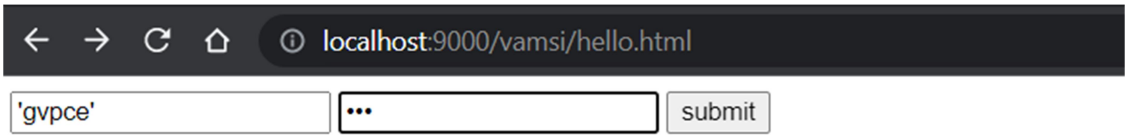
1.SQL INJECTION

AIM: - Exploit SQL injection flaws on a sample website.

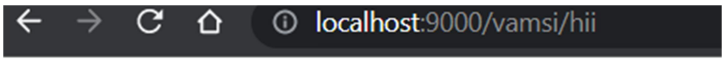
Case 1: - correct credentials

Input: - name=’gvpce’

Password=’nsc’



Output: -

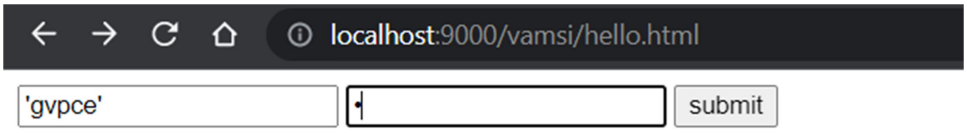


Welcome to you gvpce password = nsc

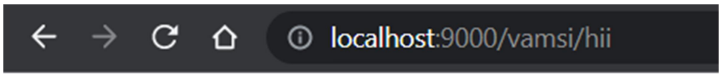
Case 2: - Invalid credentials

Username = ‘gvpce’

Password = n



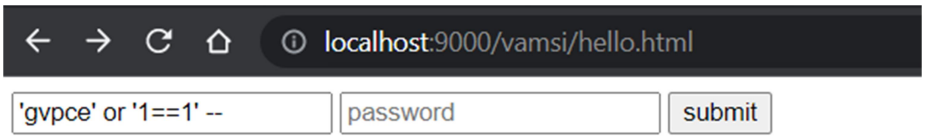
Output: -



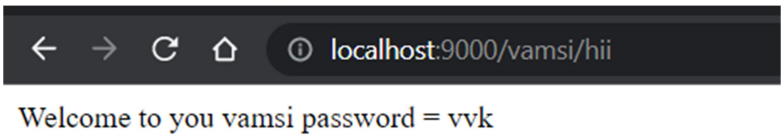
Sorry Incorrect Entry

Case 3: - Injecting sql commands to login without password

Name = ‘gvpce’ or ‘1==1’ --

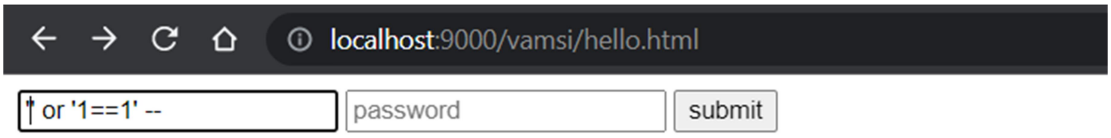


Output: -

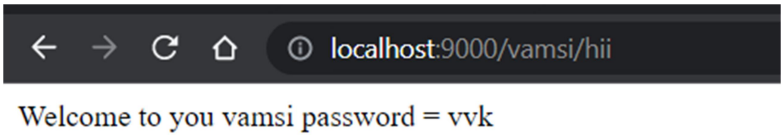


Case 4: - Injecting sql command to login without username and password

Name= ‘ ‘’ or ‘1==1’ –



Output: -

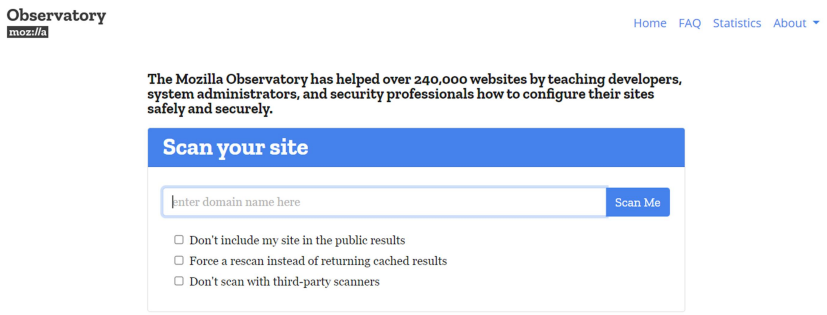


2.WEB SECURITY ANALYSIS

AIM: - Perform web security analysis on a sample website

PROCEDURE: -

Step1: - Visit https://observatory.mozilla.org/.



Step2: - Enter the URL of the website you want to perform web security analysis.

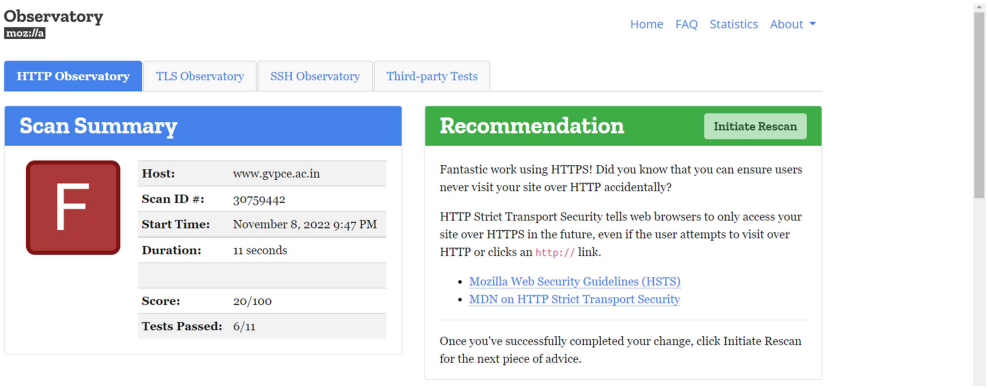
Step3: - You can observe the results by clicking on the scan me button.

