Sri Lanka Institute of Information Technology

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2023

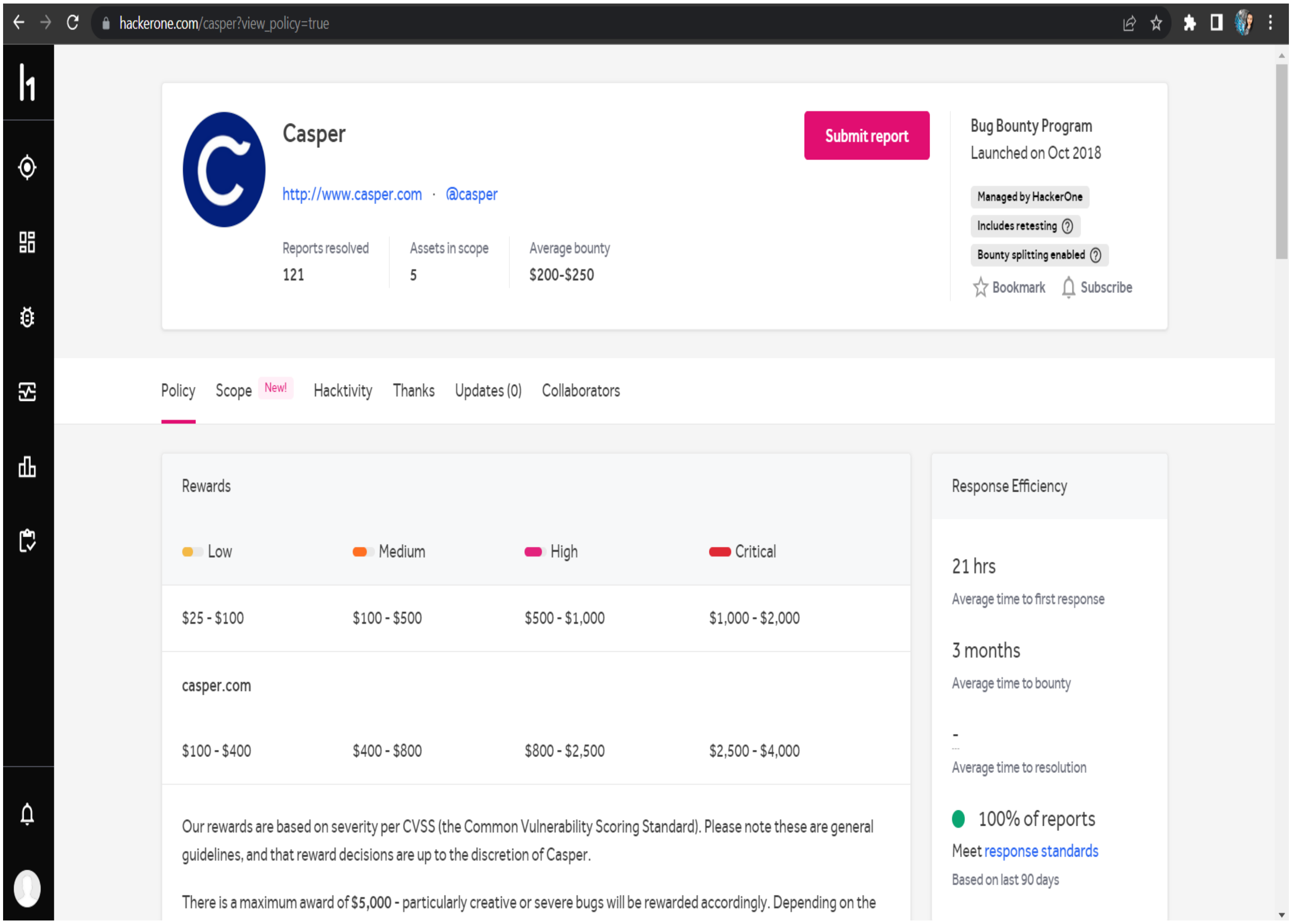
Bug Bounty vulnerabilities scanning Report 5

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

Casper.com

How does Casper.com work?

A firm that offers sleep items online and in physical stores is called Casper Sleep (also known as Casper). The business has offices in New York City and other cities, as well as showrooms there.



hackerone.com/casper?view_policy=true

Casper

http://www.casper.com · @casper

Reports resolved	Assets in scope	Average bounty
121	5	$200-$250

Bug Bounty Program
Launched on Oct 2018

Managed by HackerOne
Includes retesting
Bounty splitting enabled

Rewards

Low	Medium	High	Critical
$25 - $100	$100 - $500	$500 - $1,000	$1,000 - $2,000
casper.com			
$100 - $400	$400 - $800	$800 - $2,500	$2,500 - $4,000

Our rewards are based on severity per CVSS (the Common Vulnerability Scoring Standard). Please note these are general guidelines, and that reward decisions are up to the discretion of Casper.

