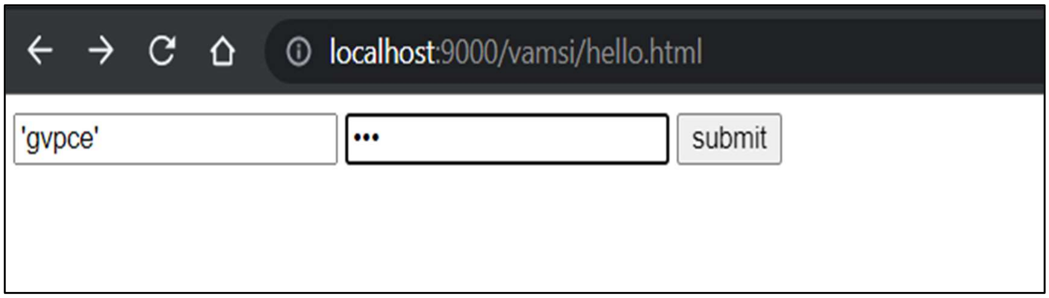
1.SQL INJECTION

Aim : Exploit SQL injection flaws on a sample website.

Case 1: Entering the correct credentials to the website login.

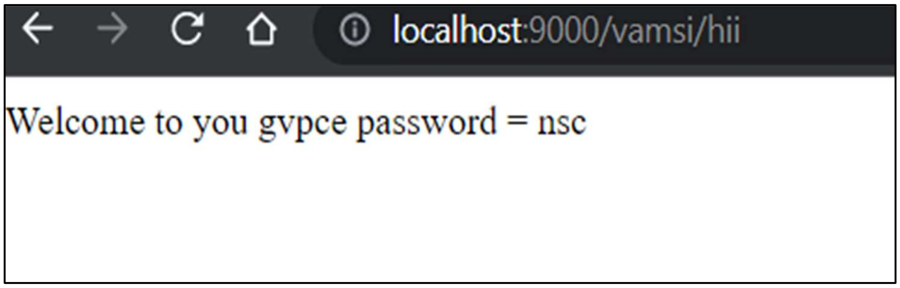
Input : **Username = “gvpce”** **Password = “nsc”**



localhost:9000/vamsi/hello.html

'gvpce' •••

Output :

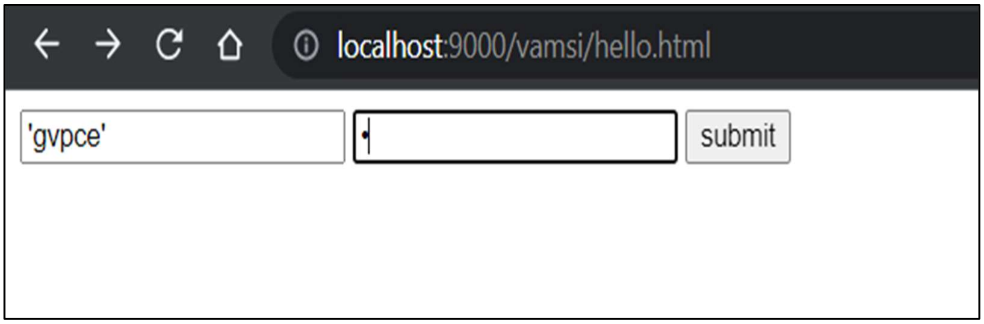


localhost:9000/vamsi/hii

Welcome to you gvpce password = nsc

Case 2 : Entering the incorrect credentials to the website login.

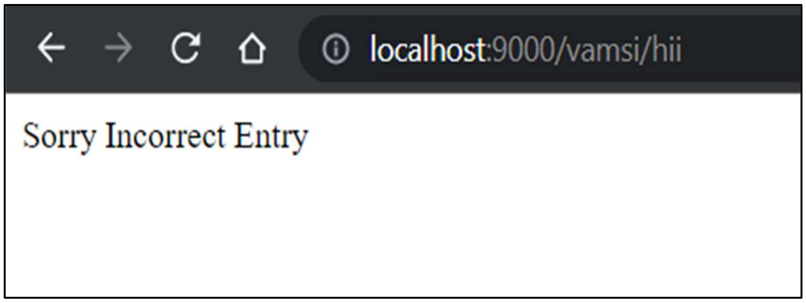
Input : **Username = “gvpce”** **Password = “s”**



localhost:9000/vamsi/hello.html

'gvpce' •

Output :

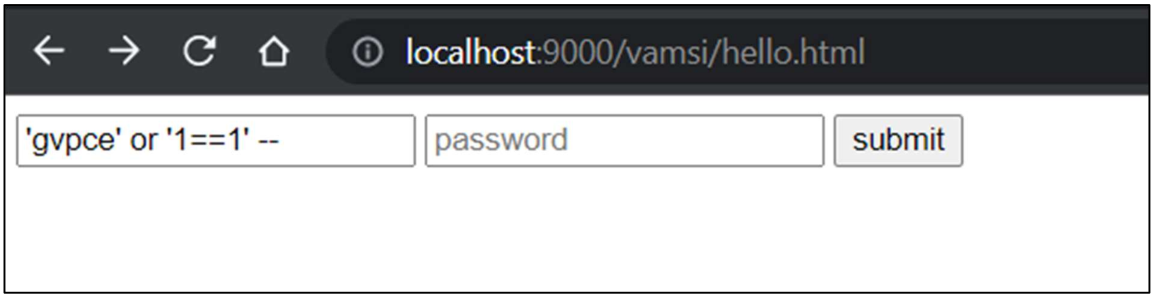


localhost:9000/vamsi/hii

Sorry Incorrect Entry

<u>Case 3 :</u> Injecting SQL commands to login without password

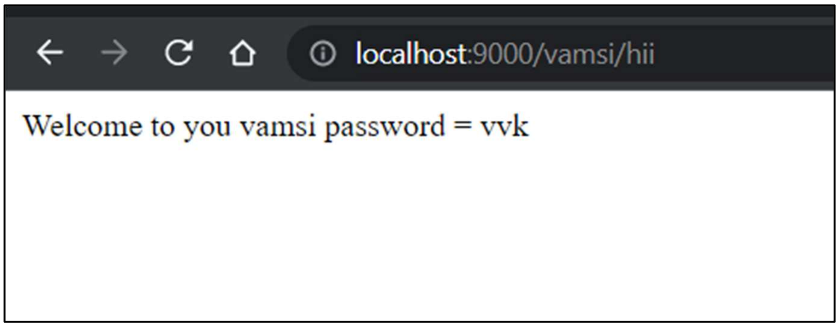
<u>Input :</u> **Username = ‘gvpce’ or ‘1==1’ --**