Results: -

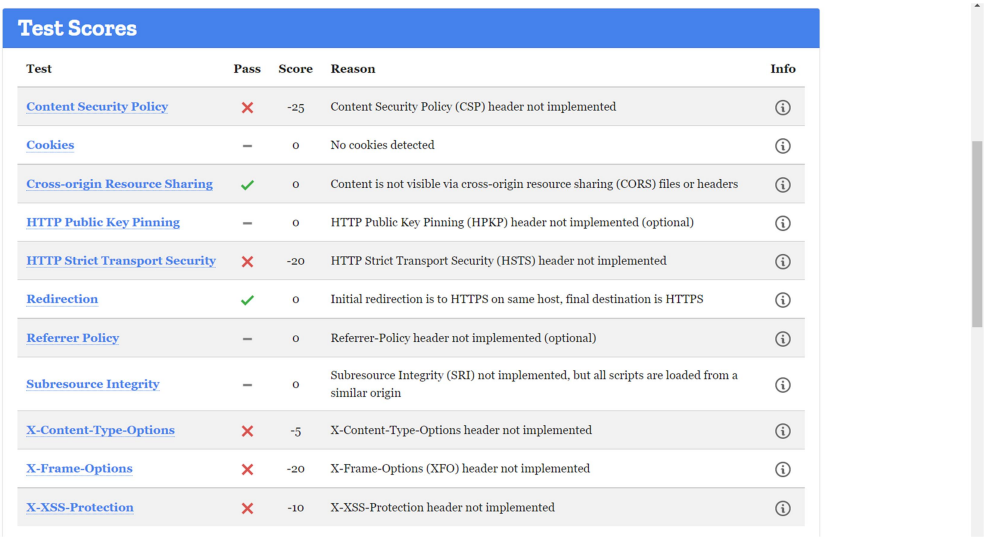
Http observatory

It performs all the Hyper text transmission protocols tests and evaluates for a score of 100

And performs 11 different testcases and shows how many testcases has been successfully executed.



It also shows which testcases has been succesfully passed and score for it.



Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	
Cookies	–	0	No cookies detected	
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented	
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented	
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	

TLS observatory

- Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network.
- It shows the compatibility level as secure or Insecure by performing relevant tests on the url provided.

Observatory
moz://a

Home FAQ Statistics About

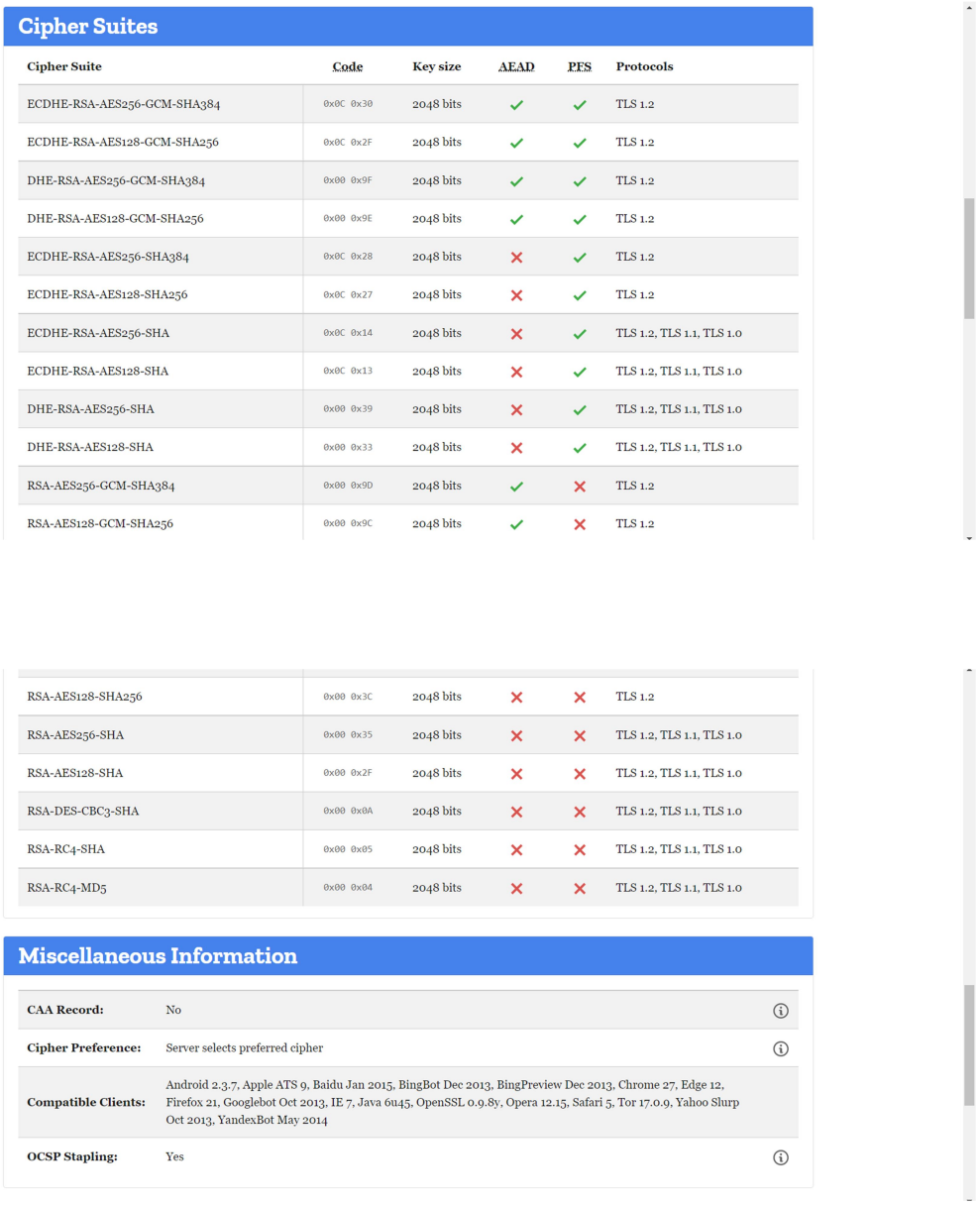
HTTP Observatory | TLS Observatory | SSH Observatory | Third-party Tests

