcb37f358988ed14aed4d94fb56 Pin SHA256: 7apX8H2PMdFB4j3NoKKJLTmM7wORGGqThV2v/a5KzOg= EC 256 bits / SHA256withRSA
2	Sent by server	GlobalSign Organization Validation CA - SHA256 - G2 Fingerprint SHA256: 74ef335e5e18788307fb9d89cb704bec112abd23487dbff41c4ded5070f241d9 Pin SHA256: IQBnNBEiFuhj+8x6X8XLgh01V9Ic5/V3IRQLNFFc7v4= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	GlobalSign Root CA Self-signed Fingerprint SHA256: ebd41040e4bb3ec742c9e381d31ef2a41a48b6685c96e7cef3c1df6cd4331c99 Pin SHA256: K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

## Configuration



## Protocols

TLS 1.3	No
<b>S 1.2</b>	<b>Yes</b>
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No



## Cipher Suites



### # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	<b>WEAK</b>		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	<b>WEAK</b>		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	<b>WEAK</b>		128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	<b>WEAK</b>		256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS <b>WEAK</b>	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	<b>WEAK</b>		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	<b>WEAK</b>		256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	<b>WEAK</b>		112



### # TLS 1.1 (suites in server-preferred order)



## Cipher Suites



# TLS 1.0 (suites in server-preferred order)



### Handshake Simulation

<a href="#">Android 2.3.7</a>	No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Android 4.0.4</a>		EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Android 4.1.1</a>		EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Android 4.2.2</a>		EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Android 4.3</a>		EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Android 4.4.2</a>		EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 5.0.0</a>		EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 6.0</a>		EC 256 (SHA256)	TLS 1.2 > spdy/3.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 7.0</a>		EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 8.0</a>		EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 8.1</a>		EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Android 9.0</a>		EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Baidu Jan 2015</a>		EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">BingPreview Jan 2015</a>		EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Chrome 49 / XP SP3</a>		RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Chrome 69 / Win 7</a>	R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

## Handshake Simulation

<a href="#">Chrome 70 / Win 10</a>	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Chrome 80 / Win 10</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Firefox 47 / Win 7</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Firefox 49 / XP SP3</a>	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Firefox 62 / Win 7</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Firefox 73 / Win 10</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Googlebot Feb 2018</a>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">IE 7 / Vista</a>	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">IE 8 / XP</a> No FS <sup>1</sup> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
<a href="#">IE 8-10 / Win 7</a> R	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">IE 11 / Win 7</a> R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">IE 11 / Win 8.1</a> R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">IE 10 / Win Phone 8.0</a>	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">IE 11 / Win Phone 8.1</a> R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">IE 11 / Win 10</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Edge 15 / Win 10</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Edge 16 / Win 10</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

## Handshake Simulation

<a href="#">Edge 18 / Win 10</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Edge 13 / Win Phone 10</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Java 6u45</a> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Java 7u25</a>	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Java 8u161</a>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Java 11.0.3</a>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Java 12.0.1</a>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">OpenSSL 0.9.8y</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">OpenSSL 1.0.1l</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">OpenSSL 1.0.2s</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">OpenSSL 1.1.0k</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">OpenSSL 1.1.1c</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Safari 6 / iOS 6.0.1</a>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
<a href="#">Safari 6.0.4 / OS X 10.8.4</a> <span>R</span>	EC 256 (SHA256)	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<a href="#">Safari 7 / iOS 7.1</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
<a href="#">Safari 7 / OS X 10.9</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
<a href="#">Safari 8 / iOS 8.4</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2 > spdy/3.1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
<a href="#">Safari 8 / OS X 10.10</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2 > spdy/3.1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
<a href="#">Safari 9 / iOS 9</a> <span>R</span>	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

## Handshake Simulation

<a href="#">Safari 9 / OS X 10.11</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Safari 10 / iOS 10</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Safari 10 / OS X 10.12</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Safari 12.1.2 / MacOS 10.14.6 Beta</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Safari 12.1.1 / iOS 12.3.1</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Apple ATS 9 / iOS 9</a> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">Yahoo Slurp Jan 2015</a>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<a href="#">YandexBot Jan 2015</a>	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS



### # Not simulated clients (Protocol mismatch)

[IE 6 / XP](#) No FS <sup>1</sup> No SNI <sup>2</sup> Protocol mismatch (not simulated)