localhost:9000/vamsi/hello.html

'gvpce' or '1==1' --

<u>Output :</u>

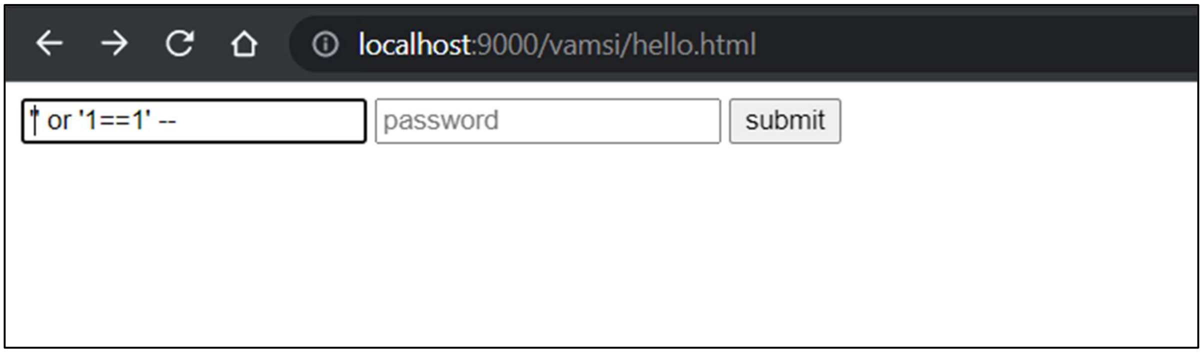


localhost:9000/vamsi/hii

Welcome to you vamsi password = vvk

<u>Case 4 :</u> Injecting SQL command to login without username and password

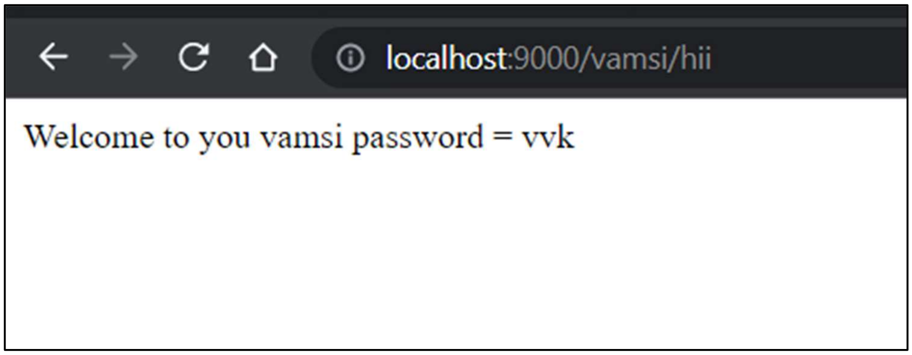
<u>Input :</u> **Username= ‘ ‘’ or ‘1==1’ –**



localhost:9000/vamsi/hello.html

' or '1==1' --

<u>Output :</u>



localhost:9000/vamsi/hii

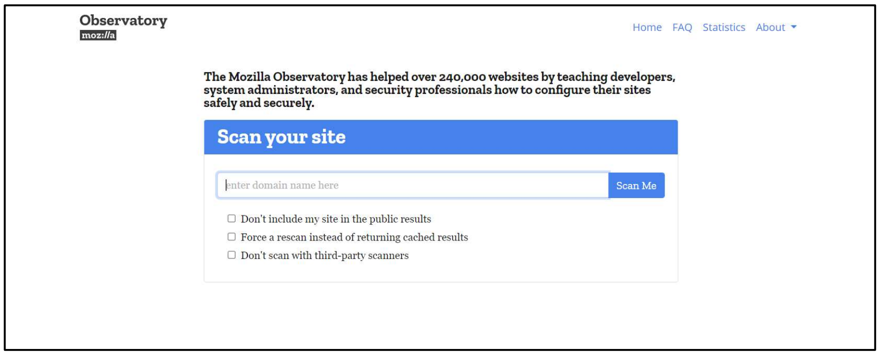
Welcome to you vamsi password = vvk

2.WEB SECURITY ANALYSIS

Aim : Perform web security analysis on a sample website

Procedure :

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



Observatory
moz://a

The Mozilla Observatory has helped over 240,000 websites by teaching developers, system administrators, and security professionals how to configure their sites safely and securely.

Scan your site

enter domain name here | Scan Me

□ Don't include my site in the public results
□ Force a rescan instead of returning cached results
□ Don't scan with third-party scanners

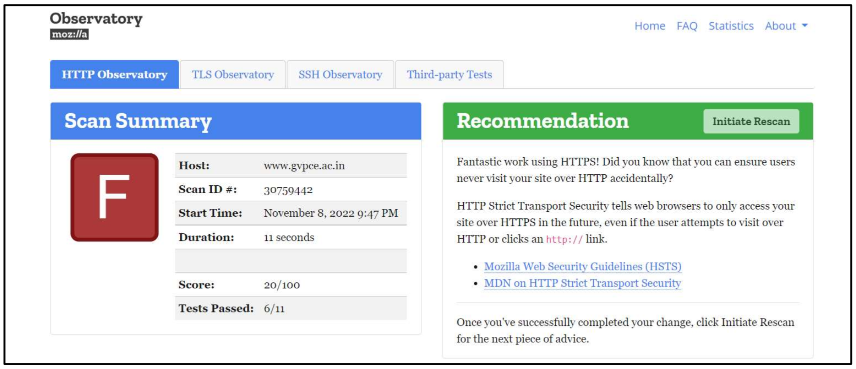
Step2 : Enter the URL of the website you want to perform web security analysis.

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.



Observatory
moz://a

Scan Summary

Host:	www.gvpce.ac.in
Scan ID #:	30759442
Start Time:	November 8, 2022 9:47 PM
Duration:	11 seconds
Score:	20/100
Tests Passed:	6/11

Recommendation Initiate Rescan

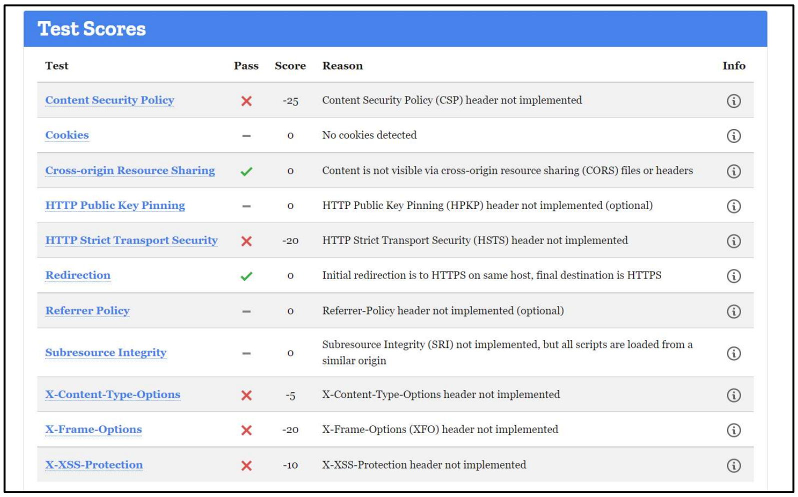
Fantastic work using HTTPS! Did you know that you can ensure users never visit your site over HTTP accidentally?

HTTP Strict Transport Security tells web browsers to only access your site over HTTPS in the future, even if the user attempts to visit over HTTP or clicks an `http://` link.