Scan Summary

F

Host:	www.gvpce.ac.in (123.108.201.250)
Scan ID #:	52058719
End Time:	November 8, 2022 9:47 PM
Compatibility Level:	Insecure
Certificate Explainer:	188910661

- It also displays the cipher suites of different cipher suite.
- It also displays the code, key size, AEAD, PFS and protocols.
- Some miscellaneous information like CAA records, Cipher reference, Compatible clients and OSCP Stapling.



Cipher Suites

Cipher Suite	Code	Key size	AEAD	PFS	Protocols
ECDHE-RSA-AES256-GCM-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x2F	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES256-GCM-SHA384	0x00 0x9F	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES128-GCM-SHA256	0x00 0x9E	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-SHA384	0x0C 0x28	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES128-SHA256	0x0C 0x27	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA	0x0C 0x14	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
ECDHE-RSA-AES128-SHA	0x0C 0x13	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-AES256-SHA	0x00 0x39	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-AES128-SHA	0x00 0x33	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES256-GCM-SHA384	0x00 0x9D	2048 bits	✓	✗	TLS 1.2
RSA-AES128-GCM-SHA256	0x00 0x9C	2048 bits	✓	✗	TLS 1.2
RSA-AES128-SHA256	0x00 0x3C	2048 bits	✗	✗	TLS 1.2
RSA-AES256-SHA	0x00 0x35	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES128-SHA	0x00 0x2F	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-DES-CBC3-SHA	0x00 0x0A	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-RC4-SHA	0x00 0x05	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-RC4-MD5	0x00 0x04	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 2.3.7, Apple ATS 9, Baidu Jan 2015, BingBot Dec 2013, BingPreview Dec 2013, Chrome 27, Edge 12, Firefox 21, Googlebot Oct 2013, IE 7, Java 6u45, OpenSSL 0.9.8y, Opera 12.15, Safari 5, Tor 17.0.9, Yahoo Slurp Oct 2013, YandexBot May 2014
OCSP Stapling:	Yes

3rd Party tests

There are some 3rd party test been performed by observatory mozilla

- Transport Layer Security
- Http header and content security

HTTP Observatory | TLS Observatory | SSH Observatory | **Third-party Tests**

Transport Layer Security

ssllabs.com

B

Host:	www.gvpce.ac.in
Complete Results:	https://www.ssllabs.com/ssltest/analyze?d=www.gvpce.ac.in

QUALYS SSL LABS

ImmuniWeb

C

Host:	www.gvpce.ac.in (123.108.201.250)
Score:	30/100
PCI-DSS:	Non-compliant
HIPAA:	Non-compliant
NIST:	Non-compliant
DROWN:	Not vulnerable
Heartbleed:	Not vulnerable
Insecure Renegotiation:	Not vulnerable
OpenSSL ChangeCipherSpec:	Not vulnerable
OpenSSL Padding Oracle:	Not vulnerable
Poodle (SSLv3):	Not vulnerable
Poodle (TLS):	Not vulnerable

HTTP Headers & Content Security

securityheaders.com

F

Host:	www.gvpce.ac.in
Complete Results:	https://securityheaders.com/?followRedirects=on&hide=on&q=www.gvpce.ac.in

Miscellaneous

hstspreload.org

X

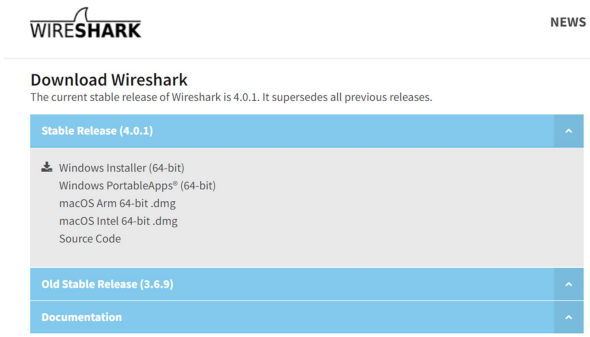
Host:	www.gvpce.ac.in
Preloaded:	No
Notes:	• Domain is a subdomain, and can't be preloaded. • Site doesn't issue an HSTS header.
Complete Results:	https://hstspreload.org?domain=www.gvpce.ac.in