(1) Clients that do not support Forward Secrecy (FS) are excluded w

(2) hen determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

**(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.**



## Protocol Details

DROWN

No, server keys and hostname not seen elsewhere with SSLv2

**(1) For a better understanding of this test, please read [this longer explanation](#)**

**(2) Key usage data kindly provided by the [Censys](#) network search engine; original DROWN website [here](#)**

## Protocol Details

	(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
<b>Secure Renegotiation</b>	<b>Supported</b>
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side ( <a href="#">more info</a> ) TLS 1.0: 0xc009
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Zombie POODLE	No ( <a href="#">more info</a> ) TLS 1.2: 0xc023
GOLDENDOODLE	No ( <a href="#">more info</a> ) TLS 1.2: 0xc023
OpenSSL 0-Length	No ( <a href="#">more info</a> ) TLS 1.2: 0xc023
Sleeping POODLE	No ( <a href="#">more info</a> ) TLS 1.2: 0xc023
<b>Downgrade attack prevention</b>	<b>Yes, TLS_FALLBACK_SCSV supported</b> ( <a href="#">more info</a> )
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )
ROBOT (vulnerability)	No ( <a href="#">more info</a> )
Forward Secrecy	With modern browsers ( <a href="#">more info</a> )
ALPN	Yes h2 spdy/3.1 http/1.1
NPN	Yes h2 spdy/3.1 http/1.1
<b>Session resumption (caching)</b>	<b>No (IDs assigned but not accepted)</b>
Session resumption (tickets)	Yes
OCSP stapling	No
<b>Strict Transport Security (HSTS)</b>	<b>Yes</b> max-age=31536000
HSTS Preloading	<b>Not in: Chrome Edge Firefox IE</b>
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )

### Protocol Details

Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	secp256r1
SSL 2 handshake compatibility	Yes



### + HTTP Requests

1 <https://www.daraz.lk/> (HTTP/1.1 200 OK)



### Miscellaneous

Test date	Fri, 08 May 2020 04:07:57 UTC
Test duration	184.997 seconds
HTTP status code	200
HTTP server signature	Tengine/Aserver
Server hostname	-

From these results we can find the details of the web server and the information about the certificates. The web server is supports to TLS 1 .0 and TLS 1.1. Here we can find the certificate details and certification validation details and keys. DNS CAA is not in the certificates and we can find the signature algorithm and protocol details.

Overall grade B is obtained by this analyze. From these analyze daraz.lk want to improve the protocol support.

Now I am going to check the SSL using the SSL checker tool. An SSL checker (Secure Sockets Layer checker) is a tool that verifies proper installation of an SSL certificate on a Web server. We can verify the SSL certificate on our web server to make sure it is correctly installed, valid, trusted and doesn't give any errors to any of our users [3].

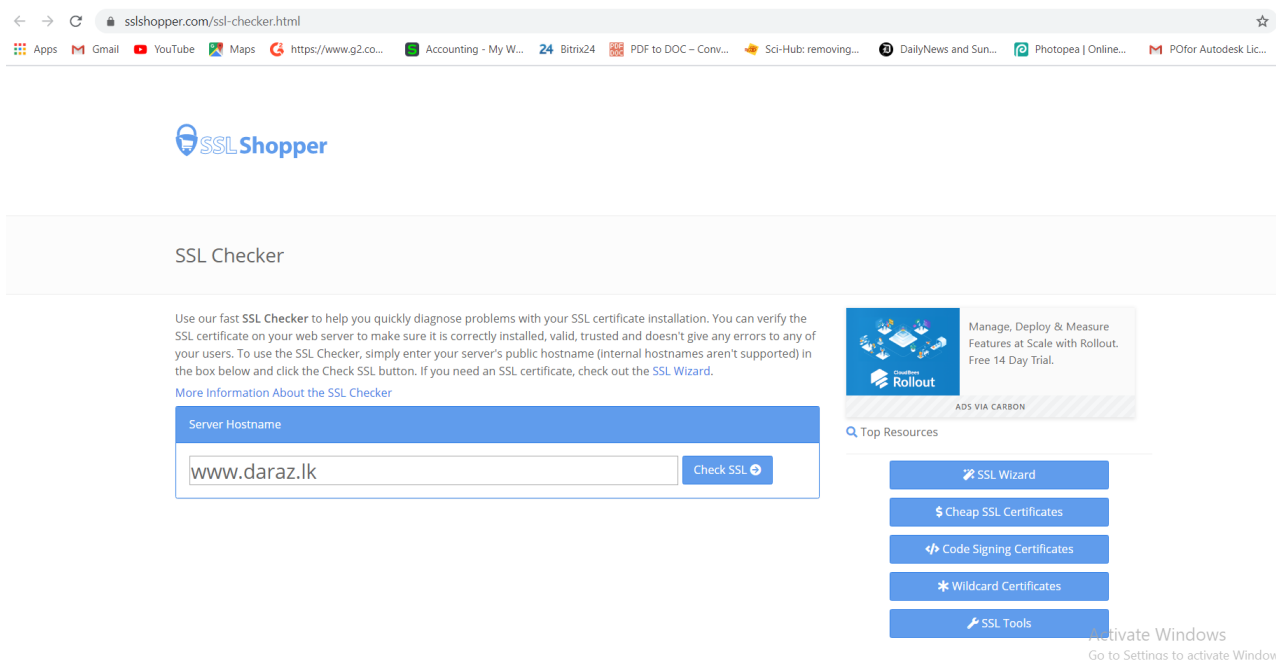


Figure 3 SSL Checker

Server Hostname

Check SSL

These results were cached from May 6, 2020, 11:03 pm PST to conserve server resources.  
 If you are diagnosing a certificate installation problem, you can get uncached results by [clicking here](#).