There is a maximum award of $5,000 - particularly creative or severe bugs will be rewarded accordingly. Depending on the

Response Efficiency

21 hrs
Average time to first response

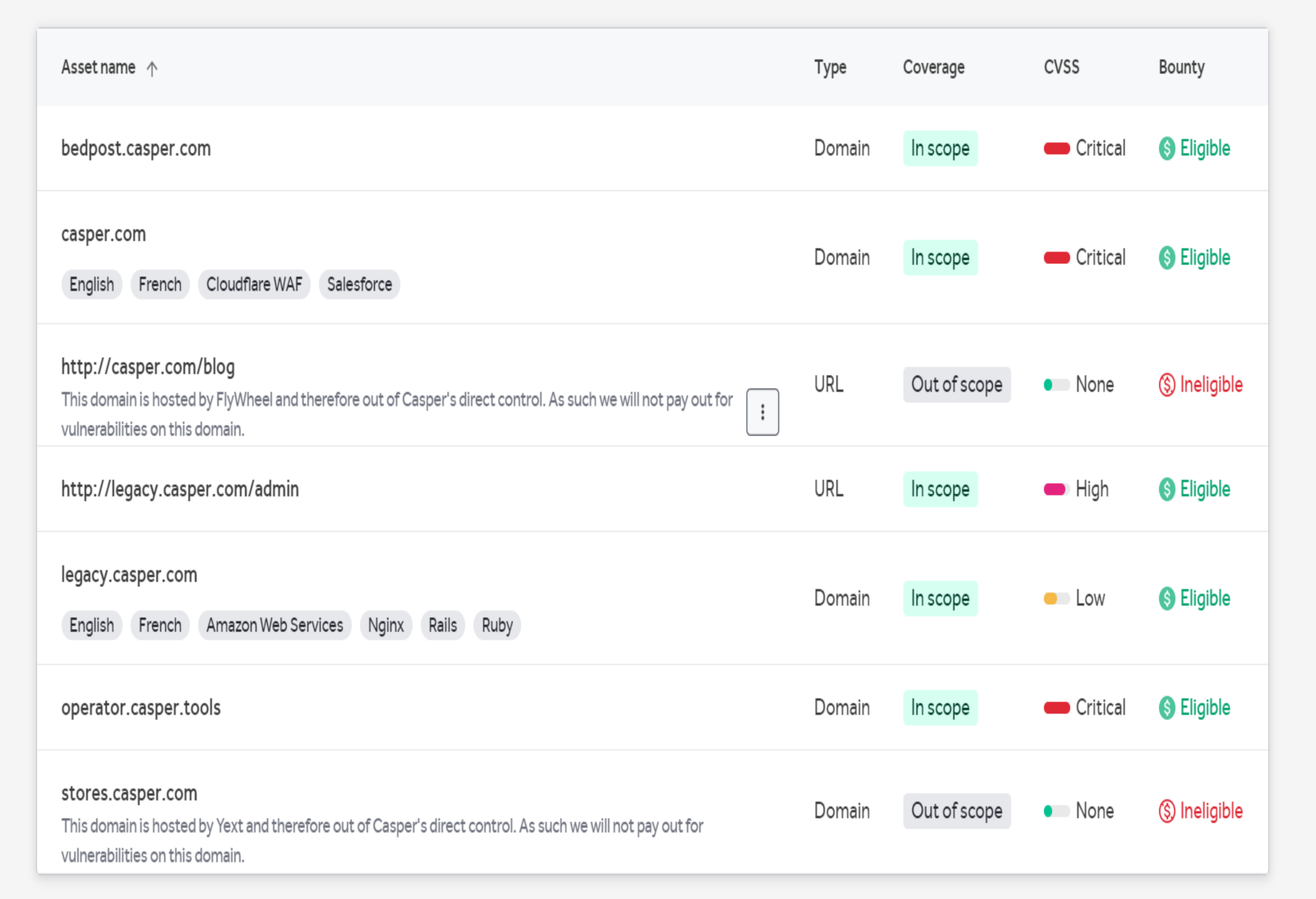
3 months
Average time to bounty

-
Average time to resolution

100% of reports
Meet response standards
Based on last 90 days

- ## Assessment scope

Scope of the security audit according https://hackerone.com/casper?type=team is as follows,



Asset name ↑	Type	Coverage	CVSS	Bounty
bedpost.casper.com	Domain	In scope	Critical	Eligible
casper.com English French Cloudflare WAF Salesforce	Domain	In scope	Critical	Eligible
http://casper.com/blog This domain is hosted by FlyWheel and therefore out of Casper's direct control. As such we will not pay out for vulnerabilities on this domain.	URL	Out of scope	None	Ineligible
http://legacy.casper.com/admin	URL	In scope	High	Eligible
legacy.casper.com English French Amazon Web Services Nginx Rails Ruby	Domain	In scope	Low	Eligible
operator.casper.tools	Domain	In scope	Critical	Eligible
stores.casper.com This domain is hosted by Yext and therefore out of Casper's direct control. As such we will not pay out for vulnerabilities on this domain.	Domain	Out of scope	None	Ineligible

In scope

- ✓ bedpost.casper.com
- ✓ casper.com
- ✓ http://legacy.casper.com/admin
- ✓ legacy.casper.com
- ✓ operator.casper.tools

Out scope

- ✓ **http://casper.com/blog**
- ✓ stores.casper.com

Subdomains for Hunting

Enumerating sub-domains for one or more domains is the process of doing so. It's an important step in the reconnaissance process. A security evaluation may encompass numerous domains and sub-domains, which improves the likelihood of discovering vulnerabilities. This is known as sub-domain enumeration.

Using obscure, abandoned sub-domains to locate programs may uncover major flaws.