3.SNIFFING ROUTER TRAFFIC

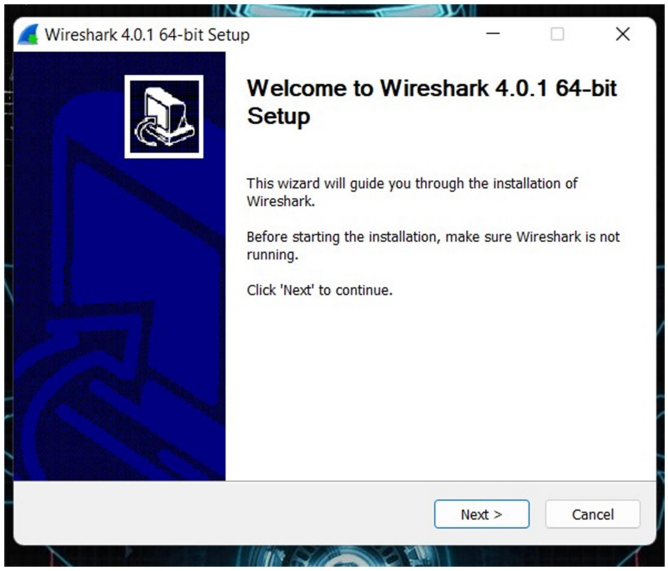
AIM: - Demonstrate how to sniff for router traffic on a sample network.