- Mozilla Web Security Guidelines (HSTS)
- MDN on HTTP Strict Transport Security

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

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

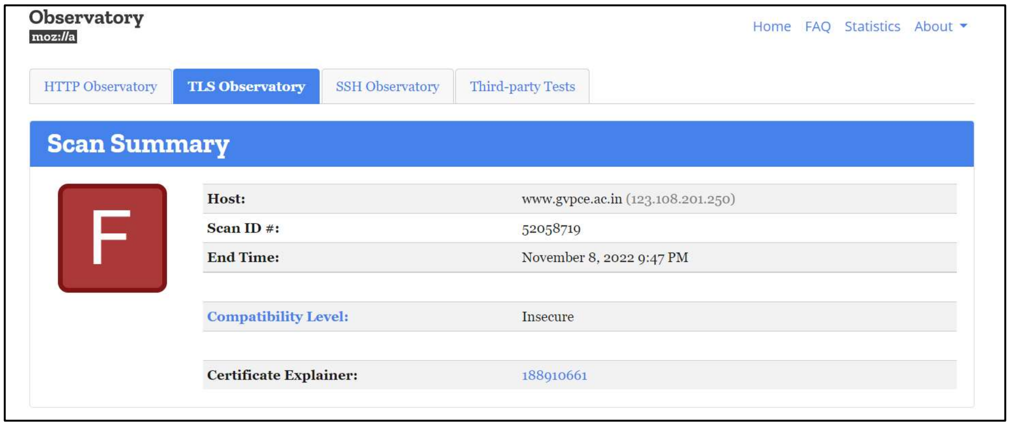


Test Scores

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	ⓘ

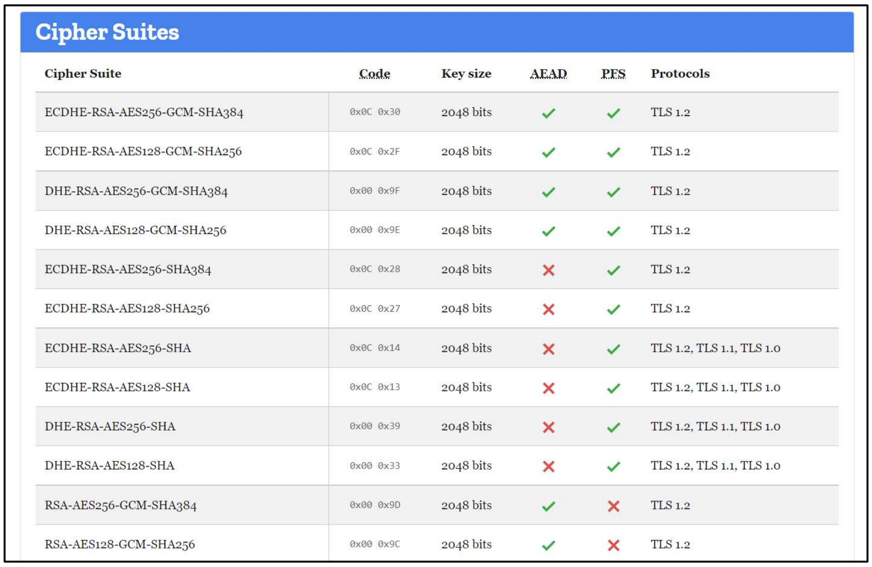
TLS observatory

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

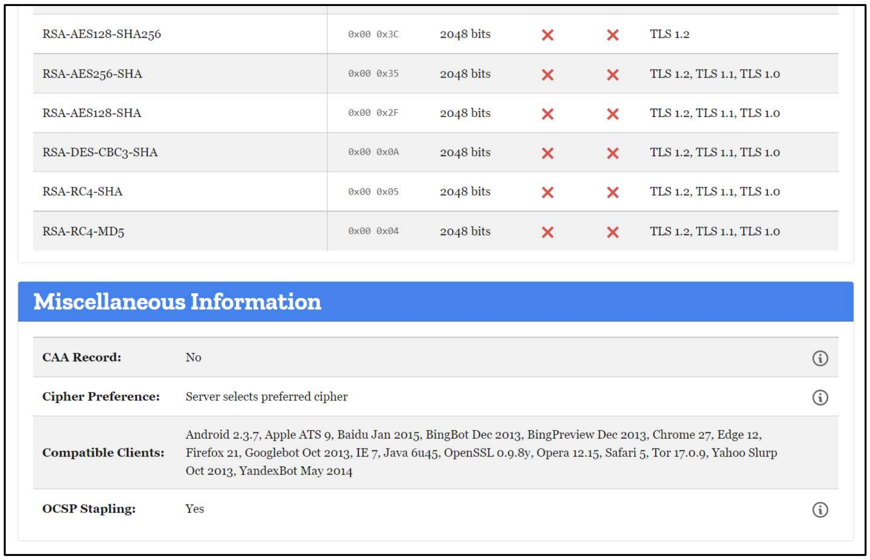


Host:	www.gvpce.ac.in (123.108.201.250)
Scan ID #:	52058719
End Time:	November 8, 2022 9:47 PM
Compatibility Level:	Insecure
Certificate Explainer:	188910661

- 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 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

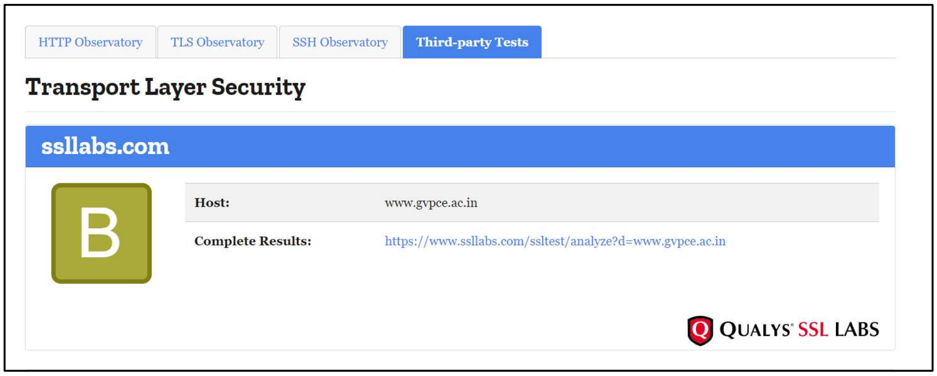


CAA Record:	No
Cipher Preference:	Server selects preferred cipher
Compatible Clients:	Android 2.3.7, Apple ATS 9, Baidu Jan 2015, BingBot Dec 2013, BingPreview Dec 2013, Chrome 27, Edge 12, Firefox 21, Googlebot Oct 2013, IE 7, Java 6u45, OpenSSL 0.9.8y, Opera 12.15, Safari 5, Tor 17.0.9, Yahoo Slurp 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