- ✓ **www.daraz.lk resolves to 47.246.32.12**
- ✓ **Server Type: Tengine/Aserver**
- ✓ **The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).**
- ✓ **The certificate was issued by GlobalSign.** [Write review of GlobalSign](#)
- ✓ **The certificate will expire in 334 days.** [Remind me](#)
- ✓ **The hostname (www.daraz.lk) is correctly listed in the certificate.**



**Common name:** \*.daraz.com

**SANs:** \*.daraz.com, \*.alimebot.daraz.com, \*.alimebot.daraz.com.bd, \*.alimebot.daraz.com.np, \*.alimebot.daraz.lk, \*.alimebot.daraz.pk, \*.alimebot.shop.com.mm, \*.daraz.com.bd, \*.daraz.com.np, \*.daraz.lk, \*.daraz.pk, \*.education.daraz.com.bd, \*.education.daraz.com.np, \*.education.daraz.lk, \*.education.daraz.pk, \*.education.shop.com.mm, \*.sellercenter.daraz.lk, \*.sellercenter-staging.daraz.com.bd, \*.sellercenter-staging.daraz.com.np, \*.sellercenter-staging.daraz.lk, \*.sellercenter-staging.daraz.pk, \*.sellercenter-staging.shop.com.mm, \*.sellercenter.daraz.com.bd, \*.sellercenter.daraz.com.np, \*.sellercenter.daraz.lk, \*.sellercenter.daraz.pk, \*.sellercenter.shop.com.mm, \*.shop.com.mm, \*.x-space.daraz.com, daraz.com.bd, daraz.com.np, daraz.lk, daraz.pk, shop.com.mm, www.university.daraz.com.bd, www.university.daraz.com.np, www.university.daraz.lk, www.university.daraz.pk, www.university.shop.com.mm, daraz.com

**Organization:** Alibaba (China) Technology Co., Ltd.

**Location:** HangZhou, Zhejiang, CN

**Valid from** April 6, 2020 to April 7, 2021

**Serial Number:** 4975c6ad807bb6c3219e8b31

**Signature Algorithm:** sha256WithRSAEncryption

**Issuer:** GlobalSign Organization Validation CA - SHA256 - G2



**Common name:** GlobalSign Organization Validation CA - SHA256 - G2

**Organization:** GlobalSign nv-sa

**Location:** BE

**Valid from** February 20, 2014 to February 20, 2024

**Serial Number:** 040000000001444ef04247

**Signature Algorithm:** sha256WithRSAEncryption

**Issuer:** GlobalSign Root CA

From these details we can check the SSL and certificate details. www.daraz.lk is resolves to 47.246.32.12 and the server type is Tengine. And the SSL certificate is trusted and correctly installed and the certificate is issued by GlobalSign and the certificate will expire in 334 days. Hostname also correctly listed in the certificate.

Now I am going to use the GTmetrix tool to see the website performance and how to optimize the site. GTmetrix is a free tool that analyzes our page's speed performance. Using Page Speed and YSlow, GTmetrix generates scores for our pages and offers actionable [4].



