

Introduction to the Tool & Company

Our The Mozilla HTTP Observatory is a set of tools to analyse your website and inform you if you are utilizing the many available methods to secure it. Observatory is a tool that is geared towards informing website owners of best practices for securing their sites, covering everything from personal blogs to eCommerce.

The tool uses a scoring system to determine how vulnerable or how well implemented security is on your website.


It is split into three projects:

- http-observatory - scanner/grader
- observatory-cli - command line interface
- http-observatory-website - web interface
-

Scanning sites with the HTTP Observatory can be scanned using:


- observatory.mozilla.org - the online interface
- observatory-cli - the official node.js command line interface
- java-http-observatory-api - a third party java library and command line interface

Screenshots


[Home](#)
[FAQ](#)
[Statistics](#)
[About](#)

[HTTP Observatory](#)
[TLS Observatory](#)
[SSH Observatory](#)
[Third-party Tests](#)

Scan Summary



Host:	www.bhadrinar.com
Scan ID #:	25432838 (unlinked)
Start Time:	March 28, 2022 3:45 PM
Duration:	3 seconds
Score:	30/100
Tests Passed:	7/11

Recommendation

Initiate Rescan

Wondering where to start?

Adding HTTPS protects your site's visitors from tracking, malware, and injected advertising.

Many services and certificate authorities now provide free HTTPS and digital certificates to make this as painless as possible!

- [Mozilla TLS Guidelines](#)
- [Mozilla TLS Configuration Generator](#)


Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-75	Content Security Policy (CSP) header not implemented	①
Cookies	✓	0	All cookies use the <code>Secure</code> flag and all session cookies use the <code>HttpOnly</code> flag	①
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) filters or headers	①
HTTP Public Key Pinning	—	0	HTTP Public Key Pinning (HPKP) header cannot be set, as site contains an invalid certificate chain (optional)	①
HTTP Strict Transport Security	✗	-70	HTTP Strict Transport Security (HSTS) header cannot be set, as site contains an invalid certificate chain	①
Redirection	✗	-70	Does not redirect to an HTTPS site	①
Referrer Policy	—	0	Referrer-Policy header not implemented (optional)	①
Subresource Integrity	—	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	①
X-Content-Type-Options	✗	-3	X-Content-Type-Options header not implemented	①
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to <code>SAMEORIGIN</code> or <code>DENY</code>	①
X-XSS-Protection	✓	0	X-XSS-Protection header set to <code>1; mode=block</code>	①

Cookies						
Name	Expires	Path	Secure	HttpOnly	SameSite	Prefixed
pleak_ext_social_login_jwt-session	Session	/	✓	✓	✗	✗

Grade History		
Date	Score	Grade
March 23, 2022 3:21 PM	30	D

[illegible]




[Home](#)
[FAQ](#)
[Statistics](#)
[About](#)

[HTTP Observatory](#)
[TLS Observatory](#)
[SSH Observatory](#)
[Third-party Tests](#)

This site uses an untrusted or invalid certificate. The following results ignore this error:

Scan Summary



Host:	www.bkdrfishar.com (43.248.68.26)
Scan ID #:	4964773
End Time:	March 28, 2022 1:43 PM
Compliance Level:	Non-compliant

Please note that non-compliance simply means that the server's configuration is either more or less strict than a pre-defined Mozilla configuration level.

Certificate Expiry: 58578622

Certificate Information	
Common name:	ssl-blackbox.45-178-61-76.plnck.page
Alternative Names:	ssl.blackbox.45-178-61-76.plnck.page
First Observed:	2022-09-23 (certificate #1807/9602)
Valid From:	2022-09-30
Valid To:	2022-09-01
Key:	RSA 2048 bits
Issuer:	R1
Signature Algorithm:	SHA256WithRSA