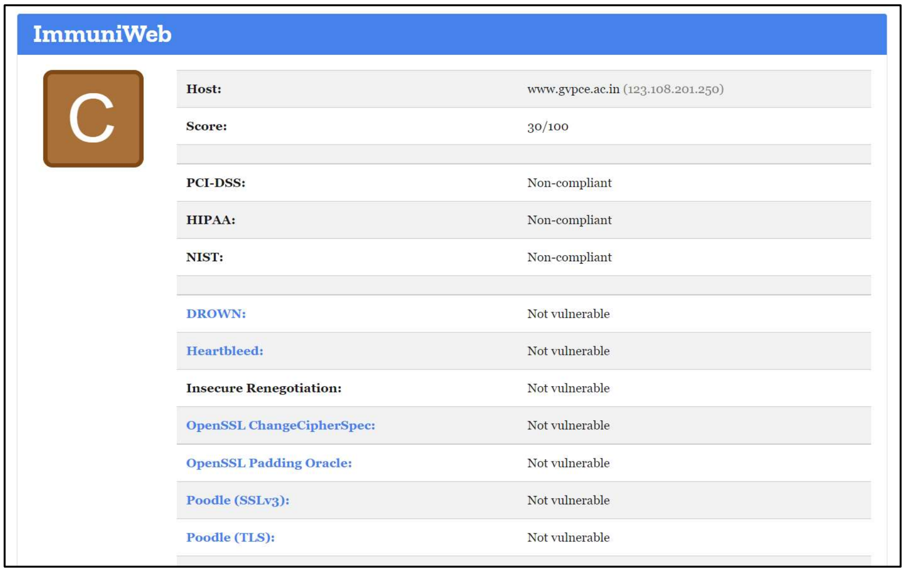


Transport Layer Security

ssllabs.com

B

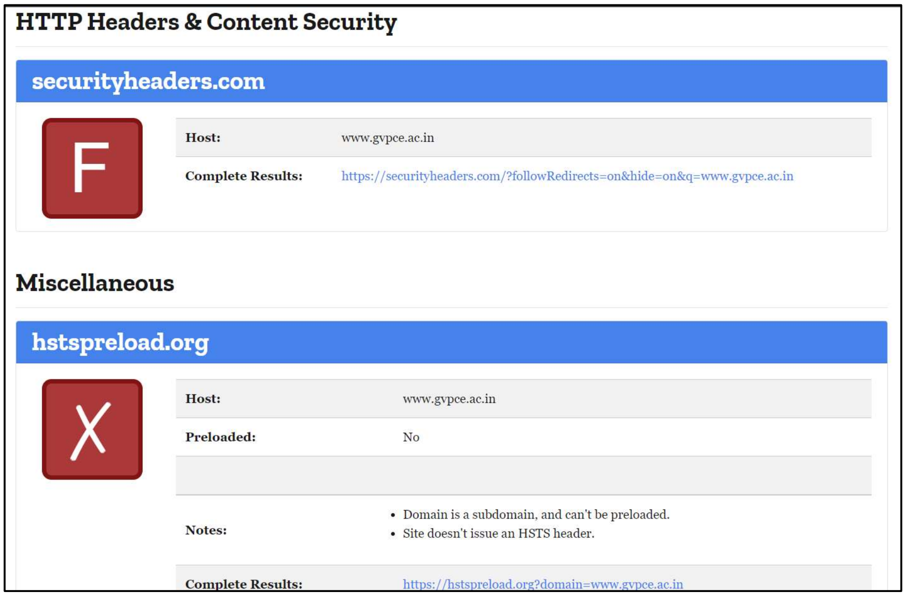
Host:	www.gvpce.ac.in
Complete Results:	https://www.ssllabs.com/ssltest/analyze?d=www.gvpce.ac.in



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

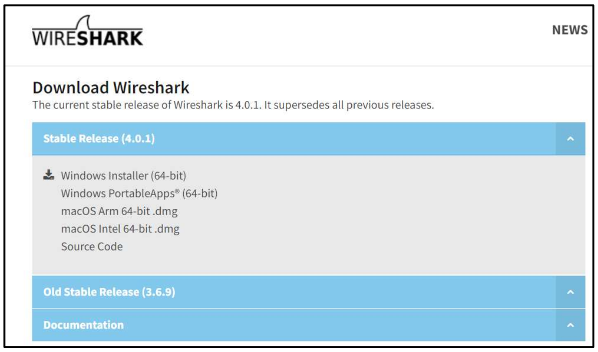
Host:	www.gvpce.ac.in
Preloaded:	No
Notes:	• Domain is a subdomain, and can't be preloaded. • Site doesn't issue an HSTS header.
Complete Results:	https://hstspreload.org?domain=www.gvpce.ac.in

3.SNIFFING ROUTER TRAFFIC

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

Procedure :

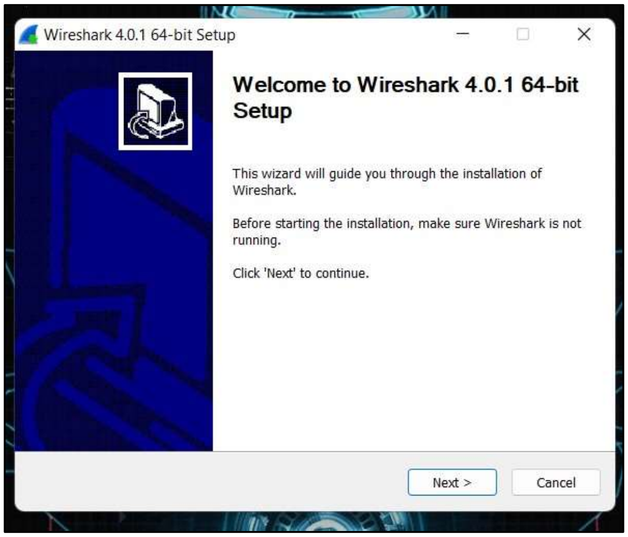
Step1 : Download **Wireshark**



Download Wireshark

The current stable release of Wireshark is 4.0.1. It supersedes all previous releases.

Step2 : Install the application with default settings

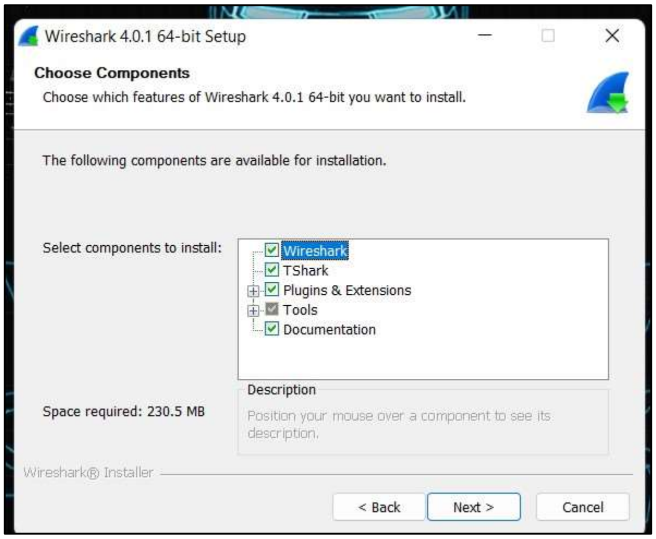


Welcome to Wireshark 4.0.1 64-bit Setup

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.



Choose Components

Choose which features of Wireshark 4.0.1 64-bit you want to install.

The following components are available for installation.

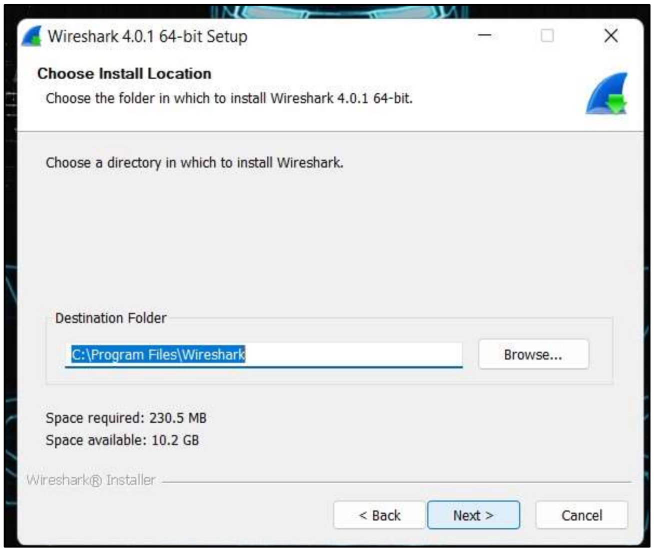
Select components to install:

- ☑ Wireshark
- ☑ TShark
- ☑ Plugins & Extensions
- ☑ Tools
- ☑ Documentation

Space required: 230.5 MB

Description

Position your mouse over a component to see its description.