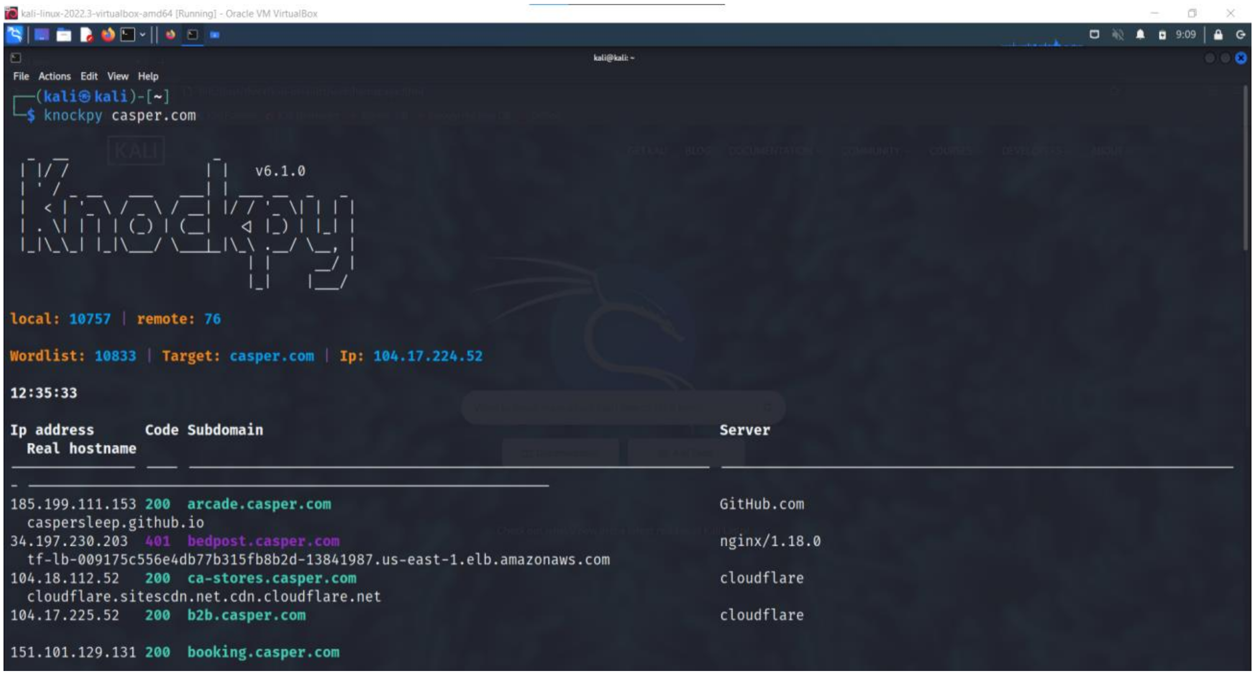
The same vulnerabilities are frequently found across several domains and apps within a single corporation.

Describe Knockpy?

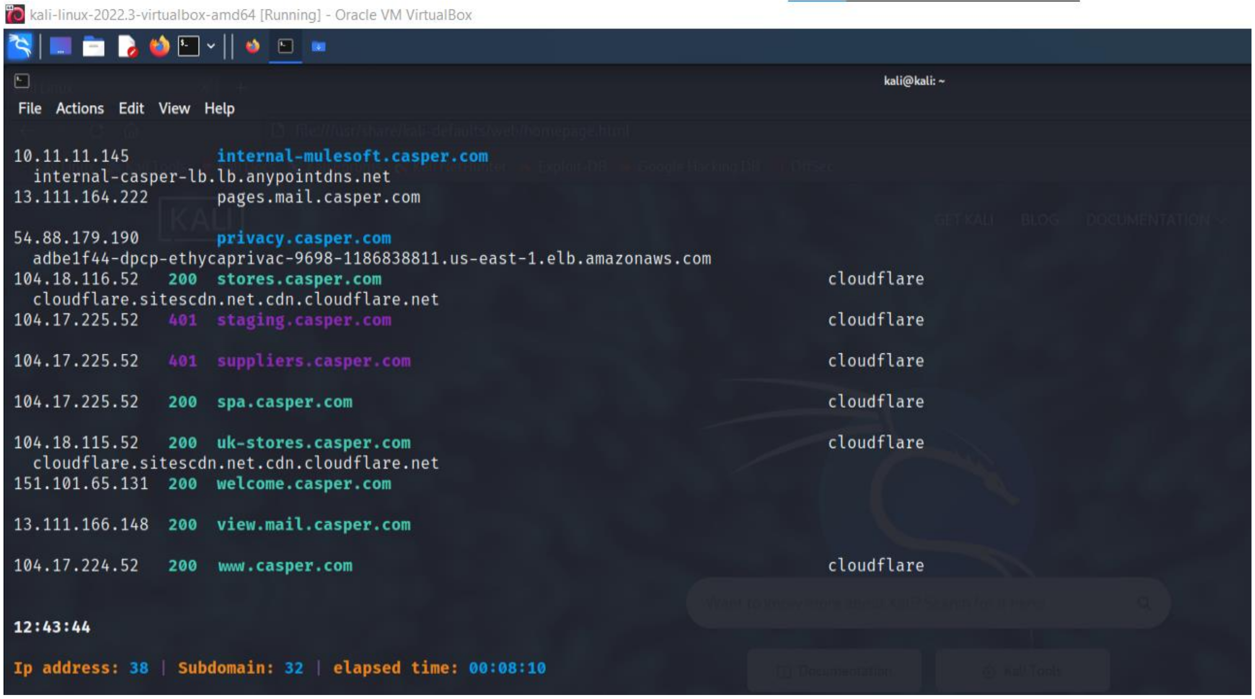
The usage of knockoff-based inference is made simple by the knockpy Python implementation of the knockoffs framework. Researchers and analysts may easily add functionality to Knockpy thanks to its modular nature.

