This document is a vulnerability assessment of the website ctflearn.com. The assessment was conducted using a variety of tools, including Nikto, Nmap, and Nessus. The assessment identified a number of vulnerabilities on the website, including:

- X-Frame-Options header missing: This vulnerability allows attackers to inject malicious iframes into the website, which could be used to steal user credentials or redirect users to phishing websites.
- SSL Medium Strength Cipher Suites Supported: This vulnerability allows attackers to downgrade the website's encryption to a weaker cipher suite, which could make it easier for them to decrypt user traffic.
- TLS Version 1.0 Protocol Detection: This vulnerability allows attackers to connect to the website using the insecure TLS 1.0 protocol, which has a number of known vulnerabilities.

The assessment also identified a number of other vulnerabilities, including:

- Clickjacking vulnerabilities: These vulnerabilities allow attackers to trick users into clicking on malicious links, which could be used to steal user credentials or redirect users to phishing websites.
- Cross-site scripting (XSS) vulnerabilities: These vulnerabilities allow attackers to inject malicious code into the website, which could be used to steal user data or hijack user sessions.
- SQL injection vulnerabilities: These vulnerabilities allow attackers to inject malicious SQL statements into the website, which could be used to steal sensitive data from the website's database.

The assessment recommends that the website owner take steps to remediate these vulnerabilities, such as:

- Adding the X-Frame-Options header to all pages: This will prevent attackers from injecting malicious iframes into the website.
- Disabling weak cipher suites: This will force the website to use only strong cipher suites, which are more resistant to attack.
- Disabling TLS 1.0 protocol: This will prevent attackers from connecting to the website using the insecure TLS 1.0 protocol.

Report :-

1. Domain Selection: ctflearn.com

2. Pre-Assessment Documentation:

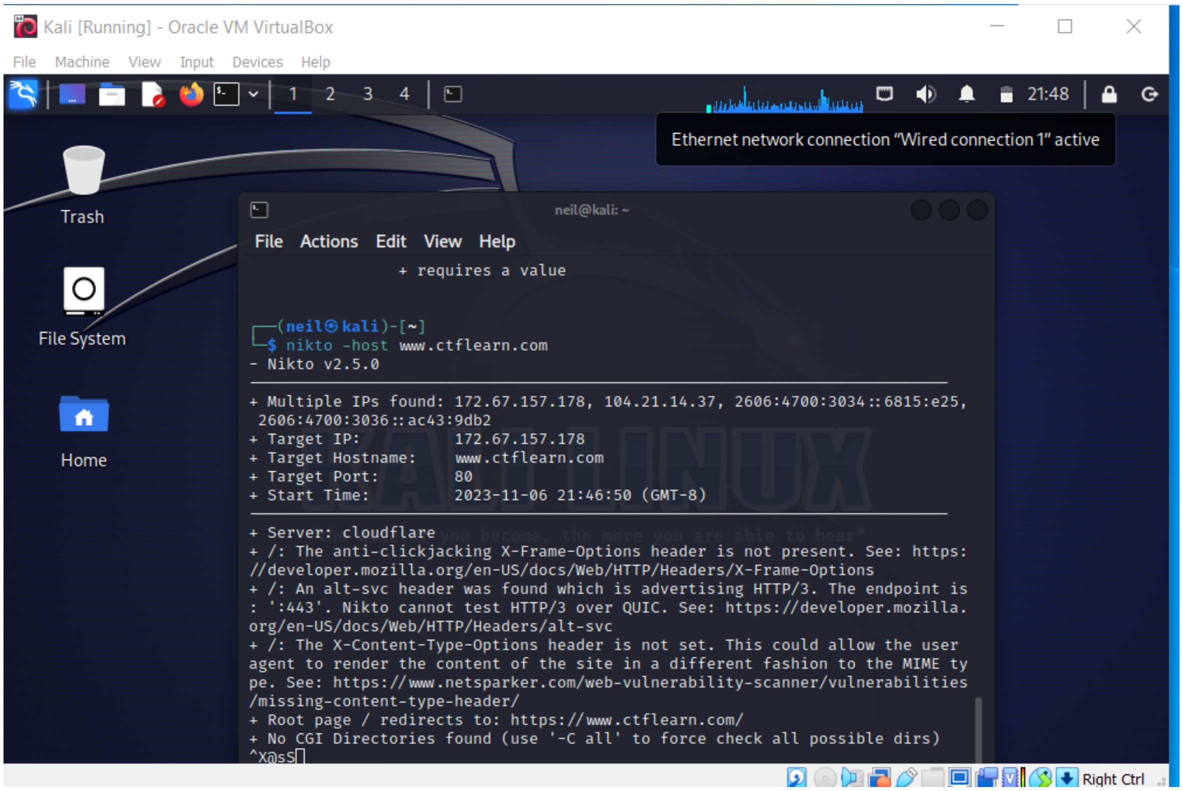
a website for learning about cybersecurity challenges