Choose Install Location

Choose the folder in which to install Wireshark 4.0.1 64-bit.

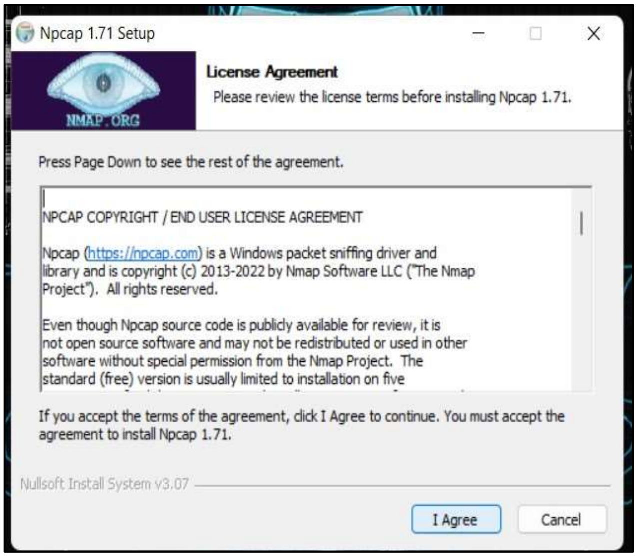
Choose a directory in which to install Wireshark.

Destination Folder

C:\Program Files\Wireshark

Space required: 230.5 MB

Space available: 10.2 GB



License Agreement

Please review the license terms before installing Npcap 1.71.

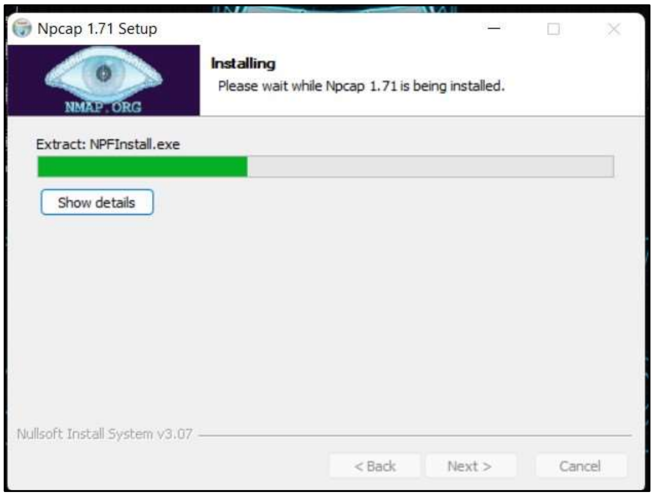
Press Page Down to see the rest of the agreement.

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.

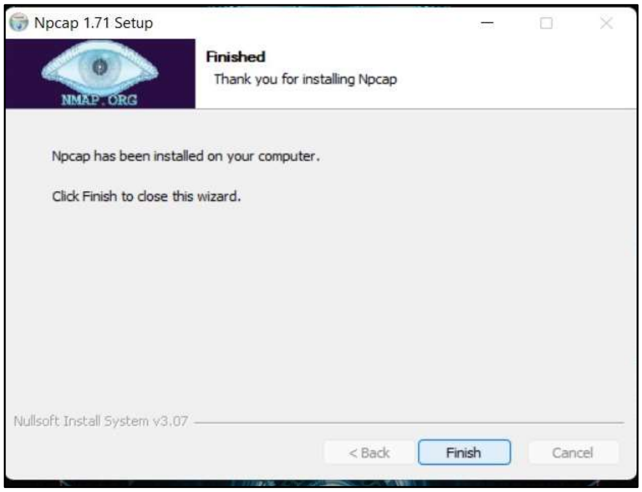


Npcap 1.71 Setup

Installing

Please wait while Npcap 1.71 is being installed.

Extract: NPFInstall.exe



Npcap 1.71 Setup

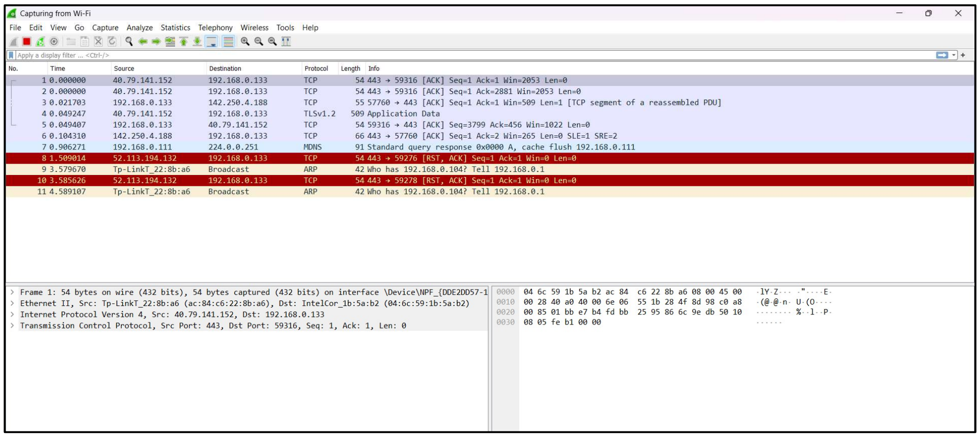
Finished

Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.

Step 3 : Click on the Ethernet/WIFI and all the packets Information will be appeared.



Capturing from Wi-Fi

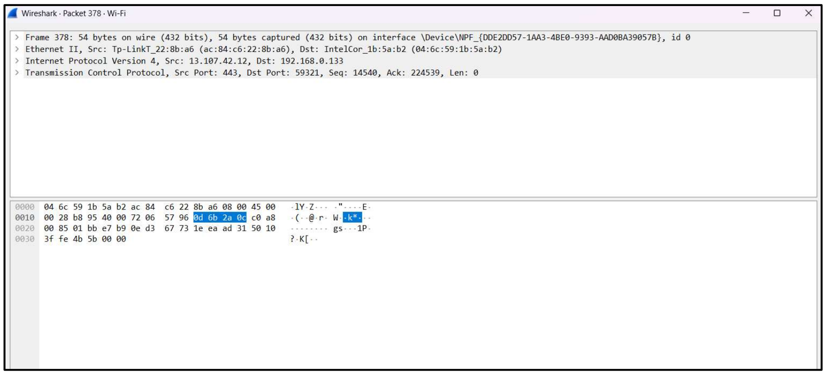
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source            Destination      Protocol  Length  Info
    1 0.000000   40.79.141.152     192.168.0.133    TCP          54 443 → 59316 [ACK] Seq=1 Ack=1 Win=2053 Len=0
    2 0.000000   40.79.141.152     192.168.0.133    TCP          54 443 → 59316 [ACK] Seq=1 Ack=2881 Win=2053 Len=0
    3 0.021703   192.168.0.133     142.250.4.188    TCP          55 57760 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
    4 0.049247   40.79.141.152     192.168.0.133    TLSv1.2     509 Application Data
    5 0.049407   192.168.0.133     40.79.141.152    TCP          54 59316 → 443 [ACK] Seq=3799 Ack=456 Win=1022 Len=0
    6 0.104310   142.250.4.188     192.168.0.133    TCP          66 443 → 57760 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
    7 0.906271   192.168.0.111     224.0.0.251      MDNS         91 Standard query response 0x0000 A, cache flush 192.168.0.111
    8 1.509014   52.113.194.132    192.168.0.133    TCP          54 443 → 59276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    9 3.579670   Tp-LinkT_22:8b:a6 Broadcast        ARP          42 Who has 192.168.0.104? Tell 192.168.0.1
   10 3.585626   52.113.194.132    192.168.0.133    TCP          54 443 → 59278 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   11 4.589107   Tp-LinkT_22:8b:a6 Broadcast        ARP          42 Who has 192.168.0.104? Tell 192.168.0.1
```

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{DDE2DD57-1
> 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: 40.79.141.152, Dst: 192.168.0.133
> Transmission Control Protocol, Src Port: 443, Dst Port: 59316, Seq: 1, Ack: 1, Len: 0
```

```
0000  04 6c 59 1b 5a b2 ac 84  c6 22 8b a6 08 00 45 00   ·lY·Z··· ·"····E·
0010  00 28 40 a0 40 00 6e 06  55 1b 28 4f 8d 98 c0 a8   ·(@·@·n· U·(O····
0020  00 85 01 bb e7 b4 fd bb  25 95 86 6c 9e db 50 10   ········ %··l··P·
0030  08 05 fe b1 00 00                                  ······
```