• knockpy subdomain search,

Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.
How to Find Subdomain in Knockpy: knockpy <Domain Name>


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
9:09
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ knockpy casper.com

  _  __                 _
 | |/ /                | |   v6.1.0
 | ' / _ __   ___   ___| | ___ __  _   _
 |  < | '_ \ / _ \ / __| |/ / '_ \| | | |
 | . \| | | | (_) | (__|   <| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/

local: 10757 | remote: 76

Wordlist: 10833 | Target: casper.com | Ip: 104.17.224.52

12:35:33

Ip address      Code Subdomain                                                Server
  Real hostname
_______________ ____ ____________________________________________________________ ______________________________________________________________
- _______________________________________________________________

185.199.111.153 200  arcade.casper.com                                        GitHub.com
  caspersleep.github.io
34.197.230.203  401  bedpost.casper.com                                       nginx/1.18.0
  tf-lb-009175c556e4db77b315fb8b2d-13841987.us-east-1.elb.amazonaws.com
104.18.112.52   200  ca-stores.casper.com                                     cloudflare
  cloudflare.sitescdn.net.cdn.cloudflare.net
104.17.225.52   200  b2b.casper.com                                           cloudflare

151.101.129.131 200  booking.casper.com
```


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help

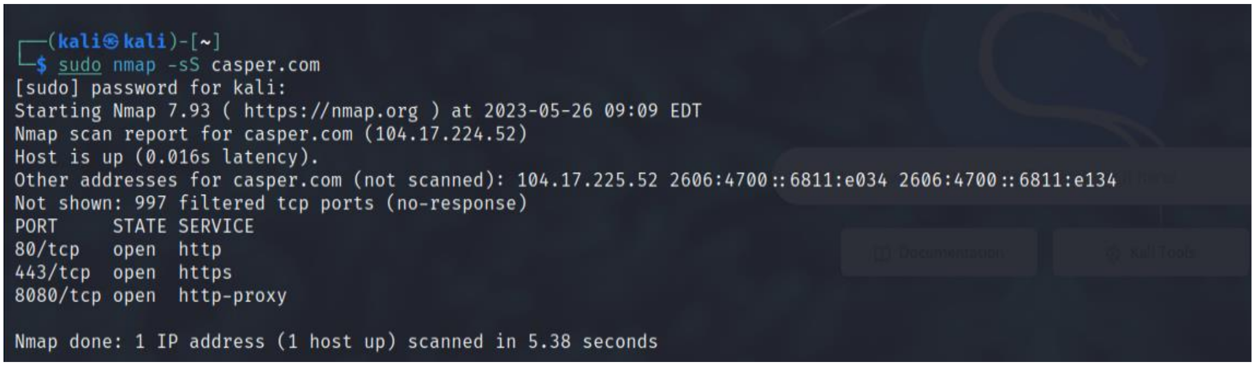
```
10.11.11.145        internal-mulesoft.casper.com
  internal-casper-lb.lb.anypointdns.net
13.111.164.222      pages.mail.casper.com

54.88.179.190       privacy.casper.com
  adbe1f44-dpcp-ethycaprivac-9698-1186838811.us-east-1.elb.amazonaws.com
104.18.116.52   200  stores.casper.com                                          cloudflare
  cloudflare.sitescdn.net.cdn.cloudflare.net
104.17.225.52   401  staging.casper.com                                         cloudflare

104.17.225.52   401  suppliers.casper.com                                       cloudflare

104.17.225.52   200  spa.casper.com                                             cloudflare

104.18.115.52   200  uk-stores.casper.com                                       cloudflare
  cloudflare.sitescdn.net.cdn.cloudflare.net
151.101.65.131  200  welcome.casper.com

13.111.166.148  200  view.mail.casper.com

104.17.224.52   200  www.casper.com                                             cloudflare