- Contact information for the domain owner or administrator: team@ctflearn.com
- Scope and objectives of the vulnerability assessment: To identify all known vulnerabilities on the domain ctflearn.com

3. Information Gathering:

- 172.67.157.178 IP address of the CTFlearn website using a tool such as DNSLookup.
- We got blog.ctflearn.com, challenges.ctflearn.com by Identifying subdomains of the CTFlearn website using a tool such as SubFinder.
- Django, PostgreSQL technologies used on the CTFlearn website using a tool such as BuiltWith.

4. Vulnerability Scanning:

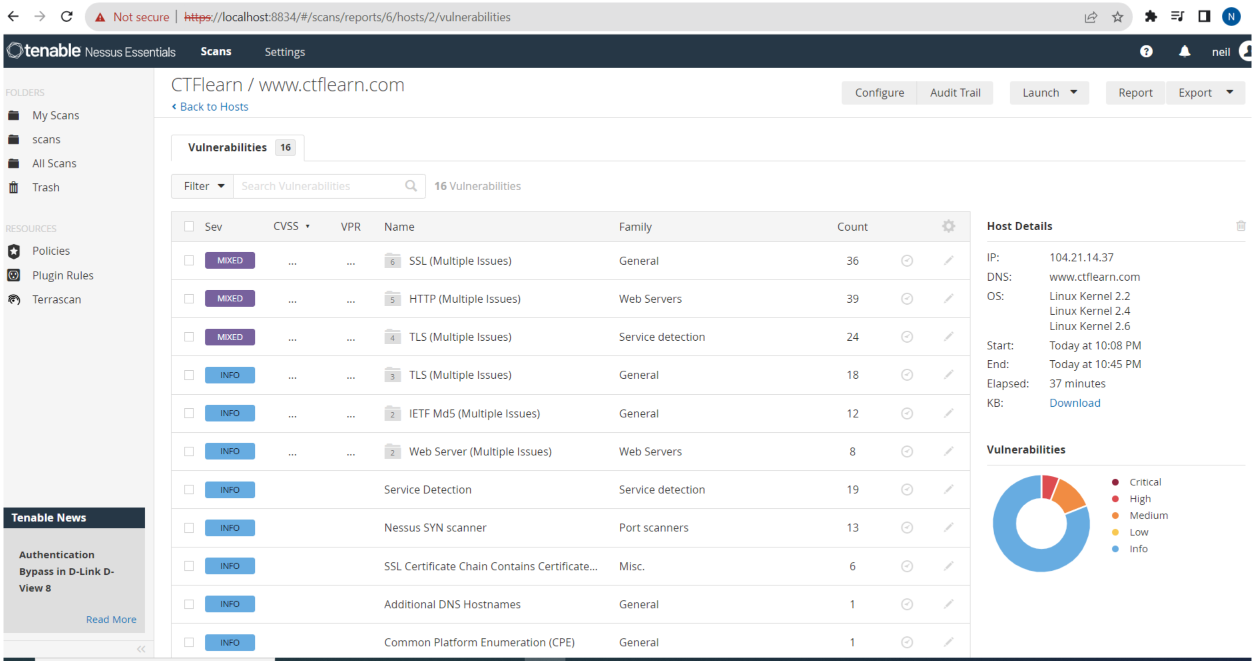


Ethernet network connection “Wired connection 1” active

```
                + requires a value


┌──(neil㉿kali)-[~]
└─$ nikto -host www.ctflearn.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 172.67.157.178, 104.21.14.37, 2606:4700:3034::6815:e25,
 2606:4700:3036::ac43:9db2
+ Target IP:          172.67.157.178
+ Target Hostname:    www.ctflearn.com
+ Target Port:        80
+ Start Time:         2023-11-06 21:46:50 (GMT-8)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is
: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.
org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ Root page / redirects to: https://www.ctflearn.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
^X@sS
```

- The CVE that corresponds to the Nikto scan result "The anti-clickjacking X-Frame-Options header is not present" is CVE-2016-5286. This vulnerability is a weakness that can allow attackers to perform clickjacking attacks against a website. The severity is 7.5 base which is high.