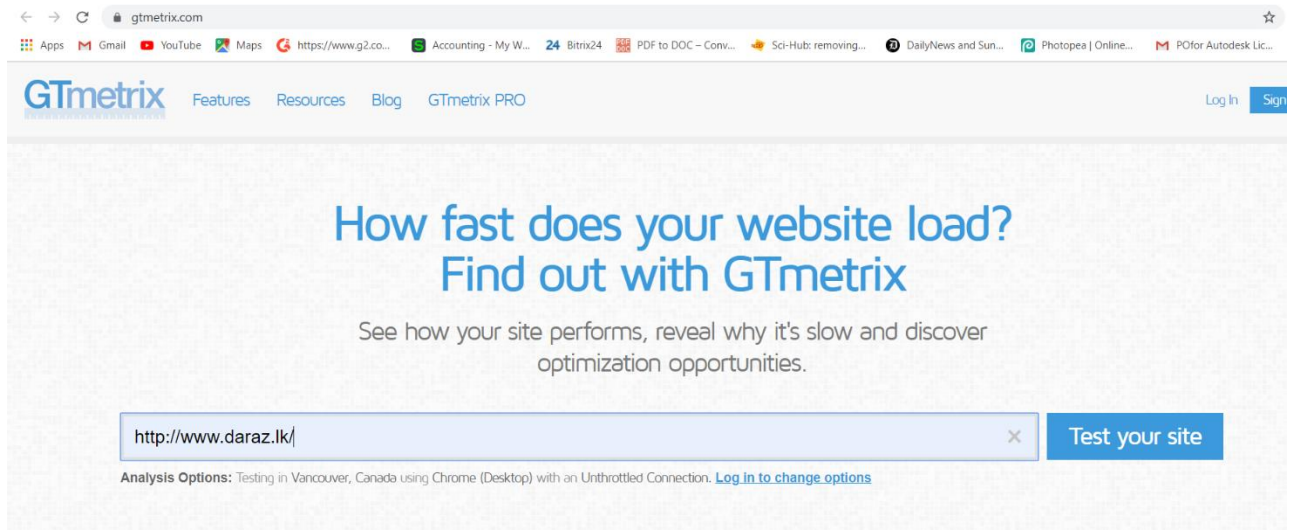
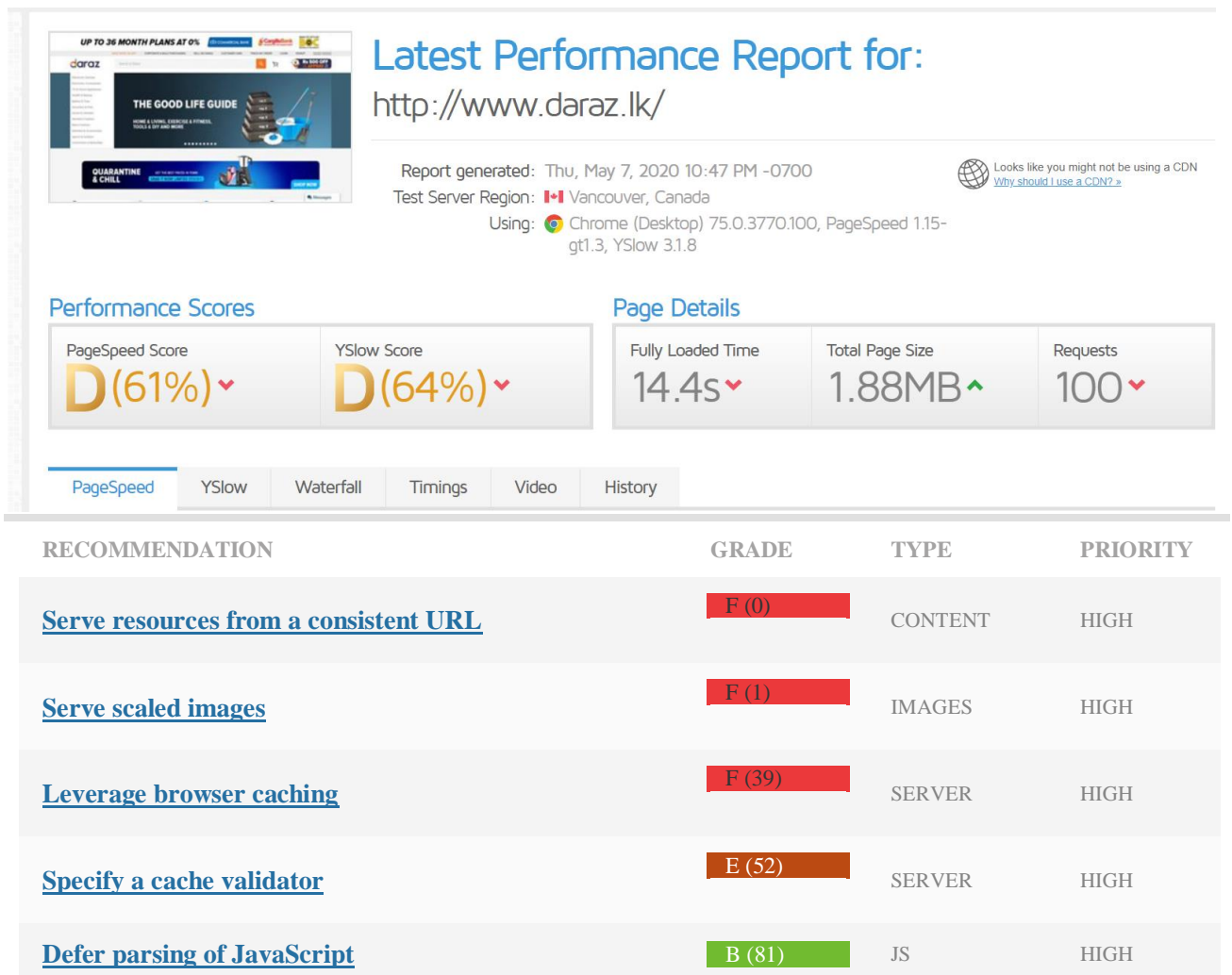


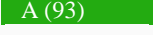

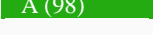
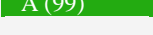
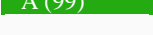