Step 4 : click on a packet to show detailed

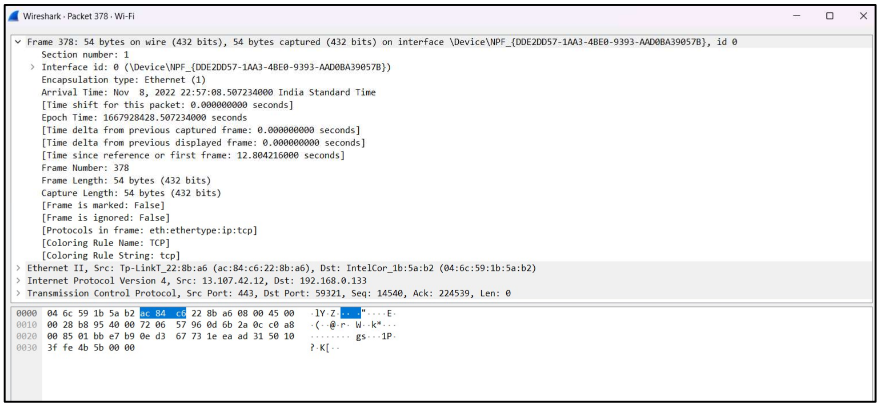


Wireshark · Packet 378 · Wi-Fi

```
> 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
> 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   ·lY·Z··· ·"····E·
0010  00 28 b8 95 40 00 72 06  57 96 0d 6b 2a 0c c0 a8   ·(··@·r· W··k*···
0020  00 85 01 bb e7 b9 0e d3  67 73 1e ea ad 31 50 10   ········ gs···1P·
0030  3f fe 4b 5b 00 00                                  ?·K[··
```

- First options shows the details regarding physical layer.

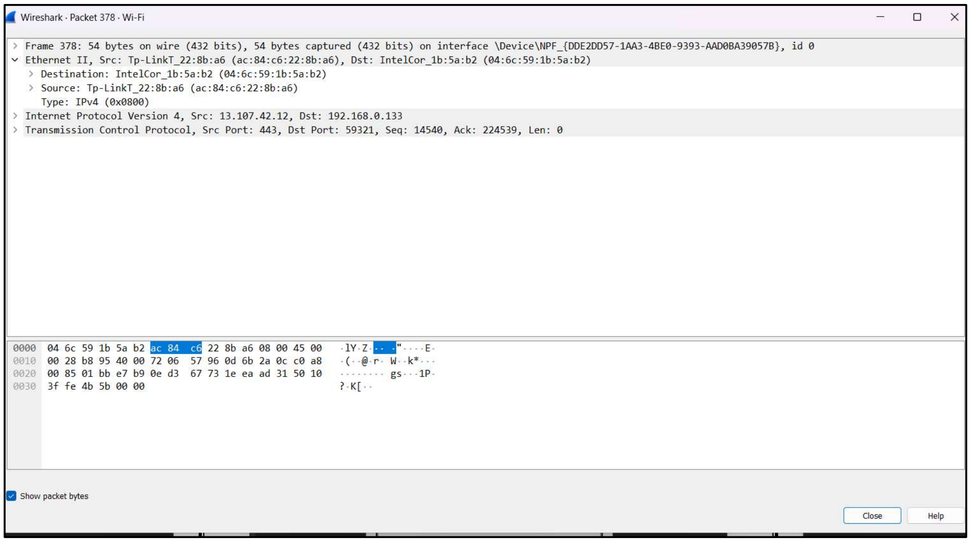


Wireshark · Packet 378 · Wi-Fi

```
∨ Frame 378: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{DDE2DD57-1AA3-4BE0-9393-AAD0BA39057B}, id 0
    Section number: 1
  > Interface id: 0 (\Device\NPF_{DDE2DD57-1AA3-4BE0-9393-AAD0BA39057B})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  8, 2022 22:57:08.507234000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667928428.507234000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 12.804216000 seconds]
    Frame Number: 378
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> 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
> 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   ·lY·Z··· ·"····E·
0010  00 28 b8 95 40 00 72 06  57 96 0d 6b 2a 0c c0 a8   ·(··@·r· W··k*···
0020  00 85 01 bb e7 b9 0e d3  67 73 1e ea ad 31 50 10   ········ gs···1P·
0030  3f fe 4b 5b 00 00                                  ?·K[··
```

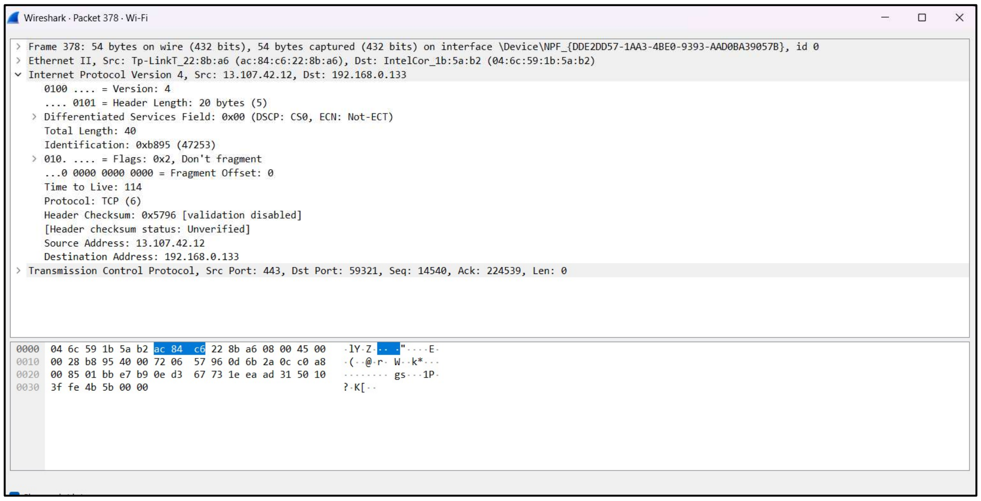
- Second option contains details regarding data link layer like destination and source mac addresses.



```
> Frame 378: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{DDE2DD57-1AA3-4BE0-9393-AAD0BA39057B}, id 0
v 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)
  > Destination: IntelCor_1b:5a:b2 (04:6c:59:1b:5a:b2)
  > Source: Tp-LinkT_22:8b:a6 (ac:84:c6:22:8b:a6)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 13.107.42.12, Dst: 192.168.0.133
> Transmission Control Protocol, Src Port: 443, Dst Port: 59321, Seq: 14540, Ack: 224539, Len: 0
```