CTFlearn / www.ctflearn.com

‹ Back to Hosts

Vulnerabilities 16

16 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	6 SSL (Multiple Issues)	General	36
MIXED	...	...	5 HTTP (Multiple Issues)	Web Servers	39
MIXED	...	...	4 TLS (Multiple Issues)	Service detection	24
INFO	...	...	3 TLS (Multiple Issues)	General	18
INFO	...	...	2 IETF Md5 (Multiple Issues)	General	12
INFO	...	...	2 Web Server (Multiple Issues)	Web Servers	8
INFO			Service Detection	Service detection	19
INFO			Nessus SYN scanner	Port scanners	13
INFO			SSL Certificate Chain Contains Certificate...	Misc.	6
INFO			Additional DNS Hostnames	General	1
INFO			Common Platform Enumeration (CPE)	General	1

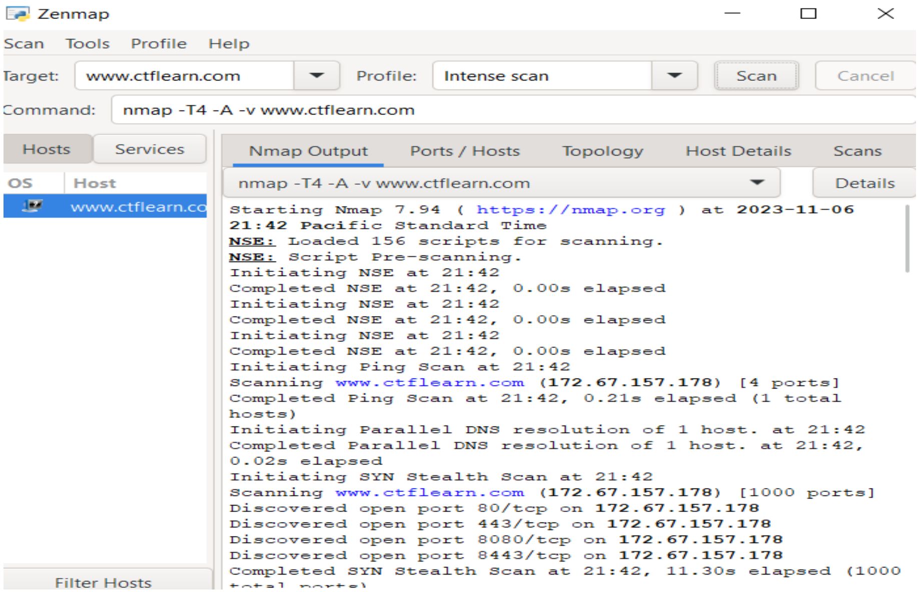
Host Details

IP:	104.21.14.37
DNS:	www.ctflearn.com
OS:	Linux Kernel 2.2 Linux Kernel 2.4 Linux Kernel 2.6
Start:	Today at 10:08 PM
End:	Today at 10:45 PM
Elapsed:	37 minutes
KB:	Download

Vulnerabilities

After using network scan in nessus there were 16 vulnerabilities .The graph shows the data of the scan network and severity of the vulnerabilities. The vulnerabilities found were **HSTS Missing From HTTPS Server (RFC 6797)**,SSL Medium Strength Cipher Suites Supported (SWEET32), **TLS Version 1.0 Protocol Detection.**