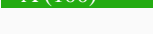


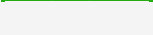

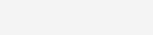

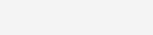

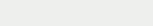


Figure 4 GTmetrix



RECOMMENDATION	GRADE	TYPE	PRIORITY
<a href="#"><u>Minimize redirects</u></a>	 B (83)	CONTENT	HIGH
<a href="#"><u>Optimize images</u></a>	 B (85)	IMAGES	HIGH
<a href="#"><u>Minify JavaScript</u></a>	 A (93)	JS	HIGH
<a href="#"><u>Minimize request size</u></a>	 A (98)	CONTENT	HIGH
<a href="#"><u>Specify image dimensions</u></a>	 A (98)	IMAGES	MEDIUM
<a href="#"><u>Minify CSS</u></a>	 A (99)	CSS	HIGH
<a href="#"><u>Enable compression</u></a>	 A (99)	SERVER	HIGH
<a href="#"><u>Avoid bad requests</u></a>	 A (100)	CONTENT	HIGH
<a href="#"><u>Avoid landing page redirects</u></a>	 A (100)	SERVER	HIGH
<a href="#"><u>Enable Keep-Alive</u></a>	 A (100)	SERVER	HIGH
<a href="#"><u>Inline small CSS</u></a>	 A (100)	CSS	HIGH
<a href="#"><u>Inline small JavaScript</u></a>	 A (100)	JS	HIGH
<a href="#"><u>Put CSS in the document head</u></a>	 A (100)	CSS	HIGH
<a href="#"><u>Combine images using CSS sprites</u></a>	 A (100)	IMAGES	HIGH
<a href="#"><u>Avoid CSS @import</u></a>	 A (100)	CSS	MEDIUM
<a href="#"><u>Prefer asynchronous resources</u></a>	 A (100)	JS	MEDIUM
<a href="#"><u>Specify a character set early</u></a>	 A (100)	CONTENT	MEDIUM
<a href="#"><u>Avoid a character set in the meta tag</u></a>	 A (100)	CONTENT	LOW

Now I am going to analyze the SEO performance of the website. And I am using the site checker online tool to do this analyze. SiteChecker is a SEO optimization tool, which we can use to get our rankings pushed to the top of Google SERP. Although it largely depends on the SEO expert we are hiring, but SiteChecker is definitely the tool that the expert needs to provide our website the acknowledgment it deserves [5].

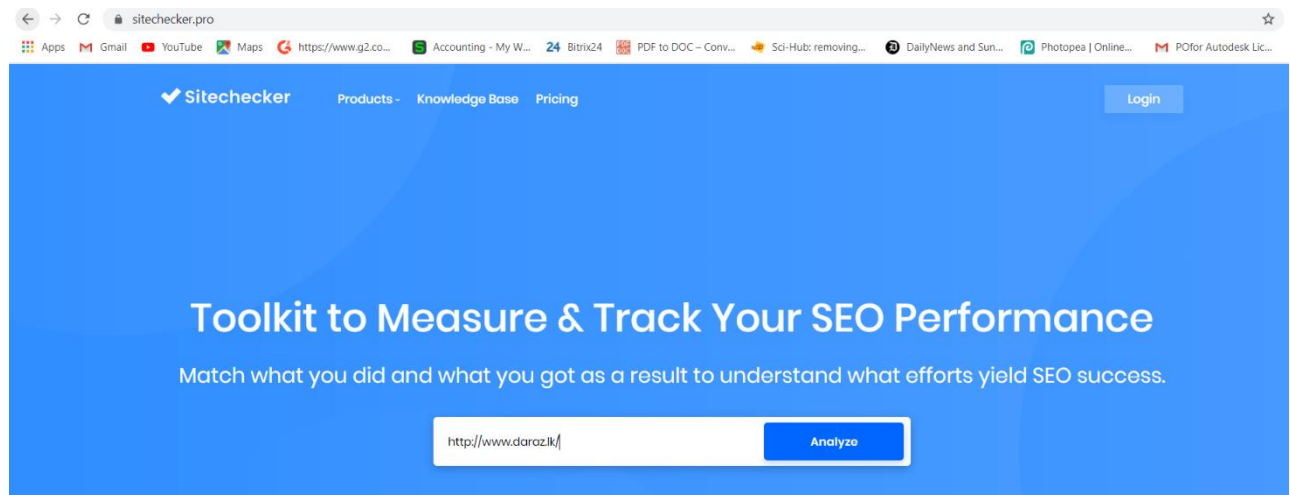
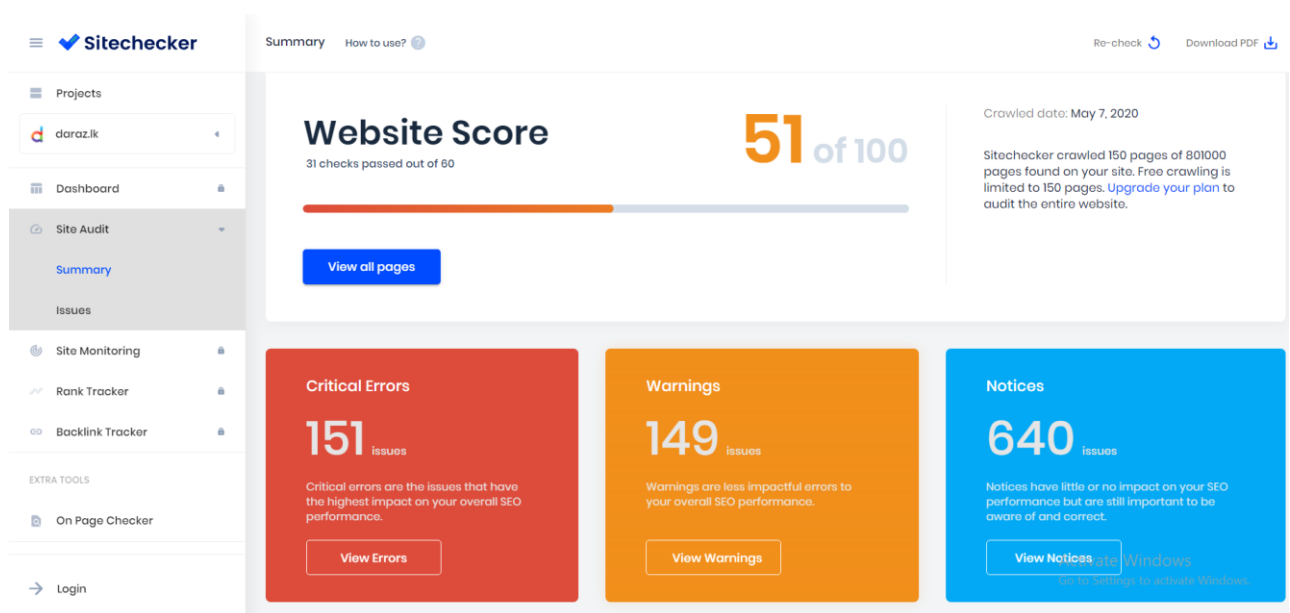