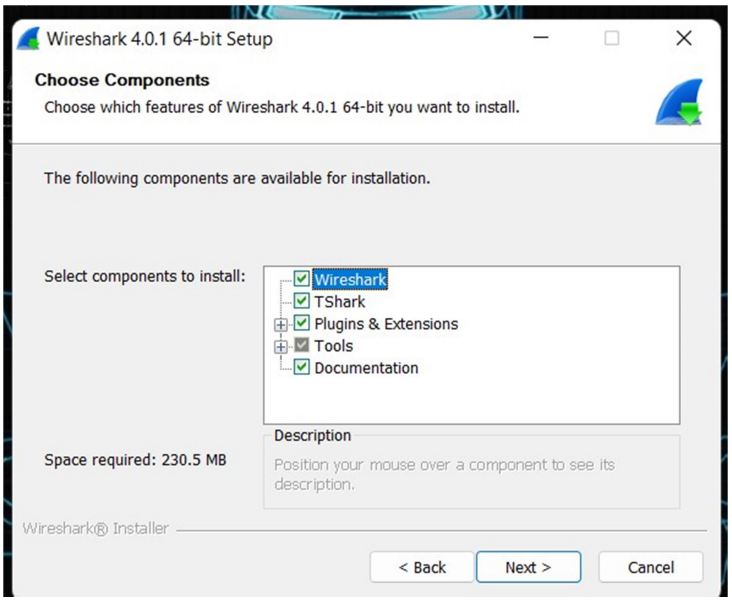
PROCEDURE: -

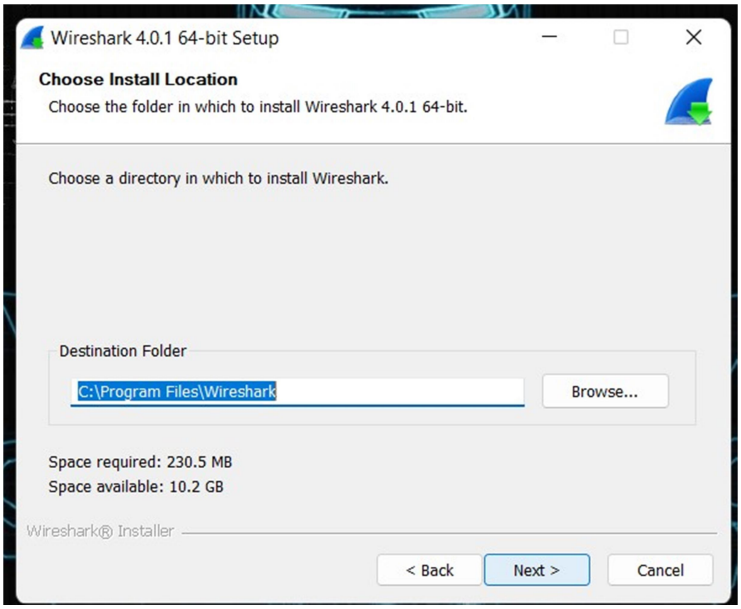
Step1: - Download wireshark

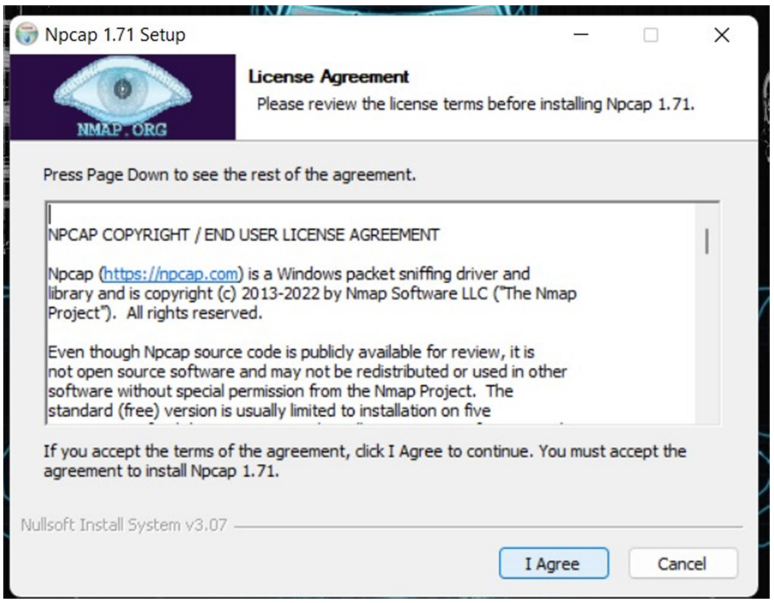


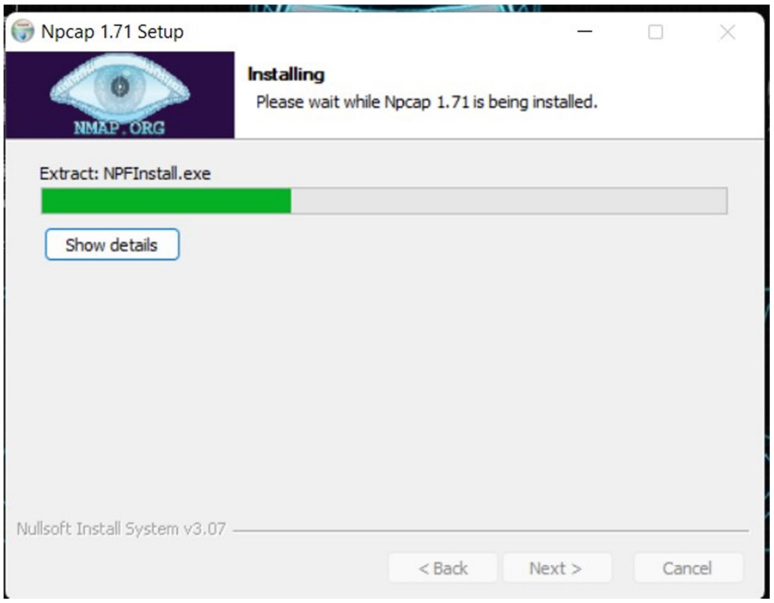
Step2: - Install the application with default settings

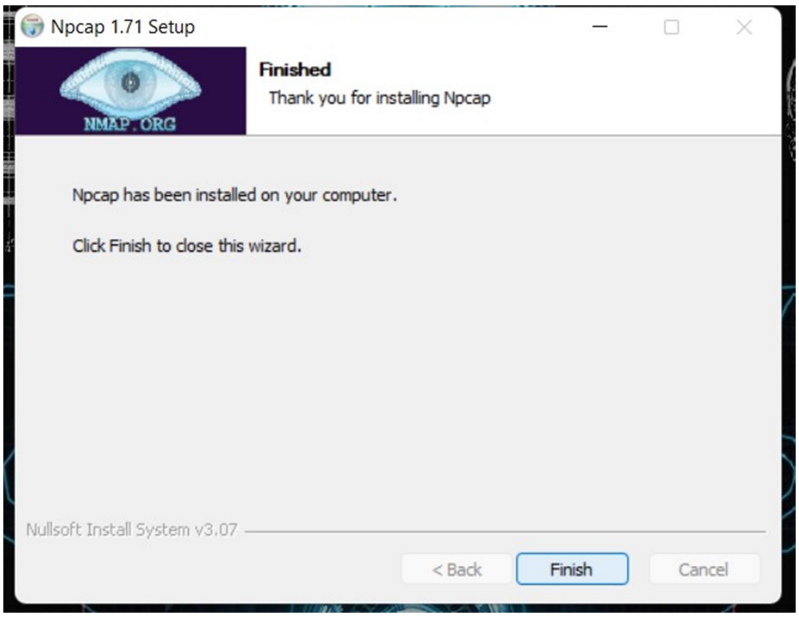



Wireshark 4.0.1 64-bit Setup
Choose Components
Choose which features of Wireshark 4.0.1 64-bit you want to install.
The following components are available for installation.
Select components to install:
Wireshark
TShark
Plugins & Extensions
Tools
Documentation
Description
Position your mouse over a component to see its description.
Space required: 230.5 MB
Wireshark® Installer
< Back
Next >
Cancel

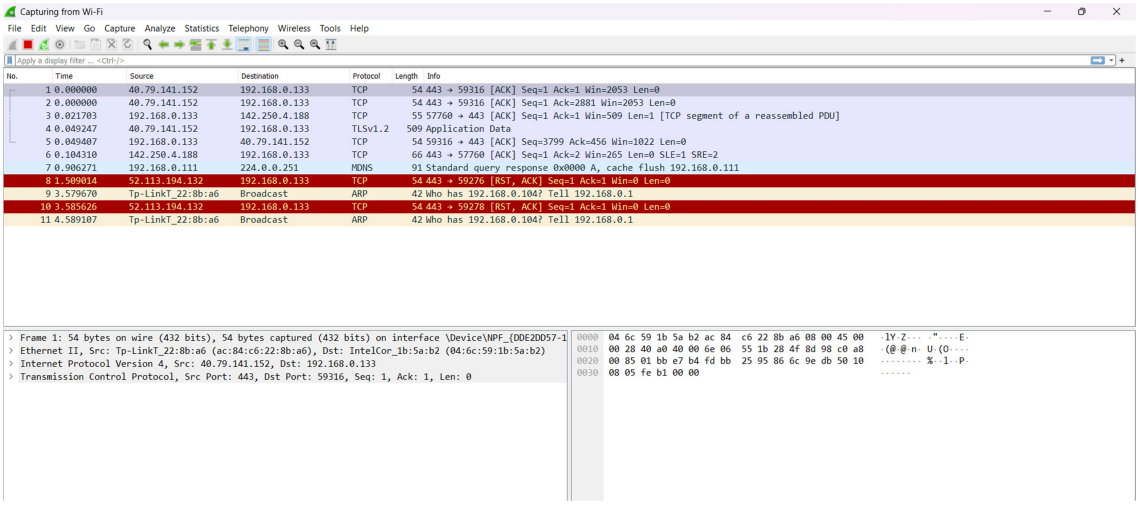

Wireshark 4.0.1 64-bit Setup
Choose Install Location
Choose the folder in which to install Wireshark 4.0.1 64-bit.
Choose a directory in which to install Wireshark.
Destination Folder
C:\Program Files\Wireshark
Browse...
Space required: 230.5 MB
Space available: 10.2 GB
Wireshark® Installer
< Back
Next >
Cancel


