



**Yuvatech**

---

Report generated by Tenable Nessus™

Thu, 06 Feb 2025 14:05:40 India Standard Time

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Plugin

• 142960 (6) - HSTS Missing From HTTPS Server (RFC 6797).....	4
• 11219 (22) - Nessus SYN scanner.....	7
• 84502 (6) - HSTS Missing From HTTPS Server.....	10
• 10107 (4) - HTTP Server Type and Version.....	13
• 11032 (1) - Web Server Directory Enumeration.....	15
• 19506 (1) - Nessus Scan Information.....	16

Nessus Essentials

---

## **Vulnerabilities by Plugin**

---

## 142960 (6) - HSTS Missing From HTTPS Server (RFC 6797)

### Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

### Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

### See Also

<https://tools.ietf.org/html/rfc6797>

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

### Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

### Plugin Output

yuvatech-computers.org.in (tcp/443/www)

```
HTTP/1.1 200 OK
Connection: close
content-type: text/html
last-modified: Thu, 30 Jan 2025 08:39:00 GMT
accept-ranges: bytes
content-length: 2667
date: Thu, 06 Feb 2025 07:46:13 GMT
server: LiteSpeed
```

```
alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
```

The remote HTTPS server does not send the HTTP  
"Strict-Transport-Security" header.

### yuvatech-computers.org.in (tcp/2078/www)

```
HTTP/1.1 401 Unauthorized
Date: Thu, 06 Feb 2025 07:46:14 GMT
Server: cPanel
Persistent-Auth: false
Host: yuvatech-computers.org.in:2078
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Restricted Area"
Content-Length: 36
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT
```

The remote HTTPS server does not send the HTTP  
"Strict-Transport-Security" header.

### yuvatech-computers.org.in (tcp/2080/www)

```
HTTP/1.1 401 Unauthorized
Date: Thu, 06 Feb 2025 07:46:15 GMT
Server: cPanel
Persistent-Auth: false
Host: yuvatech-computers.org.in:2080
Connection: close
WWW-Authenticate: Basic realm="DAV Server"
Content-Length: 36
Content-Type: text/html; charset="utf-8"
```

The remote HTTPS server does not send the HTTP  
"Strict-Transport-Security" header.

### yuvatech-computers.org.in (tcp/2083/www)

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Thu, 06 Feb 2025 07:46:17 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: cpsession=%3ak30tCm2HEPLUr4W4%2c4e5ae42201769f3a92d2e520ef3d3347; HttpOnly; path=/; port=2083; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=yuvatech-computers.org.in; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37767
```

The remote HTTPS server does not send the HTTP  
"Strict-Transport-Security" header.

### yuvatech-computers.org.in (tcp/2087/www)

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Thu, 06 Feb 2025 07:46:16 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
    secure
Set-Cookie: whostmgrsession=%3arbQGfCnEUihlF2lK%2c64185cbb3179f30c243420dbdc954741; HttpOnly;
    path=/; port=2087; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
    port=2087; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=yuvatech-computers.org.in; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
    secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37434
```

The remote HTTPS server does not send the HTTP  
"Strict-Transport-Security" header.

### yuvatech-computers.org.in (tcp/2096/www)

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Thu, 06 Feb 2025 07:46:11 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
    secure
Set-Cookie: webmailsession=%3aLqDkxENHIL6RS3MA%2c1fc0556c7872596950a895748a18b201; HttpOnly; path=/;
    port=2096; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
    port=2096; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=yuvatech-computers.org.in; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
    secure
Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Fri, 06-Feb-2026 07:46:10 GMT; path=/;
    port=2096; secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37779
```

The remote HTTPS server does not send the HTTP  
"Strict-Transport-Security" header.

## 11219 (22) - Nessus SYN scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

### Plugin Output

yuvatech-computers.org.in (tcp/21/ftp)

```
Port 21/tcp was found to be open
```

yuvatech-computers.org.in (tcp/25/smtp)

```
Port 25/tcp was found to be open
```

yuvatech-computers.org.in (tcp/53/dns)

```
Port 53/tcp was found to be open
```

yuvatech-computers.org.in (tcp/80/www)

```
Port 80/tcp was found to be open
```

yuvatech-computers.org.in (tcp/110/pop3)

Port 110/tcp was found to be open

yuvatech-computers.org.in (tcp/143/imap)

Port 143/tcp was found to be open

yuvatech-computers.org.in (tcp/443/www)

Port 443/tcp was found to be open

yuvatech-computers.org.in (tcp/465/smtp)

Port 465/tcp was found to be open

yuvatech-computers.org.in (tcp/587/smtp)

Port 587/tcp was found to be open

yuvatech-computers.org.in (tcp/993/imap)

Port 993/tcp was found to be open

yuvatech-computers.org.in (tcp/995/pop3)

Port 995/tcp was found to be open

yuvatech-computers.org.in (tcp/2077)

Port 2077/tcp was found to be open

yuvatech-computers.org.in (tcp/2078/www)

Port 2078/tcp was found to be open

yuvatech-computers.org.in (tcp/2079)

Port 2079/tcp was found to be open

yuvatech-computers.org.in (tcp/2080/www)

Port 2080/tcp was found to be open

yuvatech-computers.org.in (tcp/2082)



Port 2082/tcp was found to be open

yuvatech-computers.org.in (tcp/2083/www)

Port 2083/tcp was found to be open

yuvatech-computers.org.in (tcp/2086)

Port 2086/tcp was found to be open

yuvatech-computers.org.in (tcp/2087/www)

Port 2087/tcp was found to be open

yuvatech-computers.org.in (tcp/2095)

Port 2095/tcp was found to be open

yuvatech-computers.org.in (tcp/2096/www)

Port 2096/tcp was found to be open

yuvatech-computers.org.in (tcp/3306/mysql)

Port 3306/tcp was found to be open

## 84502 (6) - HSTS Missing From HTTPS Server

### Synopsis

The remote web server is not enforcing HSTS.

### Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

### See Also

<https://tools.ietf.org/html/rfc6797>

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

None

### Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

### Plugin Output

yuvatech-computers.org.in (tcp/443/www)