12:43:44

Ip address: 38 | Subdomain: 32 | elapsed time: 00:08:10
```

- ## Open Ports Enumeration applying with nmap

A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and cannot be used for anything else if a service uses it. Open ports offer a security risk if the services operating on them are improperly configured, unsecure, or unpatched.

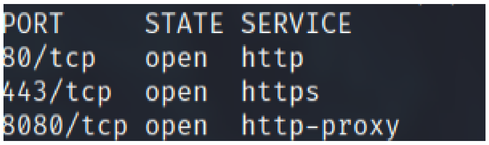
Using Nmap to List Open Ports

The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS casper.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-26 09:09 EDT
Nmap scan report for casper.com (104.17.224.52)
Host is up (0.016s latency).
Other addresses for casper.com (not scanned): 104.17.225.52 2606:4700::6811:e034 2606:4700::6811:e134
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 5.38 seconds
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
8080/tcp	open	http-proxy

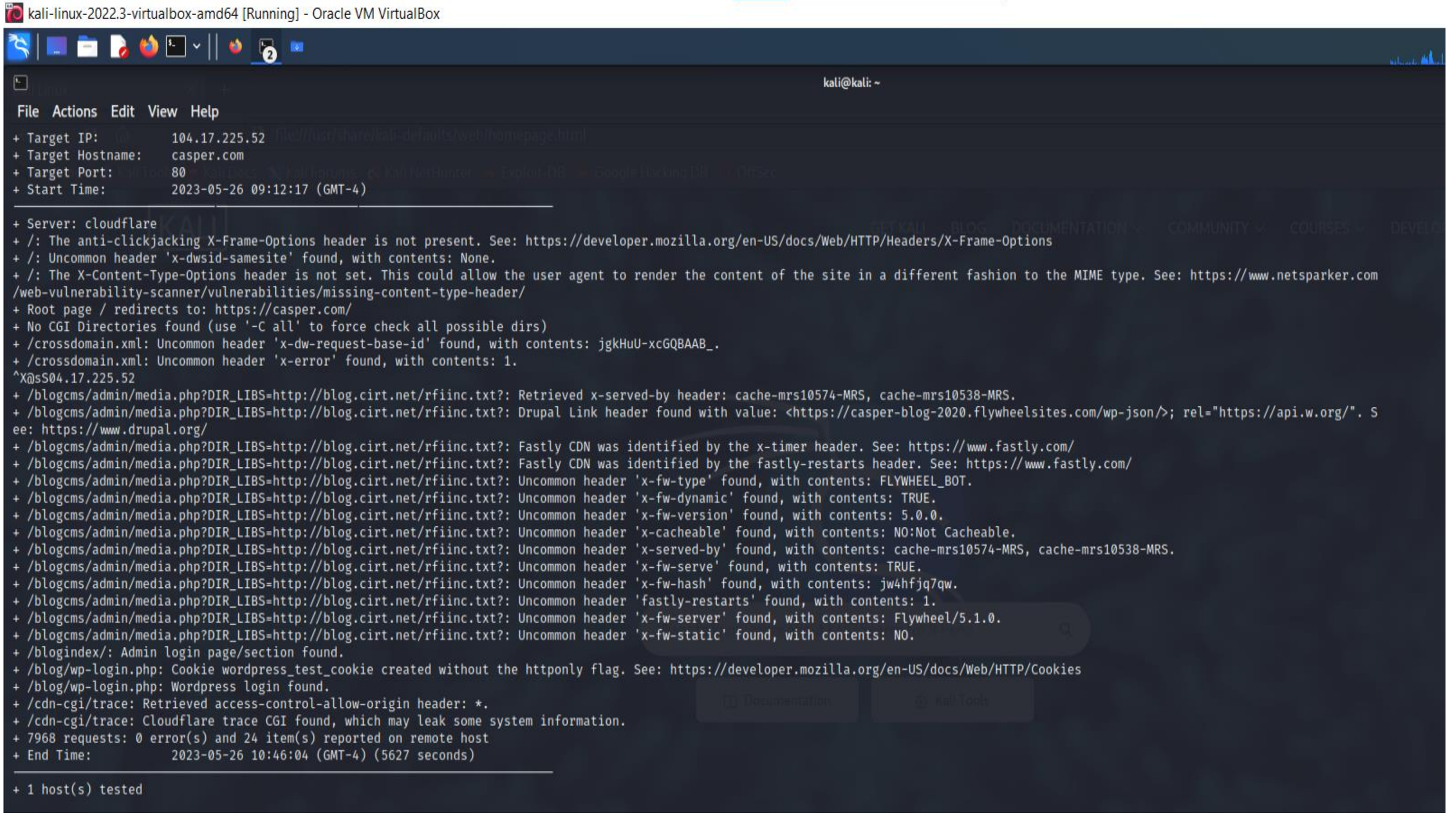