Npcap 1.71 Setup
NMAP.ORG
License Agreement
Please review the license terms before installing Npcap 1.71.
Press Page Down to see the rest of the agreement.
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT
Npcap (https://npcap.com) is a Windows packet sniffing driver and library and is copyright (c) 2013-2022 by Nmap Software LLC ("The Nmap Project"). All rights reserved.
Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed or used in other software without special permission from the Nmap Project. The standard (free) version is usually limited to installation on five
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.71.
Nullsoft Install System v3.07
I Agree
Cancel

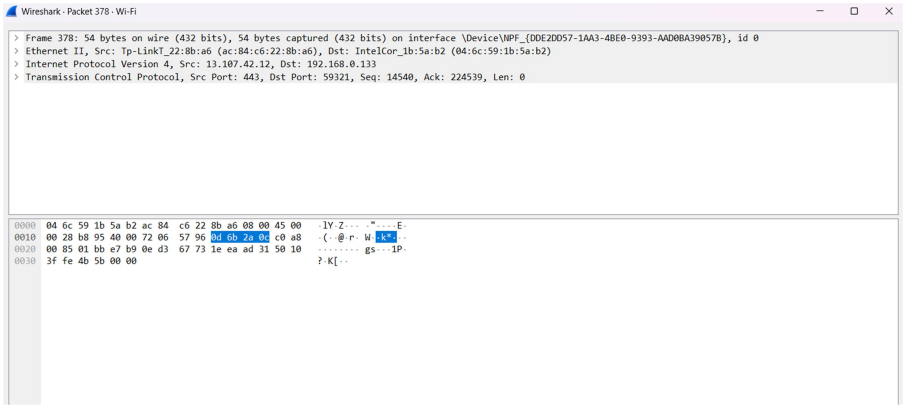

Npcap 1.71 Setup
NMAP.ORG
Installing
Please wait while Npcap 1.71 is being installed.
Extract: NPFInstall.exe
Show details
Nullsoft Install System v3.07
< Back
Next >
Cancel



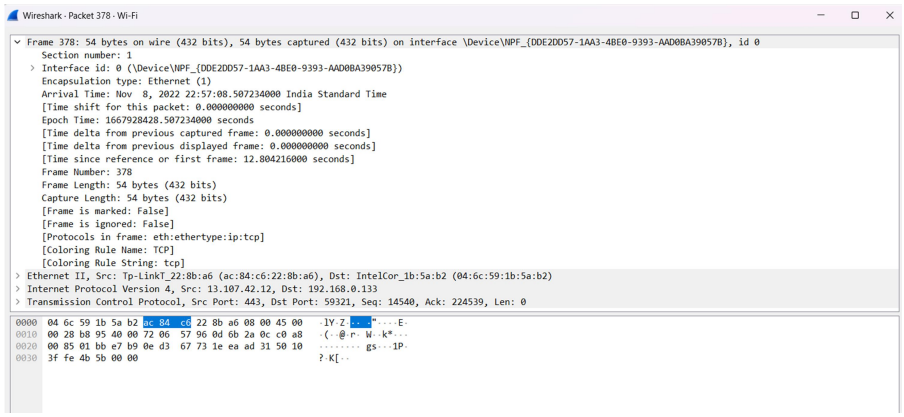
Step3: - Click on the Ethernet/WIFI and all the packets Information will be appeared.



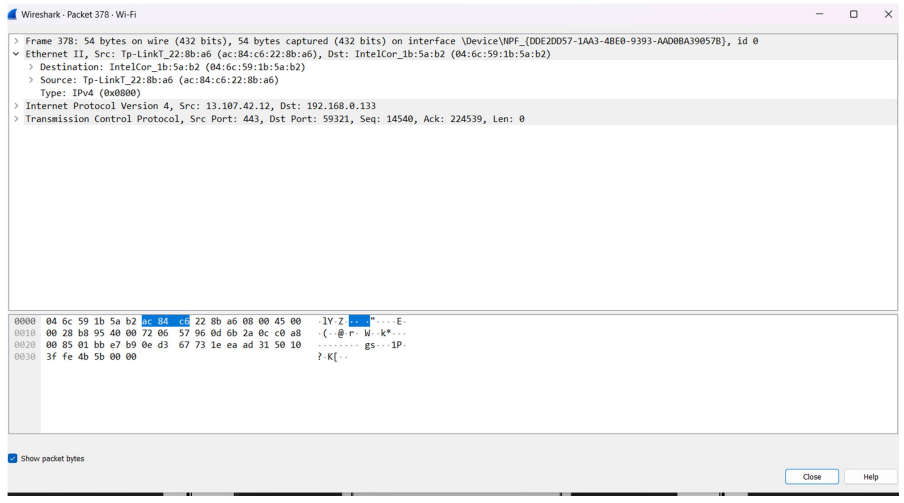
Step4: - click on a packet to show detailed