```
HTTP/1.1 200 OK
Connection: close
content-type: text/html
last-modified: Thu, 30 Jan 2025 08:39:00 GMT
accept-ranges: bytes
content-length: 2667
date: Thu, 06 Feb 2025 07:46:13 GMT
server: LiteSpeed
alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-
Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
```

The remote HTTPS server does not send the HTTP  
"Strict-Transport-Security" header.

yuvatech-computers.org.in (tcp/2078/www)

```
HTTP/1.1 401 Unauthorized
Date: Thu, 06 Feb 2025 07:46:14 GMT
Server: cPanel
Persistent-Auth: false
Host: yuvatech-computers.org.in:2078
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Restricted Area"
Content-Length: 36
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

### yuvatech-computers.org.in (tcp/2080/www)

```
HTTP/1.1 401 Unauthorized
Date: Thu, 06 Feb 2025 07:46:15 GMT
Server: cPanel
Persistent-Auth: false
Host: yuvatech-computers.org.in:2080
Connection: close
WWW-Authenticate: Basic realm="DAV Server"
Content-Length: 36
Content-Type: text/html; charset="utf-8"

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

### yuvatech-computers.org.in (tcp/2083/www)

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Thu, 06 Feb 2025 07:46:17 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: cpsession=%3ak30tCm2HEPLUr4W4%2c4e5ae42201769f3a92d2e520ef3d3347; HttpOnly; path=/;
port=2083; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
port=2083; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=yuvatech-computers.org.in; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37767

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

### yuvatech-computers.org.in (tcp/2087/www)

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
```

```
Date: Thu, 06 Feb 2025 07:46:16 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
Set-Cookie: whostmgrsession=%3arbQGFCnEUihlF2lK%2c64l85cbb3179f30c243420dbdc954741; HttpOnly; path=/; port=2087; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=yuvatech-computers.org.in; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37434
```

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

yuvatech-computers.org.in (tcp/2096/www)

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Thu, 06 Feb 2025 07:46:11 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
Set-Cookie: webmailsession=%3aLqDkxENHIL6RS3MA%2c1fc0556c7872596950a895748a18b201; HttpOnly; path=/; port=2096; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=yuvatech-computers.org.in; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Fri, 06-Feb-2026 07:46:10 GMT; path=/; port=2096; secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37779
```

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

## 10107 (4) - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

yuvatech-computers.org.in (tcp/80/www)

```
The remote web server type is :
```

```
LiteSpeed
```

yuvatech-computers.org.in (tcp/443/www)

```
The remote web server type is :
```

```
LiteSpeed
```

yuvatech-computers.org.in (tcp/2078/www)

```
The remote web server type is :
```

```
cPanel
```

yuvatech-computers.org.in (tcp/2080/www)

The remote web server type is :

cPanel

## 11032 (1) - Web Server Directory Enumeration

### Synopsis

It is possible to enumerate directories on the web server.

### Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

### See Also

<http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location>

### Solution

n/a

### Risk Factor

None

### References

XREF OWASP:OWASP-CM-006

### Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

### Plugin Output

yuvatech-computers.org.in (tcp/443/www)

```
The following directories were discovered:  
/cgi-sys, /mailman
```

```
While this is not, in and of itself, a bug, you should manually inspect  
these directories to ensure that they are in compliance with company  
security standards
```

## 19506 (1) - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

### Plugin Output

yuvatech-computers.org.in (tcp/0)

Information about this scan :

```
Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202502051440
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
```



Scan name : Yuvatech  
Scan policy used : Web Application Tests  
Scanner IP : 192.168.47.153  
Port scanner(s) : nessus\_syn\_scanner  
Port range : default  
Ping RTT : 138.595 ms  
Thorough tests : no  
Experimental tests : no  
Scan for Unpatched Vulnerabilities : no  
Plugin debugging enabled : no  
Paranoia level : 1  
Report verbosity : 1  
Safe checks : yes  
Optimize the test : no  
Credentialed checks : no  
Patch management checks : None  
Display superseded patches : yes (supersedence plugin did not launch)  
CGI scanning : enabled  
Web application tests : enabled  
Web app tests - Test mode : single  
Web app tests - Try all HTTP methods : no  
Web app tests - Maximum run time : 5 minutes.  
Web app tests - Stop at first flaw : CGI  
Max hosts : 30  
Max checks : 4  
Recv timeout : 5  
Backports : None  
Allow post-scan editing : Yes  
Nessus Plugin Signature Checking : Enabled  
Audit File Signature Checking : Disabled  
Scan Start Date : 2025/2/6 13:08 India Standard Time (UTC +05:30)  
Scan duration : 3409 sec  
Scan for malware : no