```
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
```

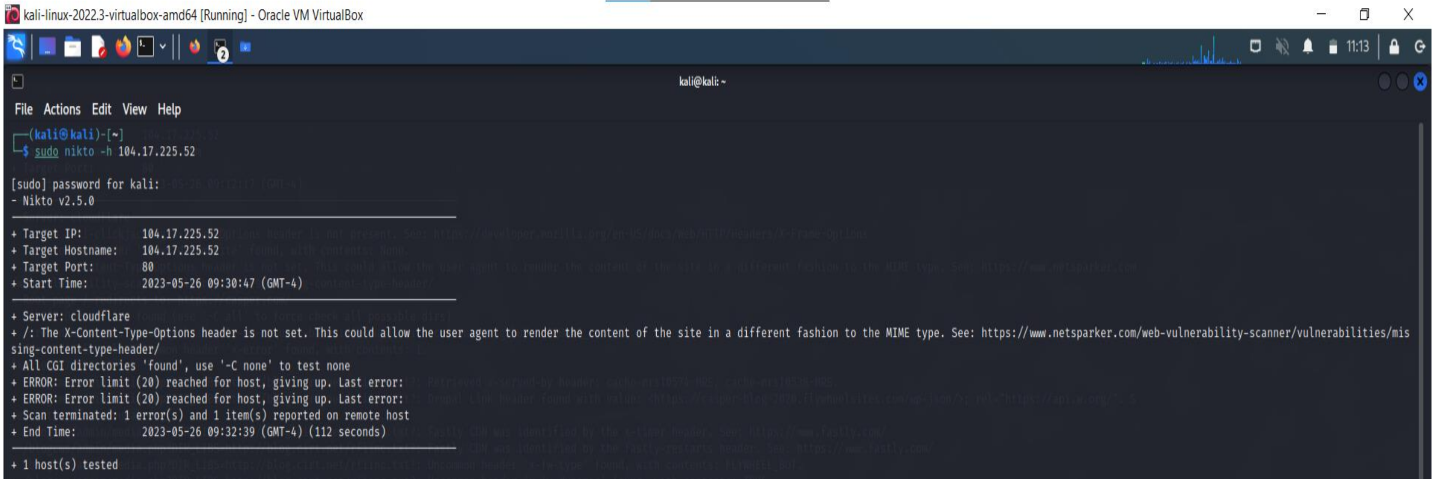
Checking for Vulnerabilities using nikto

vulnerabilities are scanned by Nikto. found some vulnerability like blogcms

A security program called the Nikto web server scanner scans a website for thousands of possible security holes. This includes malicious files, services that have been set up improperly, vulnerable scripts, and other issues. It was created using plugins and is open source to allow for feature expansion. New security checks are frequently added to these plugins through regular updates. Many penetration testers and security analysts maintain the famous Nikto Web Vulnerability Scanner in their toolkit. It typically unearths valuable data about a web server or website that may be used for subsequent exploitation or vulnerability analysis.


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help

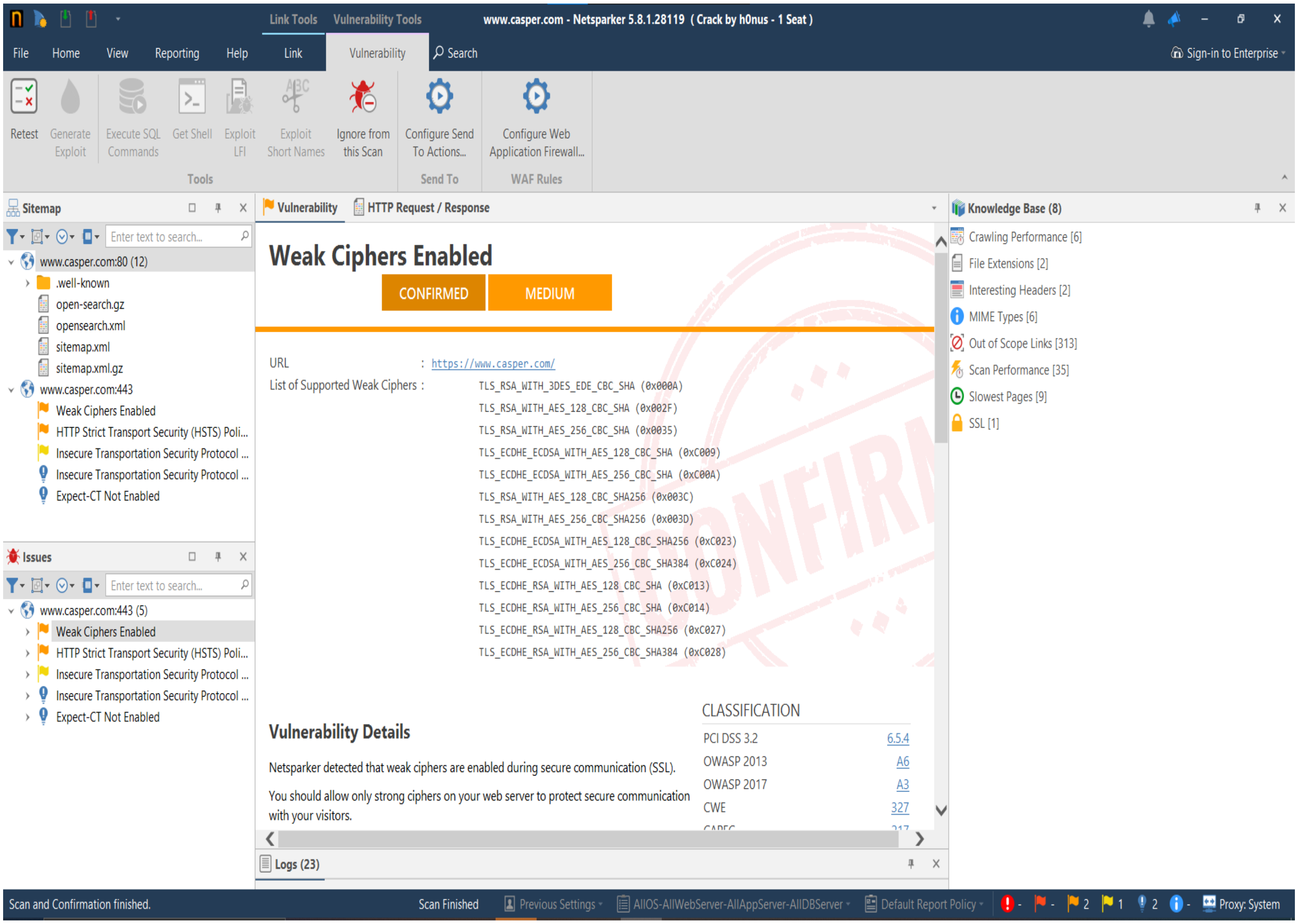
```
+ Target IP:          104.17.225.52
+ Target Hostname:    casper.com
+ Target Port:        80
+ Start Time:         2023-05-26 09:12:17 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-dwsid-samesite' found, with contents: None.
+ /: 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 type. See: https://www.netsparker.com
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://casper.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml: Uncommon header 'x-dw-request-base-id' found, with contents: jgkHuU-xcGQBAAB_.
+ /crossdomain.xml: Uncommon header 'x-error' found, with contents: 1.
^X@sS04.17.225.52
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Retrieved x-served-by header: cache-mrs10574-MRS, cache-mrs10538-MRS.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Drupal Link header found with value: <https://casper-blog-2020.flywheelsites.com/wp-json/>; rel="https://api.w.org/". S
ee: https://www.drupal.org/
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Fastly CDN was identified by the fastly-restarts header. See: https://www.fastly.com/
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-fw-type' found, with contents: FLYWHEEL_BOT.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-fw-dynamic' found, with contents: TRUE.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-fw-version' found, with contents: 5.0.0.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-cacheable' found, with contents: NO:Not Cacheable.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-served-by' found, with contents: cache-mrs10574-MRS, cache-mrs10538-MRS.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-fw-serve' found, with contents: TRUE.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-fw-hash' found, with contents: jw4hfjq7qw.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'fastly-restarts' found, with contents: 1.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-fw-server' found, with contents: Flywheel/5.1.0.
+ /blogcms/admin/media.php?DIR_LIBS=http://blog.cirt.net/rfiinc.txt?: Uncommon header 'x-fw-static' found, with contents: NO.
+ /blogindex/: Admin login page/section found.
+ /blog/wp-login.php: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /blog/wp-login.php: Wordpress login found.
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 7968 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2023-05-26 10:46:04 (GMT-4) (5627 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
11:13
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 104.17.225.52