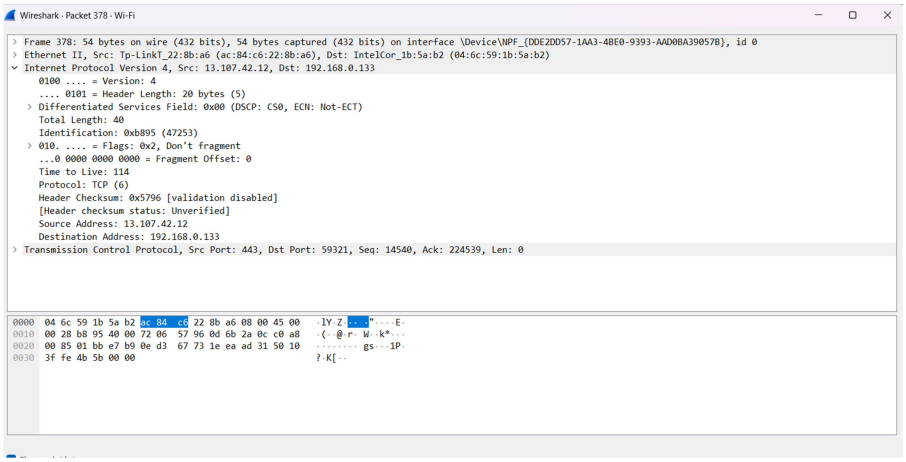
- First options shows the details regarding physical layer.

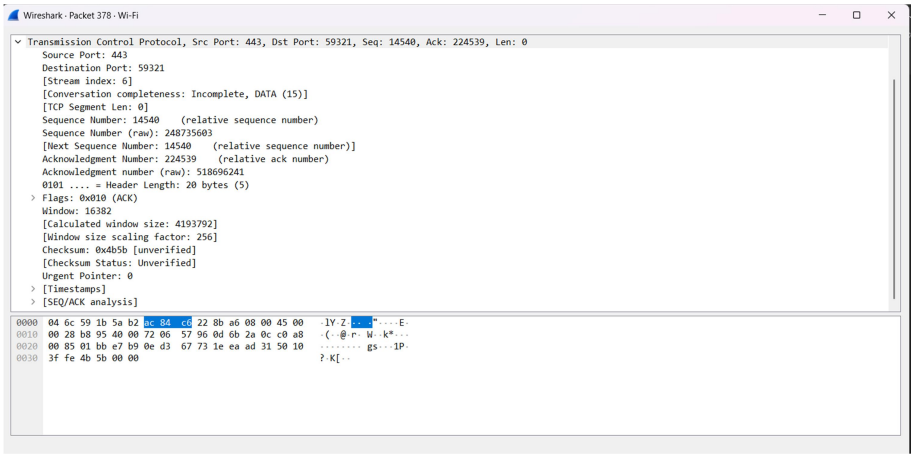


- Second option contains details regarding data link layer like destination and source mac addresses.



- Third option contains network layer details like Ip addresses of source and destinations


Wireshark · Packet 378 · Wi-Fi
Frame 378: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{DDE2DD57-1AA3-4BE0-9393-AAD0BA39057B}, id 0
Ethernet II, Src: Tp-LinkT_22:8b:a6 (ac:84:c6:22:8b:a6), Dst: IntelCor_1b:5a:b2 (04:6c:59:1b:5a:b2)
Internet Protocol Version 4, Src: 13.107.42.12, Dst: 192.168.0.133
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xb895 (47253)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 114
Protocol: TCP (6)
Header Checksum: 0x5796 [validation disabled]
[Header checksum status: Unverified]
Source Address: 13.107.42.12
Destination Address: 192.168.0.133
Transmission Control Protocol, Src Port: 443, Dst Port: 59321, Seq: 14540, Ack: 224539, Len: 0
0000 04 6c 59 1b 5a b2 ac 84 c6 22 8b a6 08 00 45 00
0010 00 28 b8 95 40 00 72 06 57 96 0d 6b 2a 0c c0 a8
0020 00 85 01 bb e7 b9 0e d3 67 73 1e ea ad 31 50 10
0030 3f fe 4b 5b 00 00

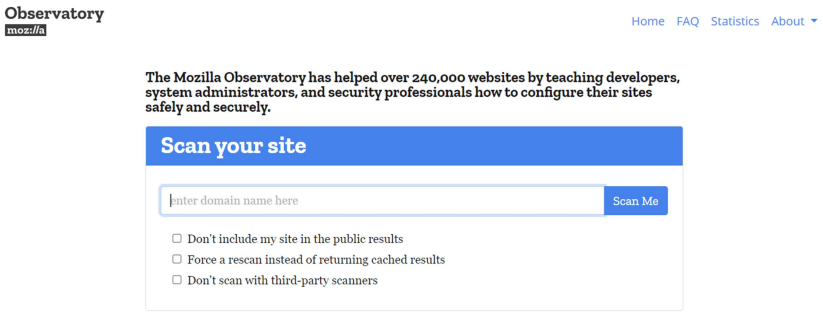

Wireshark · Packet 378 · Wi-Fi
Transmission Control Protocol, Src Port: 443, Dst Port: 59321, Seq: 14540, Ack: 224539, Len: 0
Source Port: 443
Destination Port: 59321
[Stream index: 6]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 14540 (relative sequence number)
Sequence Number (raw): 248735603
[Next Sequence Number: 14540 (relative sequence number)]
Acknowledgment Number: 224539 (relative ack number)
Acknowledgment number (raw): 518696241
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 16382
[Calculated window size: 4193792]
[Window size scaling factor: 256]
Checksum: 0x4b5b [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
0000 04 6c 59 1b 5a b2 ac 84 c6 22 8b a6 08 00 45 00
0010 00 28 b8 95 40 00 72 06 57 96 0d 6b 2a 0c c0 a8
0020 00 85 01 bb e7 b9 0e d3 67 73 1e ea ad 31 50 10
0030 3f fe 4b 5b 00 00

4. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

AIM: - Demonstrate Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Procedure: -

Step1: - Visit https://observatory.mozilla.org/.