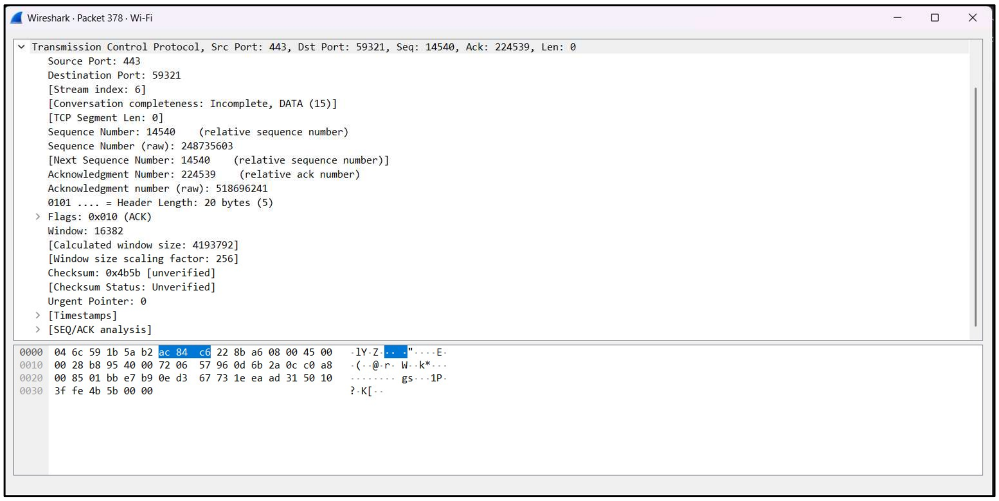
```
0000  04 6c 59 1b 5a b2 ac 84  c6 22 8b a6 08 00 45 00   ·lY·Z····"····E·
0010  00 28 b8 95 40 00 72 06  57 96 0d 6b 2a 0c c0 a8   ·(··@·r· W··k*···
0020  00 85 01 bb e7 b9 0e d3  67 73 1e ea ad 31 50 10   ········ gs···1P·
0030  3f fe 4b 5b 00 00                                  ?·K[··
```

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



```
> 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)
v 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   ·lY·Z····"····E·
0010  00 28 b8 95 40 00 72 06  57 96 0d 6b 2a 0c c0 a8   ·(··@·r· W··k*···
0020  00 85 01 bb e7 b9 0e d3  67 73 1e ea ad 31 50 10   ········ gs···1P·
0030  3f fe 4b 5b 00 00                                  ?·K[··
```



```
v 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]
```

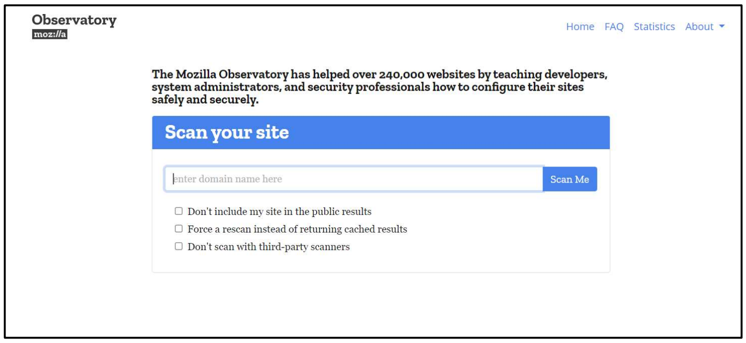
```
0000  04 6c 59 1b 5a b2 ac 84  c6 22 8b a6 08 00 45 00   ·lY·Z····"····E·
0010  00 28 b8 95 40 00 72 06  57 96 0d 6b 2a 0c c0 a8   ·(··@·r· W··k*···
0020  00 85 01 bb e7 b9 0e d3  67 73 1e ea ad 31 50 10   ········ gs···1P·
0030  3f fe 4b 5b 00 00                                  ?·K[··
```

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

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

Procedure :

Step 1 : Visit **https://observatory.mozilla.org/**



The Mozilla Observatory has helped over 240,000 websites by teaching developers, system administrators, and security professionals how to configure their sites safely and securely.

Scan your site

Enter domain name here

□ Don't include my site in the public results
□ Force a rescan instead of returning cached results
□ Don't scan with third-party scanners

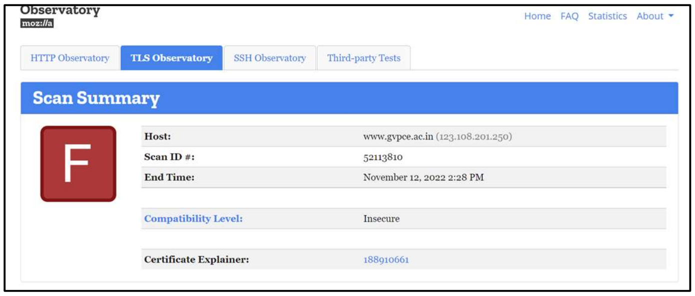
Step 2 : Enter the URL of the website you want to perform web security analysis.

Step 3 : You can observe the results by clicking on the scan me button.

Step 4 : Click on TLS observatory.

TLS (Transport Layer Security) :

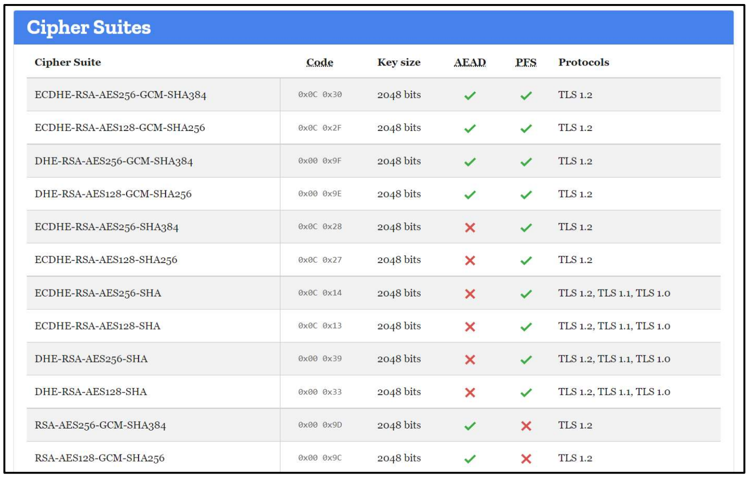
- Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network.
- It shows the compatibility level as secure or Insecure by performing relevant tests on the url provided.