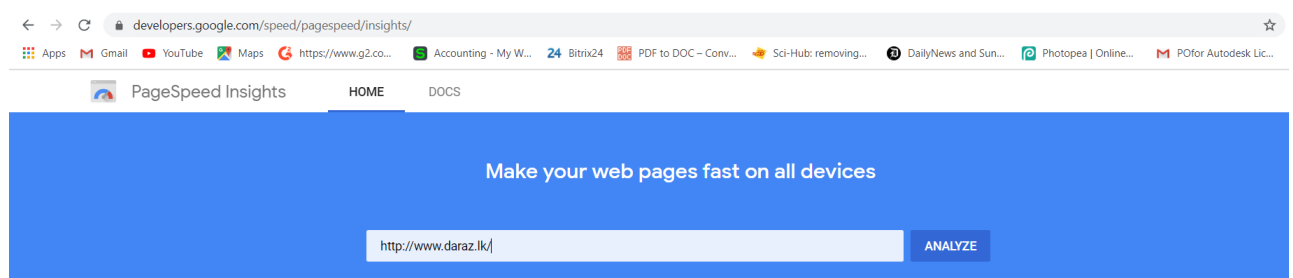
Figure 5 Sitechecker



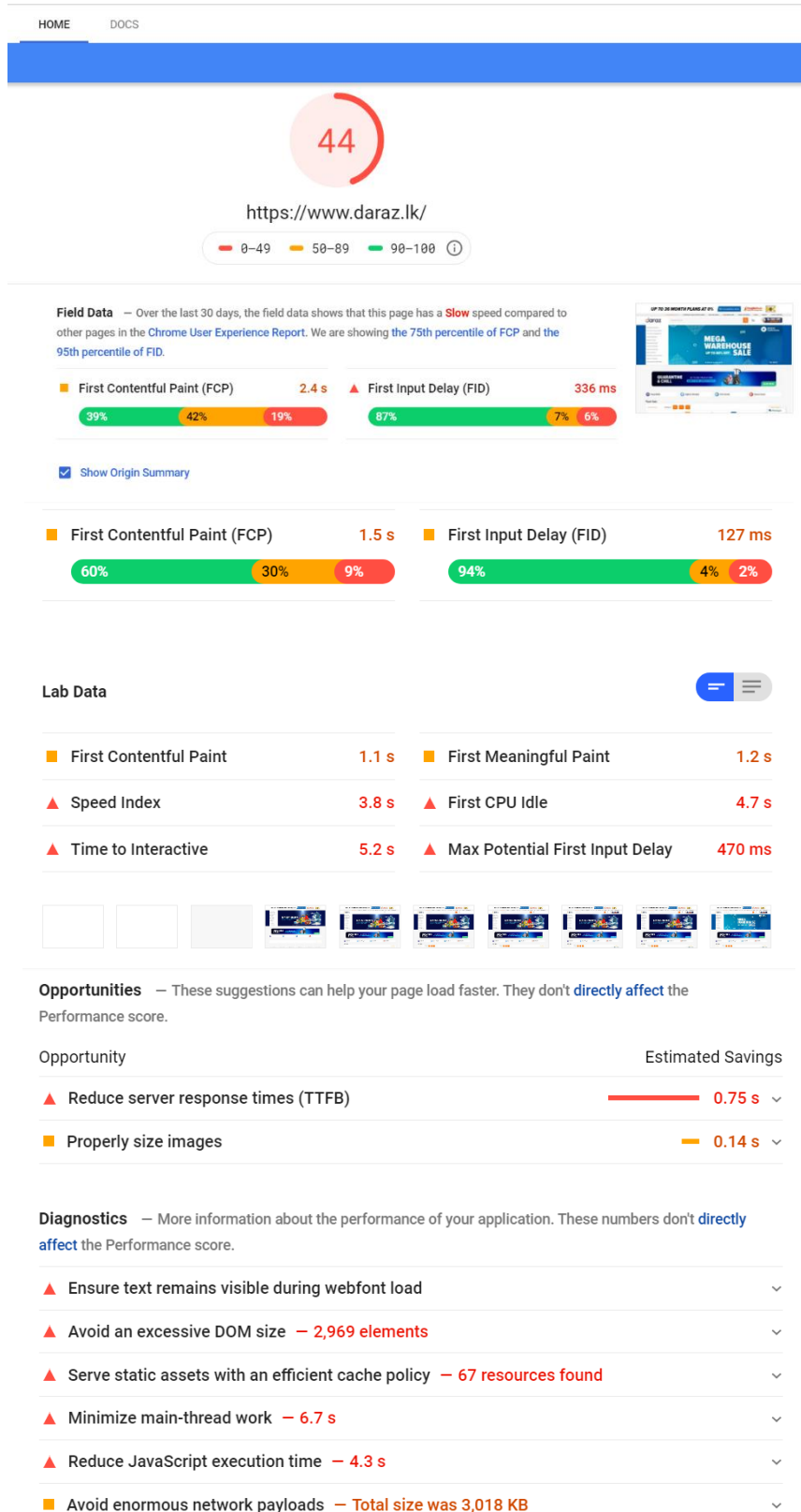
Here is a list of all technical issues Sitecheckerbot has found on the website. Start fix them step by step from the most critical errors to less important. When you finished fixing issues, recrawl the website to make sure Website Score is up.

More than one H1 on page: 2 pages
More than one Title tag on page: 148 pages
H1 is missing: 1 page
Open Graph tags incomplete: 145 pages
Canonical ≠ URL: 3 pages
4xx Client errors: 1 page
Twitter card missing: 148 pages
Code Ratio < 10%: 148 pages
Description too long: 1 page
Title too long: 52 pages
Meta Nofollow Pages: 145 pages
Meta Noindex Pages: 145 pages
301 Redirects: 1 page

Now I am going check the performance of the website using another online tool named PageSpeed Insights. PageSpeed Insights is an online tool which helps in identifying performance best practices on any given website, provides suggestions on a webpage's optimizations, and suggests overall ideas of how to make a website faster. This tool can be accessed directly in any browser [6].



*Figure 6 PageSpeed Insights*



● Avoid chaining critical requests — 16 chains found	▼
● Keep request counts low and transfer sizes small — 111 requests • 3,018 KB	▼
Passed audits (14)	
● Eliminate render-blocking resources — Potential savings of 0 ms	▼
● Defer offscreen images — Potential savings of 175 KB	▼
● Minify CSS	▼
● Minify JavaScript — Potential savings of 8 KB	▼
● Remove unused CSS — Potential savings of 24 KB	▼
● Efficiently encode images	▼
● Serve images in next-gen formats — Potential savings of 98 KB	▼
● Enable text compression	▼
● Preconnect to required origins	▼
● Avoid multiple page redirects — Potential savings of 190 ms	▼
● Preload key requests	▼
● Use video formats for animated content	▼
● User Timing marks and measures	▼
● Minimize third-party usage — Third-party code blocked the main thread for 0 ms	▼

Finally, I am going to use the Pentest-tool. It is a website vulnerability scanning tool. This tool finds common vulnerabilities which affect web applications: SQL Injection, XSS, OS Command Injection, Directory Traversal and others. The scanner also identifies specific web server configuration issues [7].