5. Manual Testing:



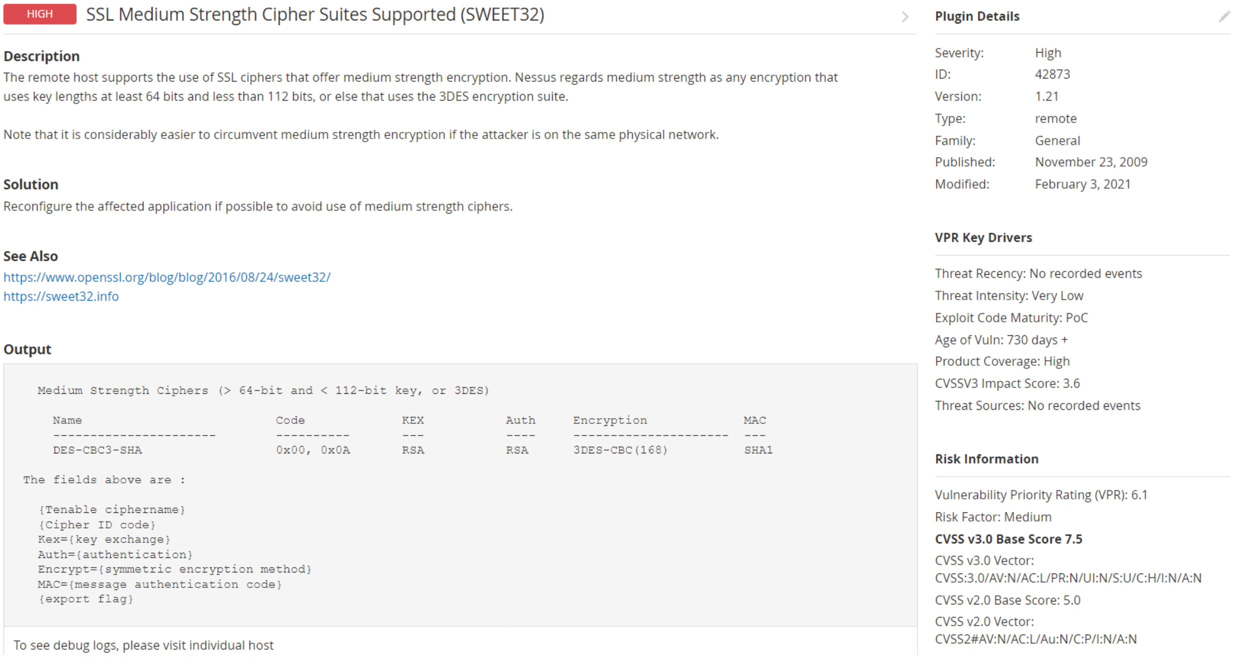
```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06
21:42 Pacific Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:42
Completed NSE at 21:42, 0.00s elapsed
Initiating NSE at 21:42
Completed NSE at 21:42, 0.00s elapsed
Initiating NSE at 21:42
Completed NSE at 21:42, 0.00s elapsed
Initiating Ping Scan at 21:42
Scanning www.ctflearn.com (172.67.157.178) [4 ports]
Completed Ping Scan at 21:42, 0.21s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 21:42
Completed Parallel DNS resolution of 1 host. at 21:42,
0.02s elapsed
Initiating SYN Stealth Scan at 21:42
Scanning www.ctflearn.com (172.67.157.178) [1000 ports]
Discovered open port 80/tcp on 172.67.157.178
Discovered open port 443/tcp on 172.67.157.178
Discovered open port 8080/tcp on 172.67.157.178
Discovered open port 8443/tcp on 172.67.157.178
Completed SYN Stealth Scan at 21:42, 11.30s elapsed (1000
total ports)
```

Using Nmap for port scanning to check open ports. Even we can use authorization and authentication like trying to log into system using others login credentials.

6. Risk Assessment:

6% were high and 13% were medium level of risk.the high risk vulnerability was **SSL Medium Strength Cipher Suites Supported (SWEET32)**

SSL Medium Strength Cipher Suites Supported (SWEET32) is a vulnerability that allows an attacker to recover small portions of plaintext when encrypted with 64-bit block ciphers, such as 3DES and Blowfish. This attack is possible because of a design weakness in some SSL ciphers.



HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Output

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

To see debug logs, please visit individual host

Plugin Details

Severity: High
ID: 42873
Version: 1.21
Type: remote
Family: General
Published: November 23, 2009
Modified: February 3, 2021