Step2: - Enter the URL of the website you want to perform web security analysis.

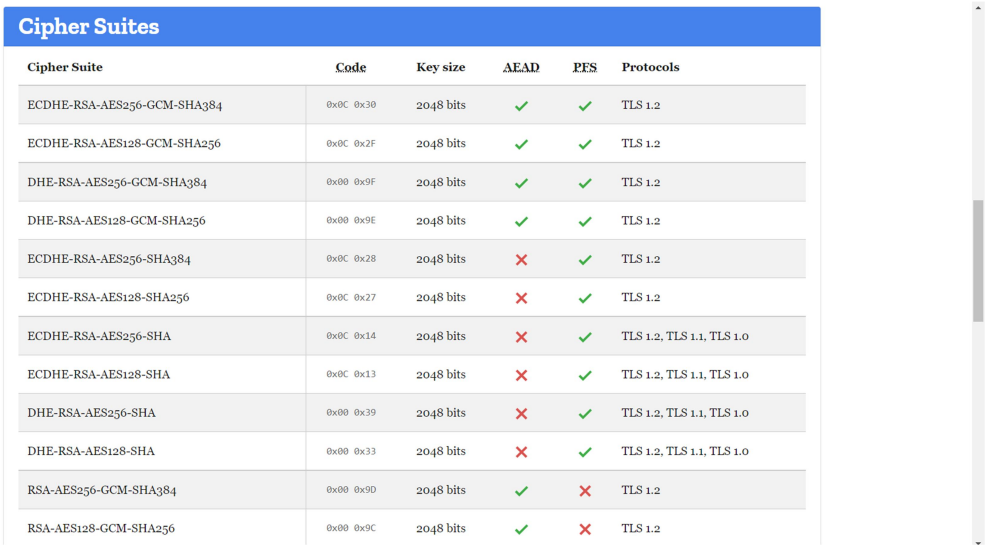
Step3: - You can observe the results by clicking on the scan me button.

Step4: - Click on TLS observatory.

TLS: -

- Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network.
- It shows the compatibility level as secure or Insecure by performing relevant tests on the url provided.

- It also displays the cipher suites of different cipher suite.
- It also displays the code, key size, AEAD, PFS and protocols.
- Some miscellaneous information like CAA records, Cipher reference, Compatible clients and OSCP Stapling.



Cipher Suites

Cipher Suite	Code	Key size	AEAD	PFS	Protocols
ECDHE-RSA-AES256-GCM-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x2F	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES256-GCM-SHA384	0x00 0x9F	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES128-GCM-SHA256	0x00 0x9E	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-SHA384	0x0C 0x28	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES128-SHA256	0x0C 0x27	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA	0x0C 0x14	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
ECDHE-RSA-AES128-SHA	0x0C 0x13	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-AES256-SHA	0x00 0x39	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-AES128-SHA	0x00 0x33	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES256-GCM-SHA384	0x00 0x9D	2048 bits	✓	✗	TLS 1.2
RSA-AES128-GCM-SHA256	0x00 0x9C	2048 bits	✓	✗	TLS 1.2
RSA-AES128-SHA256	0x00 0x3C	2048 bits	✗	✗	TLS 1.2
RSA-AES256-SHA	0x00 0x35	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES128-SHA	0x00 0x2F	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-DES-CBC3-SHA	0x00 0x0A	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-RC4-SHA	0x00 0x05	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-RC4-MD5	0x00 0x04	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 2.3.7, Apple ATS 9, Baidu Jan 2015, BingBot Dec 2013, BingPreview Dec 2013, Chrome 27, Edge 12, Firefox 21, Googlebot Oct 2013, IE 7, Java 6u45, OpenSSL 0.9.8y, Opera 12.15, Safari 5, Tor 17.0.9, Yahoo Slurp Oct 2013, YandexBot May 2014
OCSP Stapling:	Yes

SSL: -

- SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details.
- SSL Labs gives a report containing the details regarding
  - Certificate
  - Protocol support
  - Key exchange
  - Cypher strength

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.gvpce.ac.in

SSL Report: www.gvpce.ac.in (123.108.201.250)

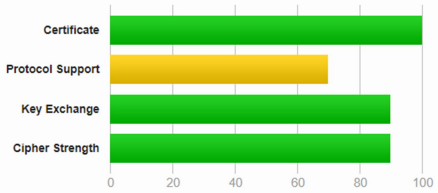
Assessed on: Sat, 12 Nov 2022 09:41:53 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »

This server's certificate is not trusted by Apple, Android and Java trust store (see below for details).

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	gvpce.ac.in Fingerprint SHA256: 0e4d74b87f09f1de33918c3b6400572d04927d7aa258b4506a3b706378b6f1ba Pin SHA256: MrmHQftzv6mKKiIxjaM5G9zul0uAR6BvAsOjq5kVTCE=
Common names	gvpce.ac.in
Alternative names	www.gvpce.ac.in gvpce.ac.in
Serial Number	00efb82aa8883a7350
Valid from	Mon, 08 Aug 2022 10:57:52 UTC
Valid until	Tue, 08 Aug 2023 10:57:52 UTC (expires in 8 months and 27 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	emSign SSL CA - G1 AIA: http://repository.emsign.com/certs/emSignSSLCAG1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.emsign.com?emSignSSLCAG1.crl OCSP: http://ocsp.emSign.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows