Sri Lanka Institute of Information Technology

BUG BOUNTY REPORT - 5

Web Security – IE2062

IT22362780

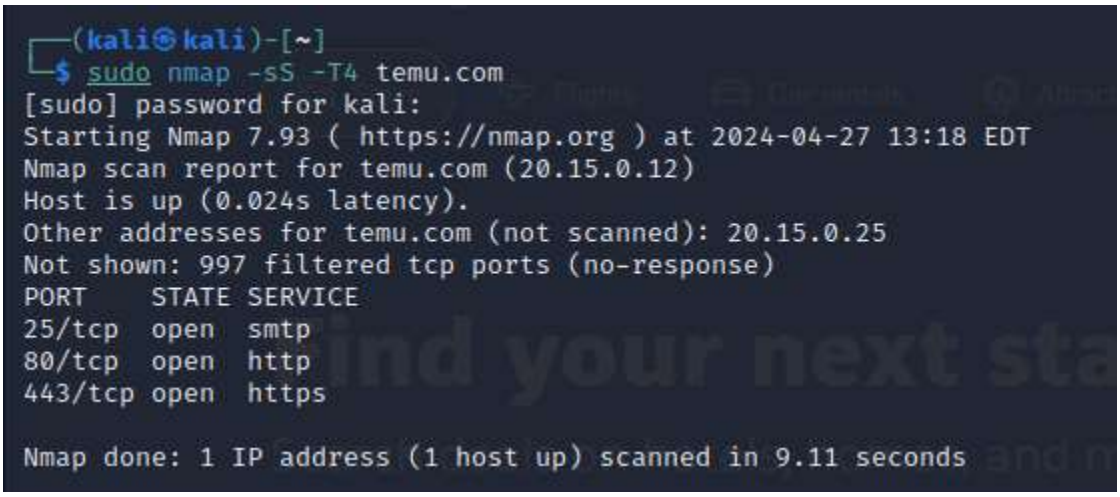
Jayaweera N.S

Report Details

Report #	- 05
Domain	- https://temu.com
Platform	-bugcrowd.com
Scans performed -	Nmap scan Nslookup metasploit Wafw00f scan Dotdotpwn scan Nikto scan Sqlmap scan Manual scanning using Wapplyzer Recon-ng scan

Nmap scan

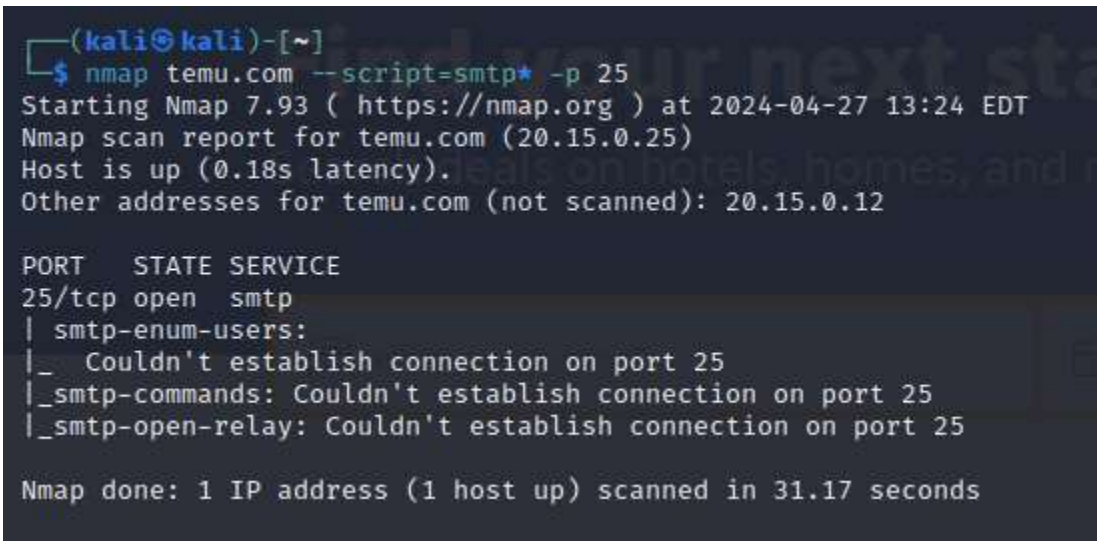
Using nmap scan all the open ports in the target can be identified.



No unusual ports are open.

But Smtp port 25 is vulnerable when it's opened, because it lacks authentication and encryption.

Let's see if we can establish a connection on port 25.

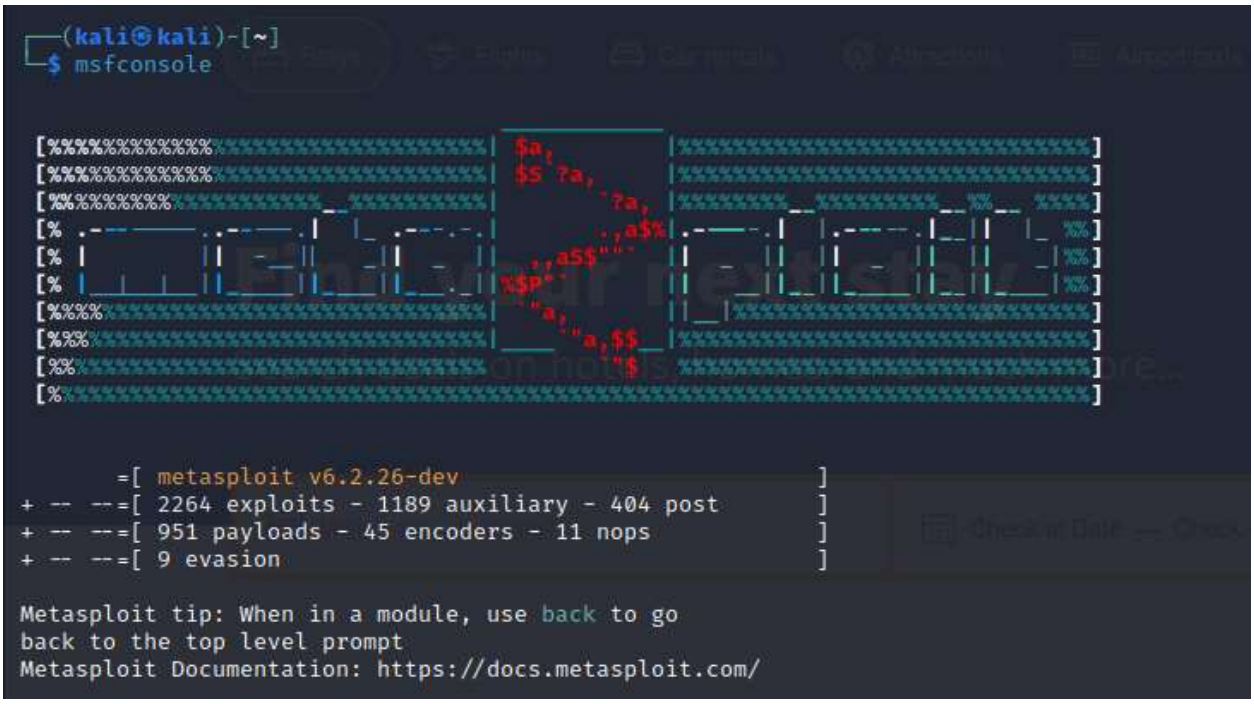


Connection cannot be established therefore a vulnerability cannot be identified.

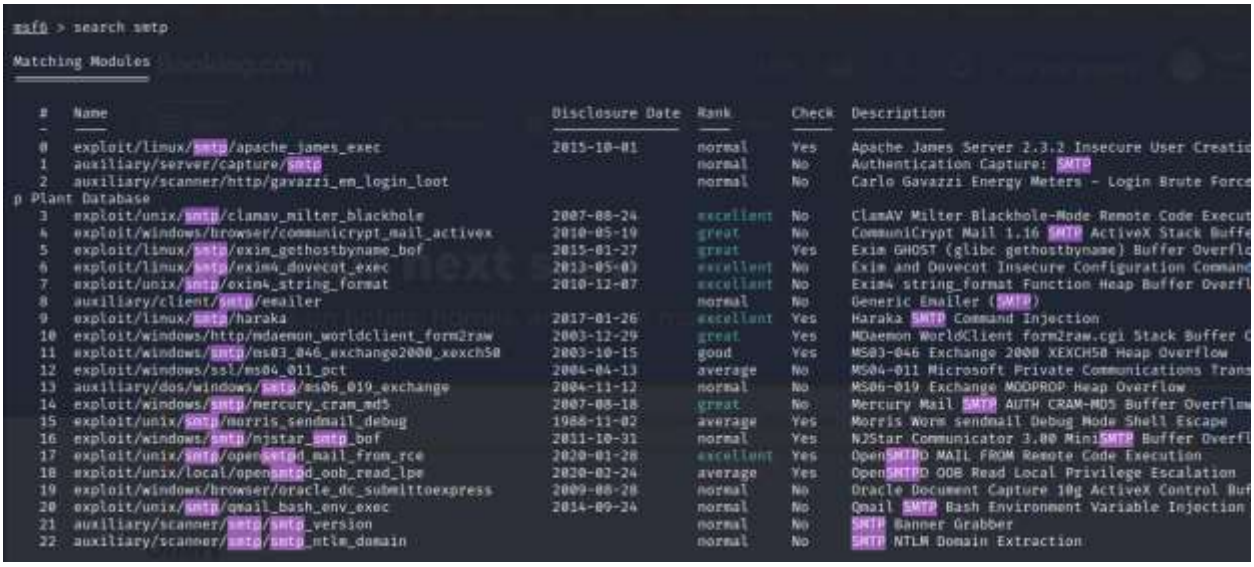
Nslookup

The ip address of temu.com can be found.

Metasploit



Search for smtp



The module “fuzzer” is used to fuzz the smtp service. And “smtp_enum” is used for the username enumeration.

Set the RHOSTS to temu.com

Fuzzing failed due to connection time out indicating inability to enumerate the service. Fuzzing attempts are blocked by the server.

Nikto scan

Results obtained from the scan:

- The anti-clickjacking "X-Frame-Options" header, which helps prevent clickjacking attacks, is not present.

- The "X-XSS-Protection" header is not defined, which can protect against some forms of XSS.

- The site uses SSL and Expect -CT header is not present.

The "expect-CT" header is a security feature that helps websites, and their users avoid the risks associated with incorrectly issued SSL certificates.

It supports transparency and accountability when issuing SSL certificates, which improves overall web security.

There are some issues/disadvantages occurred when the “expect-CT” header is absent:

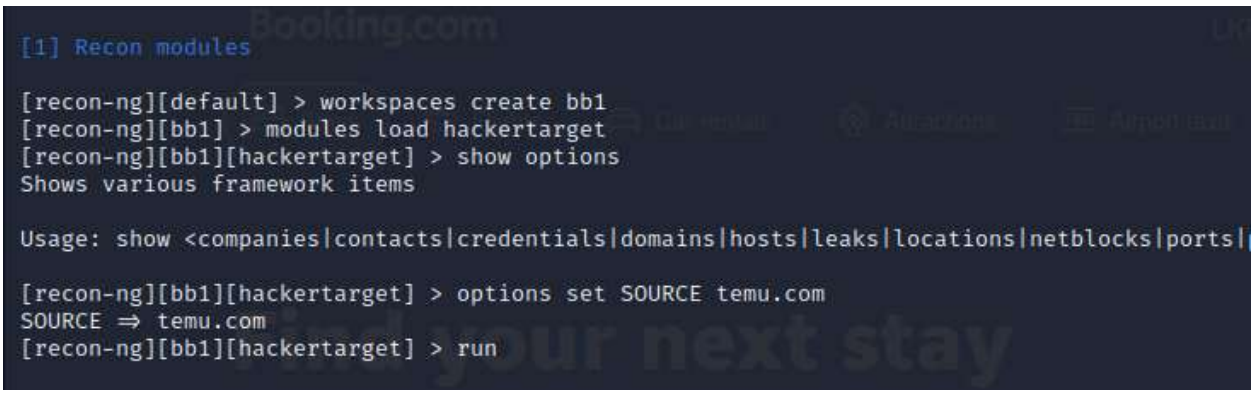
- The protection against the mis issuing of SSL certificates will be low.
- Mismanagement of SSL certificates.
- No trust and security

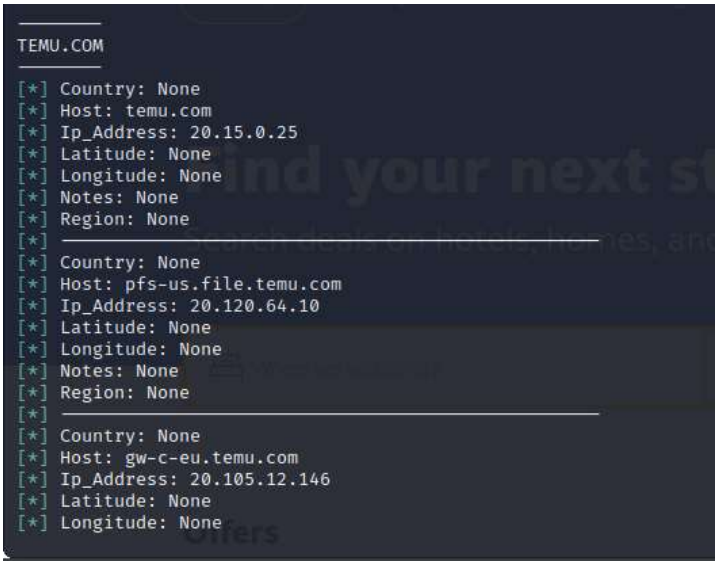
But the absence of “expected-CT” header is not a huge vulnerability or a security issue in a website.

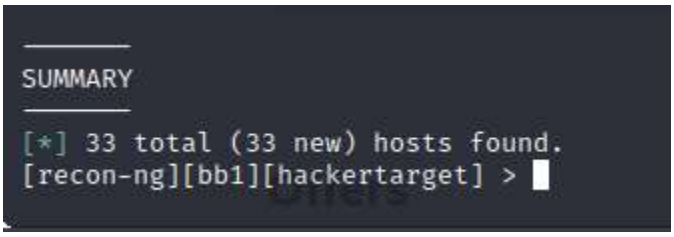
- The site uses SSL and the Strict-transport-security HTTP header is not defined.
- The X-content-Type-options header is not set.

Recon-ng

here the recon-ng will be used to find all the sub domains in the target.







33 sub domains were found.

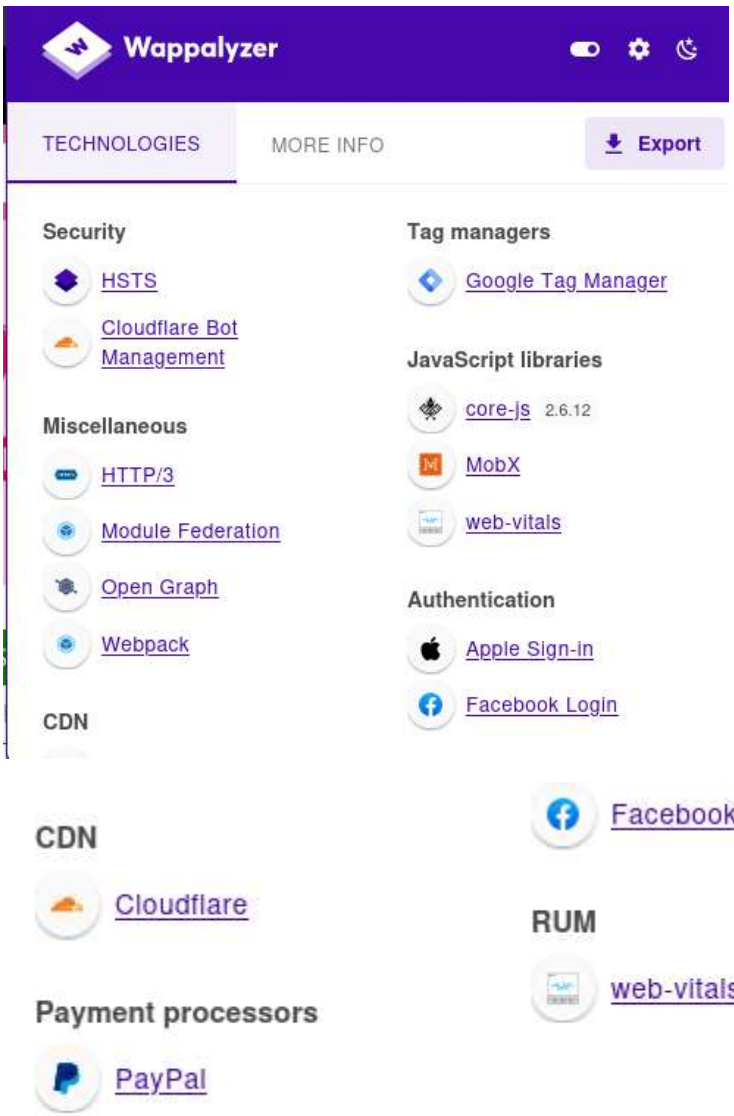
Wafw00f scan

Used to identify the type of WAF that is used to protect the web application.

According to the test results, “Cloudflare (Cloudflare Inc.)” is used as the firewall of the web application.

Wapplyzer

The Wapplyzer is used to identify the technologies used in the web application.



these are the technologies used.

The java script library contains a core.js

[1] figure from https://security.snyk.io

there are no directl vulnerabilities in this version of core.js

Dotdotpwn

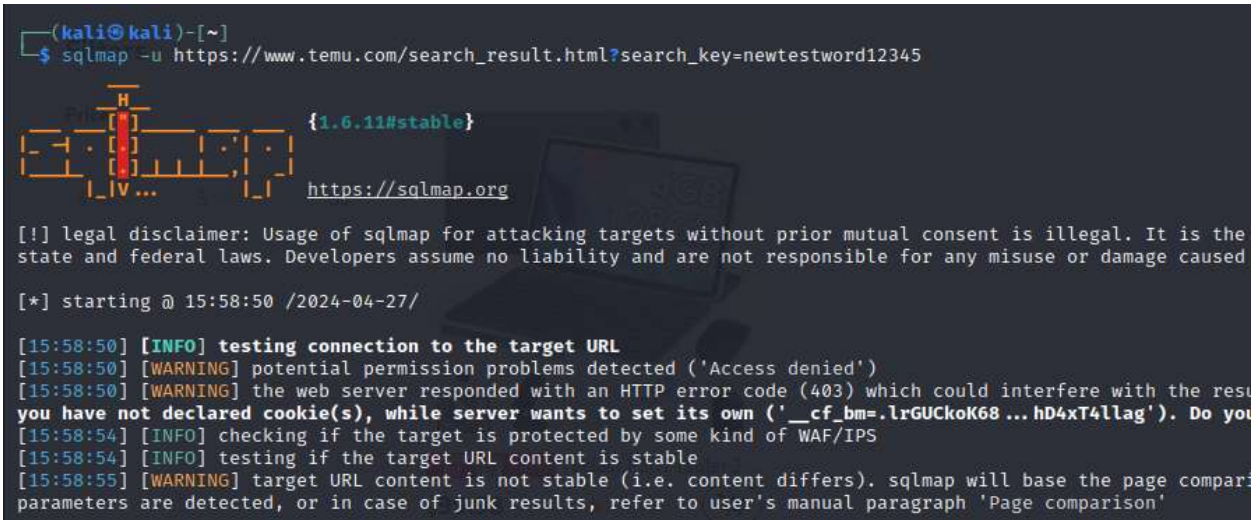
Dotdotpwn is a directory traversal checker.

The scan results returned status codes within the range 400 (400-499). It shows a client error.

Therefore, we can conclude that the tested destinations are not vulnerable to a directory traversal.

Sqlmap

With the use of this scan, we can identify whether a sql injection can be done or not.



there is no injection vulnerability in the above web application.