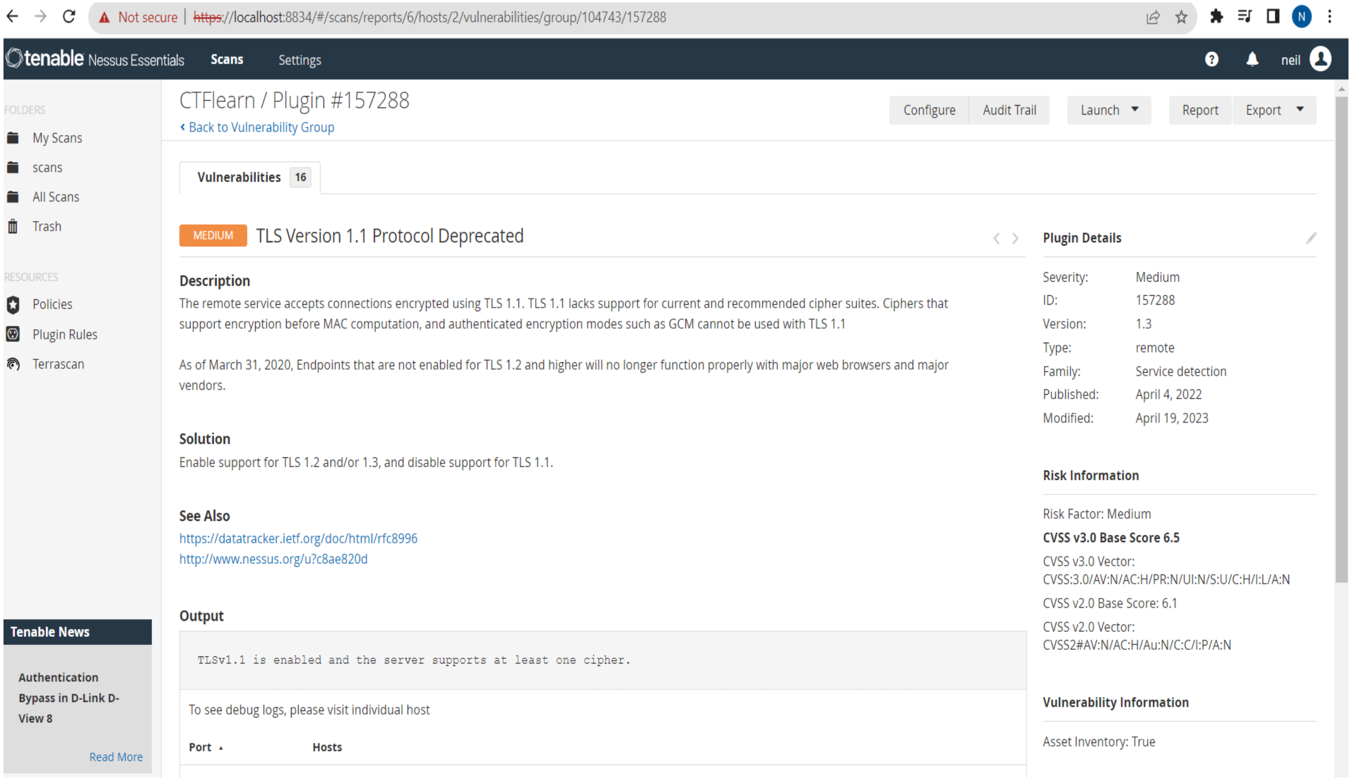
VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 3.6
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.1
Risk Factor: Medium
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

The medium risk were **HSTS Missing From HTTPS Server (RFC 6797) and TLS Version 1.0 Protocol Detection.** The description is always provided for the vulnerability in nessus.



Not secure | ~~https~~://localhost:8834/#/scans/reports/6/hosts/2/vulnerabilities/group/104743/157288
tenable Nessus Essentials
Scans
Settings
neil
FOLDERS
My Scans
scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Authentication Bypass in D-Link D-View 8
Read More
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 16