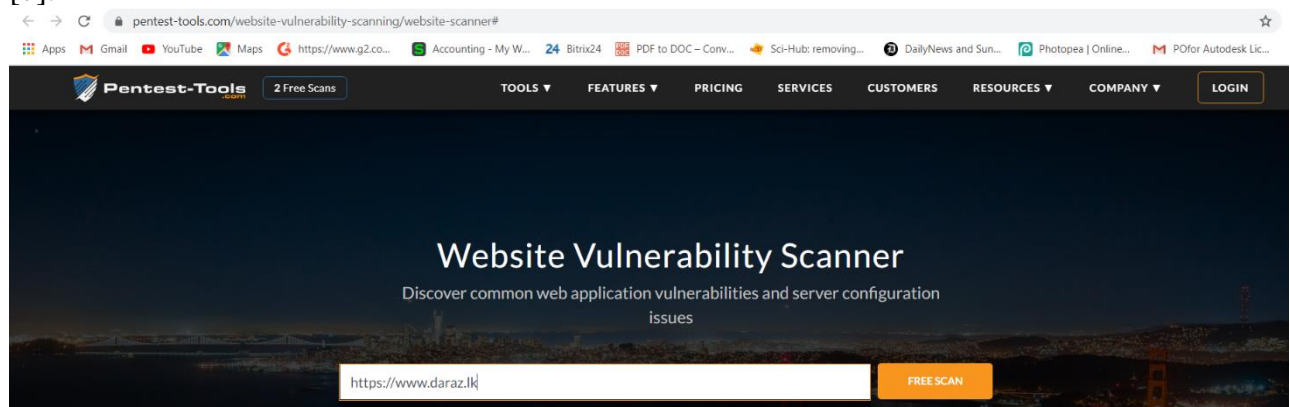


Figure 7 pentest tool

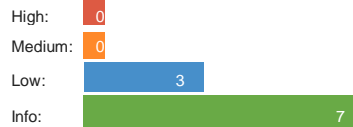
# Website Vulnerability Scanner Report (Light)

## Summary

### Overall risk level:

Low

### Risk ratings:



### Scan information:

Start time: 2020-05-07 11:37:04 UTC+03  
Finish time: 2020-05-07 11:37:20 UTC+03  
Scan duration: 16 sec  
Tests performed: 10/10  
Scan status: **Finished**

## Findings

### Server software and technology found

Software / Version	Category
Tengine	Web Servers

#### Details

#### Risk description:

An attacker could use this information to mount specific attacks against the identified software type and version.

#### Recommendation:

We recommend you to eliminate the information which permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

More information about this issue:

[https://www.owasp.org/index.php/Fingerprint\\_Web\\_Server\\_\(OTG-INFO-002\)](https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002)).

### Missing HTTP security headers

HTTP Security Header	Header Role	Status
X-Frame-Options	Protects against Clickjacking attacks	Not set
X-XSS-Protection	Mitigates Cross-Site Scripting (XSS) attacks	Not set
X-Content-Type-Options	Prevents possible phishing or XSS attacks	Not set

#### Details

#### Risk description:

Because the **X-Frame-Options** header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:

<https://www.owasp.org/index.php/Clickjacking>

The **X-XSS-Protection** HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

The HTTP **X-Content-Type-Options** header is addressed to Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

**Recommendation:**

We recommend you to add the **X-Frame-Options** HTTP response header to every page that you want to be protected against Clickjacking attacks.

More information about this issue:

[https://www.owasp.org/index.php/Clickjacking\\_Defense\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet)

We recommend setting the **X-XSS-Protection** header to "X-XSS-Protection: 1; mode=block".

More information about this issue:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection>

We recommend setting the **X-Content-Type-Options** header to "X-Content-Type-Options: nosniff".

More information about this issue:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

## Robots.txt file found

<https://www.daraz.lk/robots.txt>

### Details

**Risk description:**

There is no particular security risk in having a robots.txt file. However, this file is often misused to try to hide some web pages from the users. This should not be done as a security measure because these URLs can easily be read from the robots.txt file.

**Recommendation:**

We recommend you to remove the entries from robots.txt which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

More information about this issue:

<https://www.theregister.co.uk/2015/05/19/robotstxt/>

No vulnerabilities found for server-side software

No security issue found regarding HTTP cookies

Communication is secure

No security issue found regarding client access policies

Directory listing not found (quick scan)

No password input found (auto-complete test)

No password input found (clear-text submission test)



## References

- [1] Information technology audit [online]  
[https://en.wikipedia.org/wiki/Information\\_technology\\_audit](https://en.wikipedia.org/wiki/Information_technology_audit) [Accessed 02-May-2020]
- [2] SSL Server Test [online] <https://www.ssllabs.com/ssltest/> [Accessed 02-May-2020]
- [3] SSL Checker [online] <https://www.sslshopper.com/ssl-checker.html> [Accessed 04 -May-2020]
- [4] GTmetrix [online] <https://gtmetrix.com/> [Accessed 04-May-2020]
- [5] Sitechecker [online] <https://sitechecker.pro/> [Accessed 04-May-2020]
- [6] PageSpeed Insights [online] <https://developers.google.com/speed/pagespeed/insights/> [Accessed 04-May-2020]
- [7] pentest-tools [online] <https://pentest-tools.com/website-vulnerability-scanning/website-scanner#>  
[Accessed 04-May-2020]