Cipher Suite	Code	Key size	AEAD	EPS	Protocols
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x27	2048 bits	✓	✓	TLS 1.2
ECDFHE-RSA-AES128-GCM-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.3
DHE-RSA-AES128-GCM-SHA256	0x0B 0x29	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES128-GCM-SHA384	0x0B 0x31	2048 bits	✓	✓	TLS 1.3
ECDHE-RSA-AES256-SHA256	0x0C 0x27	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.3
DHE-RSA-AES256-SHA256	0x0B 0x27	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES256-SHA384	0x0B 0x30	2048 bits	✓	✓	TLS 1.3
ECDFHE-RSA-AES192-SHA	0x0C 0x2A	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
ECDHE-RSA-AES192-SHA	0x0C 0x2A	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-AES192-SHA	0x0B 0x25	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-AES256-SHA	0x0B 0x29	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
ECDHE-RSA-CAMELLIA256-SHA256	0x0C 0x27	2048 bits	✗	✓	TLS 1.2
ECDFHE-RSA-CAMELLIA192-SHA256	0x0C 0x3A	2048 bits	✗	✓	TLS 1.3
DHE-RSA-CAMELLIA256-SHA256	0x0B 0x3A	2048 bits	✗	✓	TLS 1.3
DHE-RSA-CAMELLIA192-SHA	0x0B 0x26	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-CAMELLIA256-SHA	0x0B 0x28	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-CAMELLIA192-SHA	0x0B 0x25	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES128-GCM-SHA256	0x0B 0x2C	2048 bits	✓	✗	TLS 1.2
RSA-AES128-GCM-SHA384	0x0B 0x35	2048 bits	✓	✗	TLS 1.3
RSA-AES192-SHA256	0x0C 0x2C	2048 bits	✗	✗	TLS 1.3
RSA-AES256-SHA256	0x0B 0x2D	2048 bits	✗	✗	TLS 1.2
RSA-AES192-SHA	0x0B 0x26	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES256-SHA	0x0B 0x28	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-CAMELLIA256-SHA256	0x0B 0x3A	2048 bits	✗	✗	TLS 1.2
RSA-CAMELLIA192-SHA256	0x0B 0x3B	2048 bits	✗	✗	TLS 1.3
RSA-CAMELLIA256-SHA	0x0B 0x28	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-CAMELLIA192-SHA	0x0B 0x25	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0

Miscellaneous Information	
CAA Record:	No (?)
Cipher Preference:	Server selects preferred cipher (?)
Compatible Clients:	Android 3.0-7, Apple ATG 6, Baidu Jan 7013, BingBot Feb 7013, BingPreview Feb 7013, Chrome 72, Fido 19, Firefox 101, Googlebot Oct 2013, IE 11, JZRM 6013, Openbot 0.0.0.0, Opera 12.10, Safari 5, Tor 1.0.0, Yahoo Slurp Oct 2012, YandexBot May 2014
OCSP Stapling:	No (?)

Suggestions

Looking for improved security and have a user base of only modern clients?

Take a look at the [Mozilla "Modern" TLS configuration](#): It provides an extremely high level of security and performance and is compatible with all clients released in the last couple years. It is not recommended for general purpose websites that may need to service older clients such as Android 4.x, Internet Explorer 10, or Java 6.x.

Still want secure website, but need compatibility with those older clients?

No problem! The Mozilla "intermediate" TLS configuration may be just right for you! It provides the similar level of security to the "Modern" configuration when used with current clients, but still supports older versions of web browsers and tools.

Please note that these suggestions may not be appropriate for your particular usage requirements! If they do sound like something you'd like assistance with, then holla on board!

Teleport me to Mozilla's configuration generator!

Conclusion

In this test, we took a look at Observatory by Mozilla, which is a free online service performs a deep analysis of website vulnerabilities. The tool also scans and rates the implementation of TLS on the website. It will check the certificate information and cipher suites used. While Observatory's TLS scan is not as robust as the Qualys SSL Labs SSL Server Test, it does integrate this test as a third-party scanner, along with other tools. After correctly configuring the security settings on your website, we will get a result. By utilizing tools like Mozilla Observatory, you can gain some level of assurance that your site's information is safe, but it's important to ensure that you are regularly monitoring your security and keeping your systems up to date to address any new concerns that arise.

Certificate