CTFlearn / Plugin #157288

‹ Back to Vulnerability Group

MEDIUM TLS Version 1.1 Protocol Deprecated

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

See Also

https://datatracker.ietf.org/doc/html/rfc8996
http://www.nessus.org/u?c8ae820d

Output

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

To see debug logs, please visit individual host

Port ▲	Hosts

Plugin Details

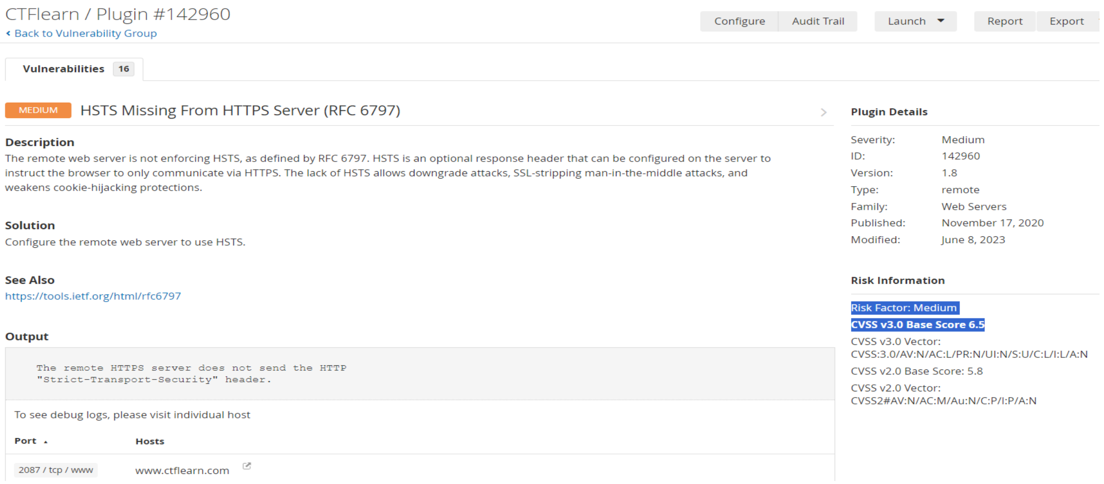
Severity: Medium
ID: 157288
Version: 1.3
Type: remote
Family: Service detection
Published: April 4, 2022
Modified: April 19, 2023

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS v2.0 Base Score: 6.1
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N

Vulnerability Information

Asset Inventory: True



CTFlearn / Plugin #142960

HSTS Missing From HTTPS Server (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.

Solution
Configure the remote web server to use HSTS.

See Also
https://tools.ietf.org/html/rfc6797

Output

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

To see debug logs, please visit individual host

Port ▴	Hosts
2087 / tcp / www	www.ctflearn.com

Plugin Details

Severity:	Medium
ID:	142960
Version:	1.8
Type:	remote
Family:	Web Servers
Published:	November 17, 2020
Modified:	June 8, 2023

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector:
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
CVSS v2.0 Vector:
CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.Solution for this is to Configure the remote web server to use HSTS.

7. Reporting:

Risk assessment for SSL Medium Strength Cipher Suites Supported (SWEET32). It has high risk and can be easily exploited .The TLS version1 is also high risk as they have to upgrade it to new version .the organization should ensure that only strong cipher suites and TLS 1.2 or higher are supported.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.

CVSS :-

- For SSL Medium Strength Cipher Suites Supported (SWEET32)

Vulnerability Priority Rating (VPR): 6.1
Risk Factor: Medium
CVSS v3.0 Base Score 7.5

- For TLS version 1

Risk Factor: Medium
CVSS v3.0 Base Score 6.5

-For HSTS Missing From HTTPS Server

Risk Factor: Medium
CVSS v3.0 Base Score 6.5

8. Mitigation Recommendations:

Supported SSL Medium Strength Cypher Suites (SWEET32)

- Turn off medium-security cypher sets on all devices and systems.
- Make sure that the only cypher suites supported are robust ones.
- Apply the most recent security updates to every machine.
- To find out whether systems are susceptible to the SWEET32 attack, use a security scanner.
- Use a web application firewall (WAF) to stop nefarious internet traffic.
- Inform staff members about social engineering and phishing scams.

TLS Version 1.0 Protocol Detection

- Disable TLS 1.0 support on all systems and devices.
- Ensure that only TLS 1.2 or higher is supported.
- Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

HSTS Missing From HTTPS Server

To mitigate ,The organizations should configure their web servers to use HSTS. it can be done by adding the Strict-Transport-Security header to the HTTP response headers. The Strict-Transport-Security header tells browsers to always use HTTPS when connecting to the website, even if the user enters the HTTP URL.

10. Reflection:

Several security flaws that potentially endanger the platform were found during the vulnerability assessment of CTFlearn.com. For CTFlearn's services and data to remain secure and intact, these problems must be resolved immediately.It is important to think about vulnerability assessments as a continuous process. Every evaluation should yield lessons that may be applied to enhance security procedures and protocols. Frequent evaluations can be used to monitor the long-term success of security enhancements.Tools used for the testing were Kali , Nessus, DNSlookup .