[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          104.17.225.52
+ Target Hostname:    104.17.225.52
+ Target Port:        80
+ Start Time:         2023-05-26 09:30:47 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: 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 type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 1 error(s) and 1 item(s) reported on remote host
+ End Time:           2023-05-26 09:32:39 (GMT-4) (112 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scanned Vulnerabilities Using Netsparker

1) Weak Ciphers Enabled



Weak Ciphers Enabled

CONFIRMED MEDIUM

URL : https://www.casper.com/

List of Supported Weak Ciphers :

```
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
```

Vulnerability Details

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217

Risk type : Medium

URL :https://www.casper.com/

List of Supported Weak Ciphers :TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

- **Vulnerability Details**

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

- **Impact**

Attackers might decrypt SSL traffic between your server and your visitors.

- **Actions to Take**

For Apache, you should modify the SSLCipherSuite directive in the

```
httpd.conf.


SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"

ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry.

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

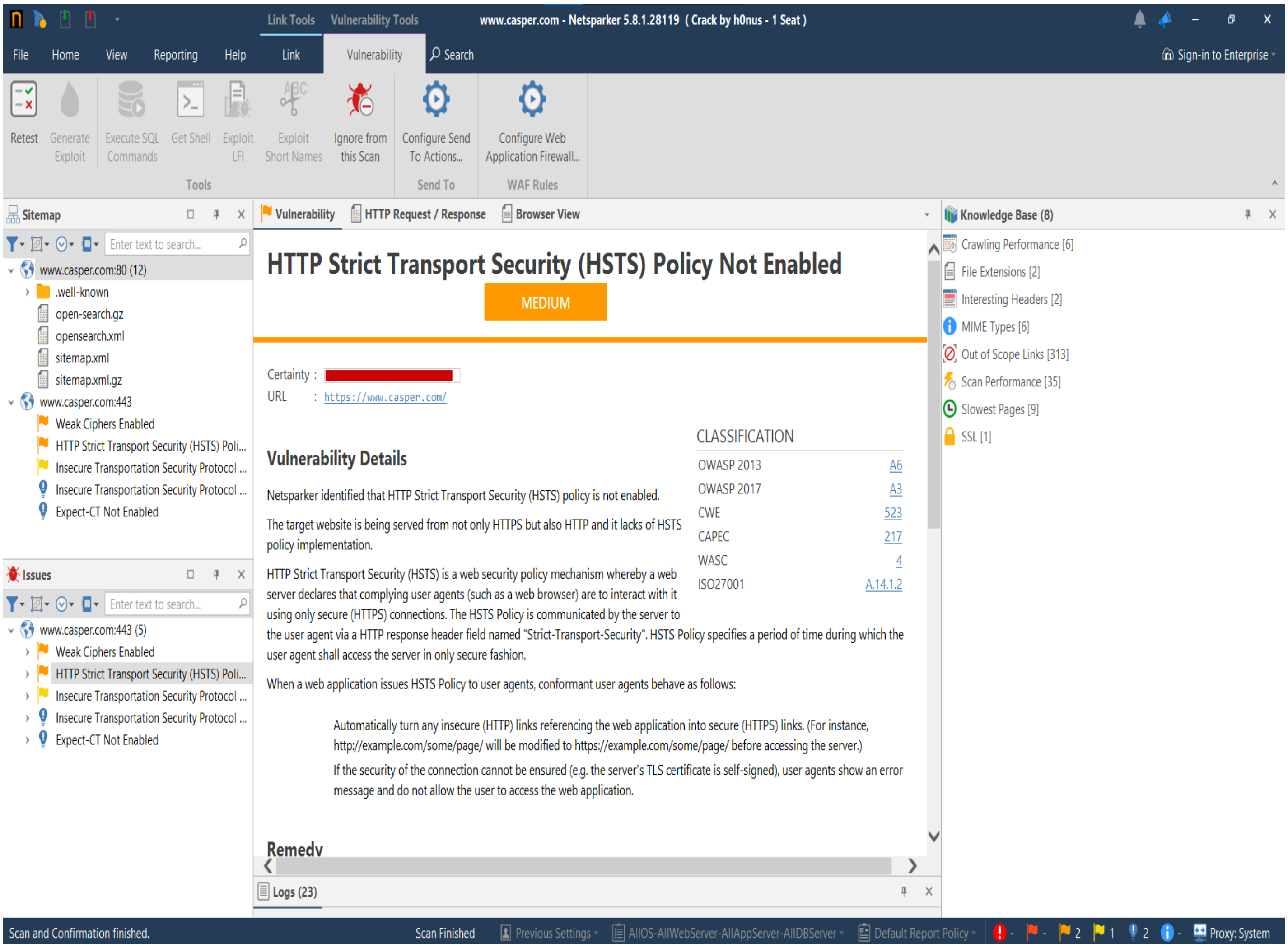
b.In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c. Set "Enabled" DWORD to "0x0" for the following registry keys:

SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5

- **Remedy**
  Configure your web server to disallow using weak ciphers.

2) HTTP Strict Transport Security (HSTS) Policy Not Enabled



HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Certainty :

URL : https://www.casper.com/

Vulnerability Details

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)

If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

CLASSIFICATION	
OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

Risk type : Medium

- **Vulnerability Details**

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)