Scan Summary

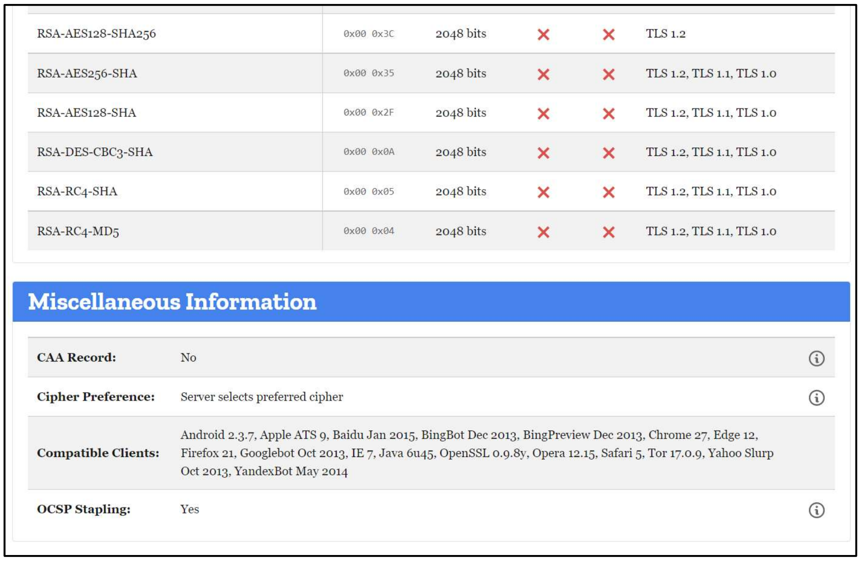
Host:	www.gvpce.ac.in (123.108.201.250)
Scan ID #:	52113810
End Time:	November 12, 2022 2:28 PM
Compatibility Level:	Insecure
Certificate Explainer:	188910661

- 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

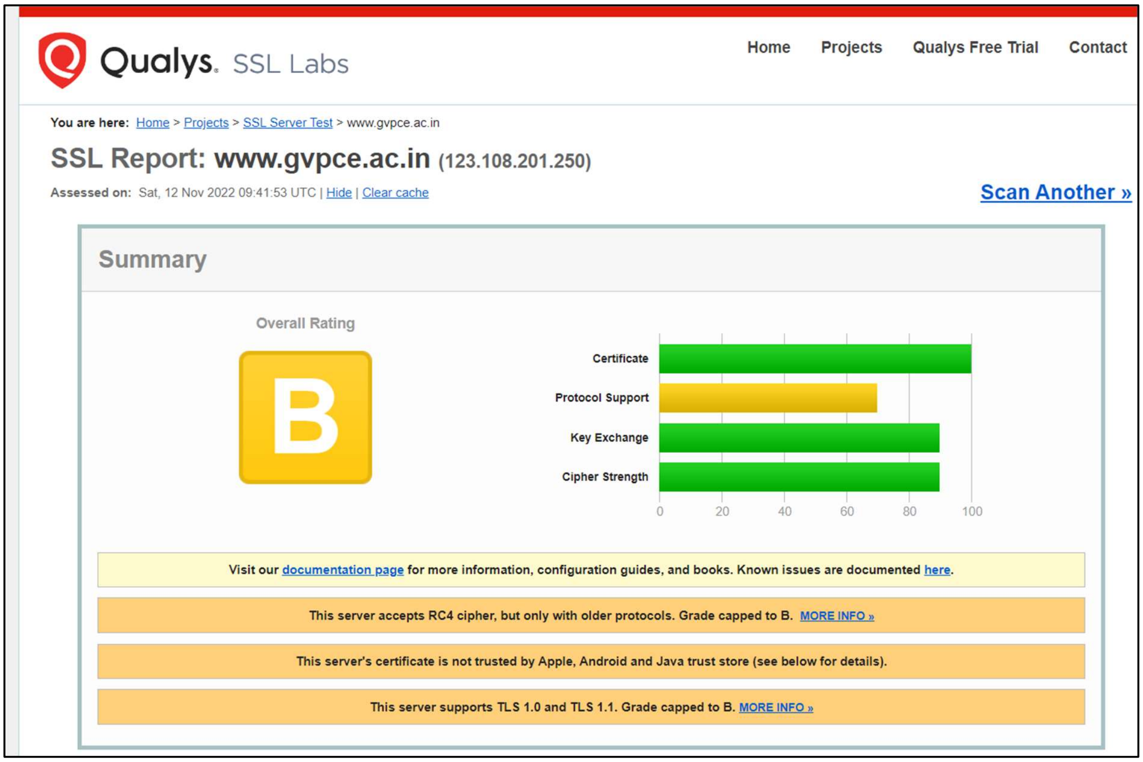
Miscellaneous Information

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

SSL (Secure Socket Layer) :

- 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
  - ➢ Cipher strength

SSL Report of the Tested Website



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

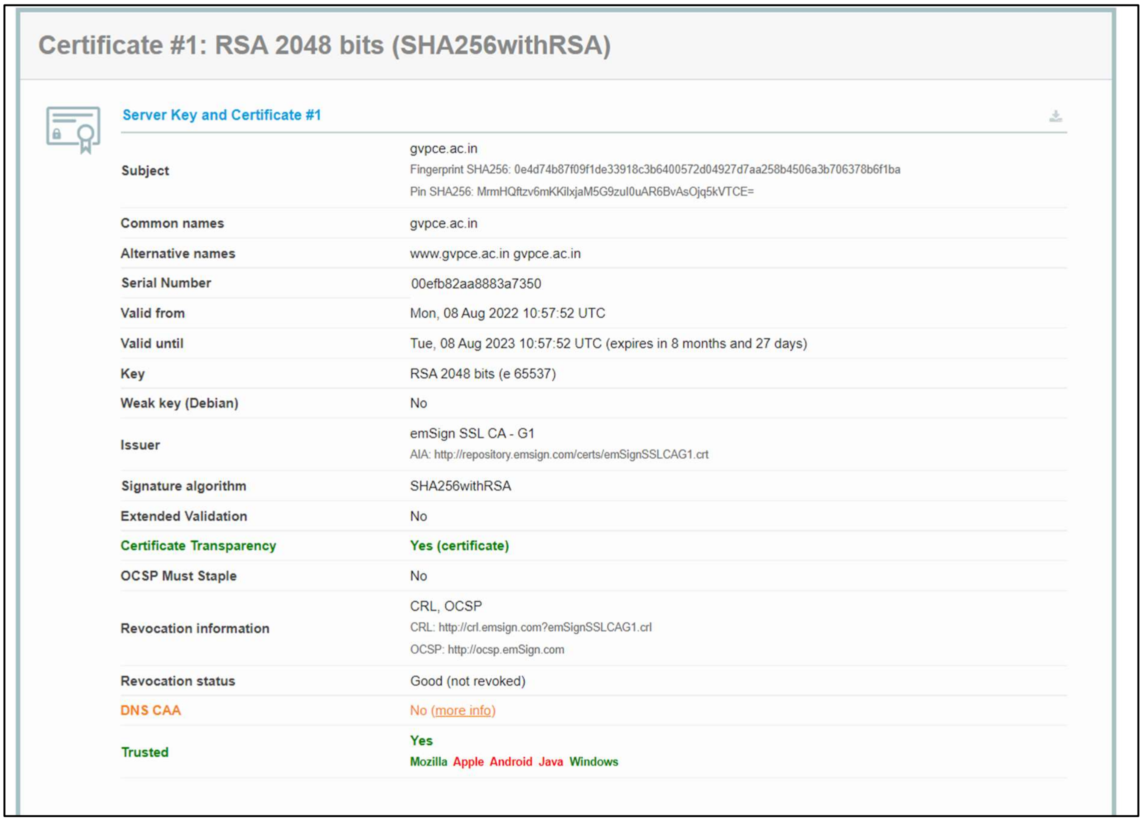
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

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 for the tested website and along with the Server Key



Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	gvpce.ac.in Fingerprint SHA256: 0e4d74b87f09f1de33918c3b6400572d04927d7aa258b4506a3b706378b6f1ba Pin SHA256: MrmHQftzv6mKKilxjaM5G9zuI0uAR6BvAsOjq5kVTCE=
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**