If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

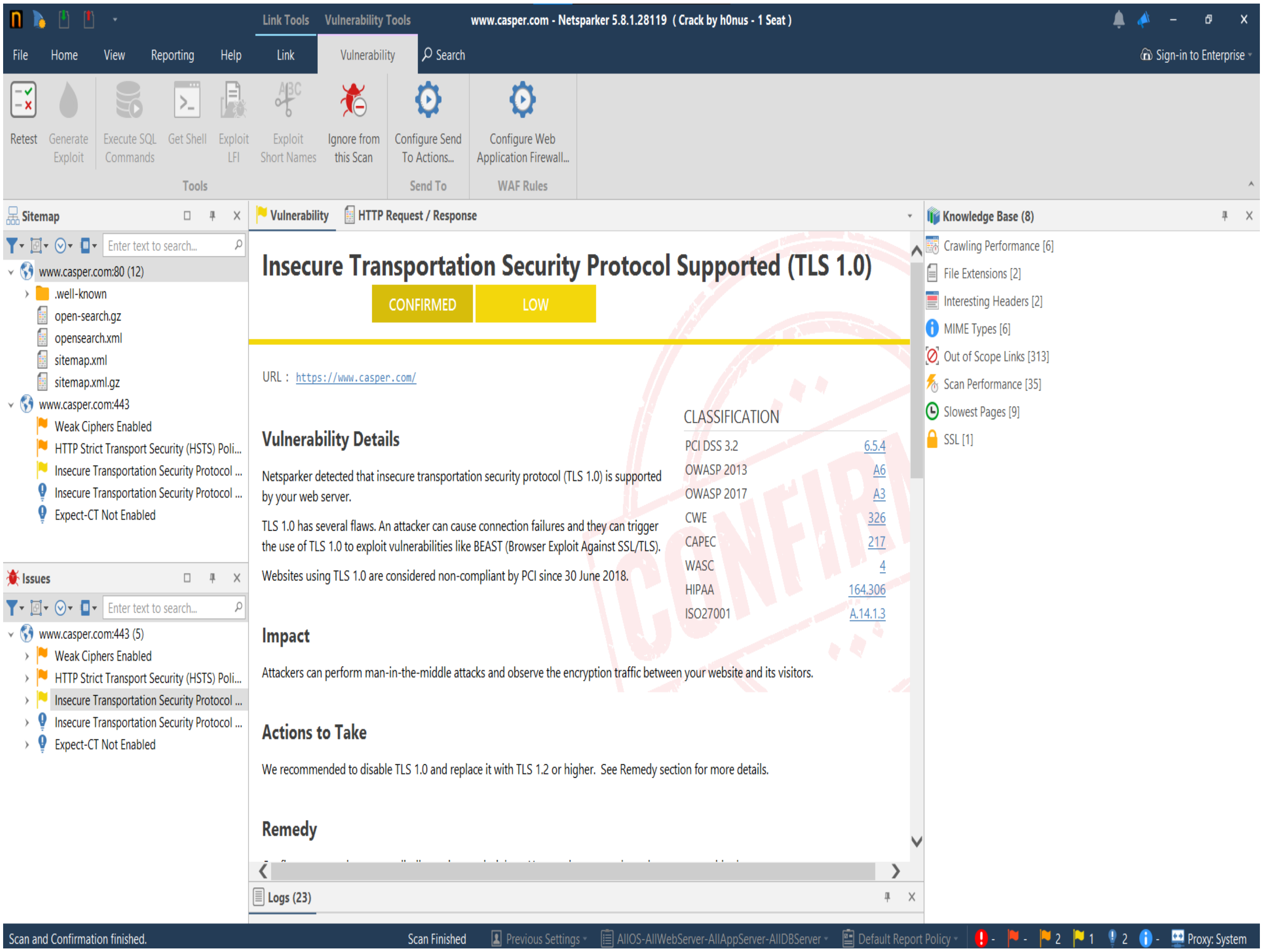
- **Remedy**

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module

LoadModule headers_module modules/mod_headers.so


# redirect all HTTP to HTTPS (optional)

<VirtualHost *:80>

    ServerAlias *

    RewriteEngine On

    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]

</VirtualHost>


# HTTPS-Host-Configuration

<VirtualHost *:443>

   # Use HTTP Strict Transport Security to force client to use secure connections only

   Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"


   # Further Configuration goes here

   [...]

</VirtualHost>
```

3) Insecure Transportation Security Protocol Supported (TLS 1.0)



Insecure Transportation Security Protocol Supported (TLS 1.0)

CONFIRMED LOW

URL : https://www.casper.com/

Vulnerability Details

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Risk type : Low

- **Vulnerability Details**

  Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

  TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

  Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

- **Impact**

  Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

- **Actions to Take**

  We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

- **Remedy**

  Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

  For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

  SSLProtocol +TLSv1.2

  For Nginx, locate any use of the directive ssl_protocols in the nginx.conf file and remove TLSv1.

  ssl_protocols TLSv1.2;

  For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

  Click on Start and then Run, type regedt32 or regedit, and then click OK.

  In Registry Editor, locate the following registry key or create if it does not exist:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\

  Locate a key named Server or create if it doesn't exist.

  Under the Server key, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".

  For lighttpd, put the following lines in your configuration file:

  ssl.use-sslv2 = "disable"
  ssl.use-sslv3 = "disable"
  ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
  ssl.ec-curve = "secp384r1"