Sri Lanka Institute of Information Technology

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2023

Bug Bounty vulnerabilities scanning Report 7

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

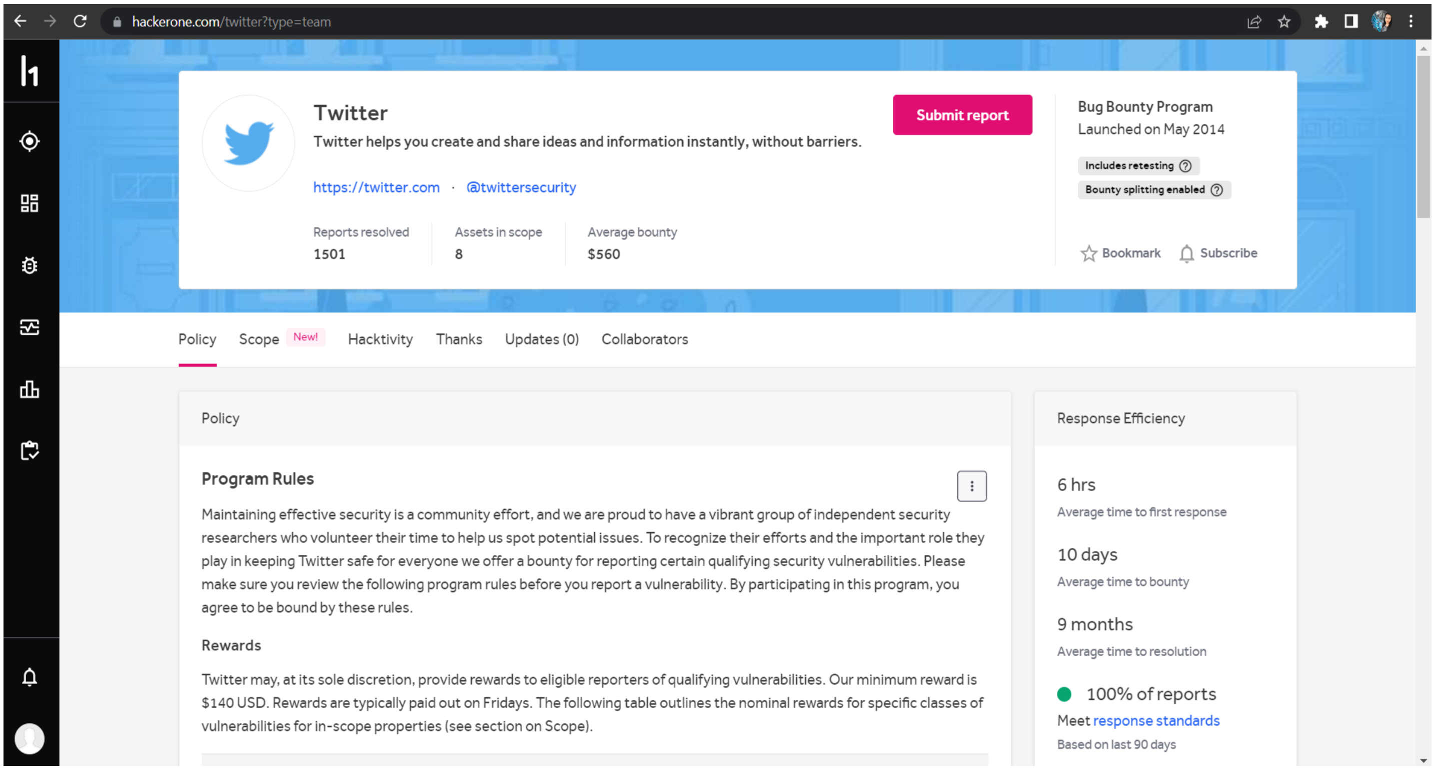
Twitter

- **Overview**

Users may publish brief articles known as tweets on Twitter, a free social networking service. Text, movies, photographs, or links may be included in these tweets. Users must have a smartphone or internet connectivity in order to utilize the Twitter app or website, Twitter.com.

Registered users may publish, share, like, and react to tweets with brief messages using this microblogging service, which combines blogging with instant messaging. Users who are not signed up can only view tweets.

Twitter is used by people to stay up to speed on brand news and promotions, connect with friends, and follow public figures in business, politics, and entertainment. They utilize it to remain up to date on news and events as well.



Twitter

Twitter helps you create and share ideas and information instantly, without barriers.

https://twitter.com · @twittersecurity

Reports resolved	Assets in scope	Average bounty
1501	8	$560

Bug Bounty Program
Launched on May 2014

Policy

Program Rules

Maintaining effective security is a community effort, and we are proud to have a vibrant group of independent security researchers who volunteer their time to help us spot potential issues. To recognize their efforts and the important role they play in keeping Twitter safe for everyone we offer a bounty for reporting certain qualifying security vulnerabilities. Please make sure you review the following program rules before you report a vulnerability. By participating in this program, you agree to be bound by these rules.

Rewards

Twitter may, at its sole discretion, provide rewards to eligible reporters of qualifying vulnerabilities. Our minimum reward is $140 USD. Rewards are typically paid out on Fridays. The following table outlines the nominal rewards for specific classes of vulnerabilities for in-scope properties (see section on Scope).

Response Efficiency

6 hrs
Average time to first response

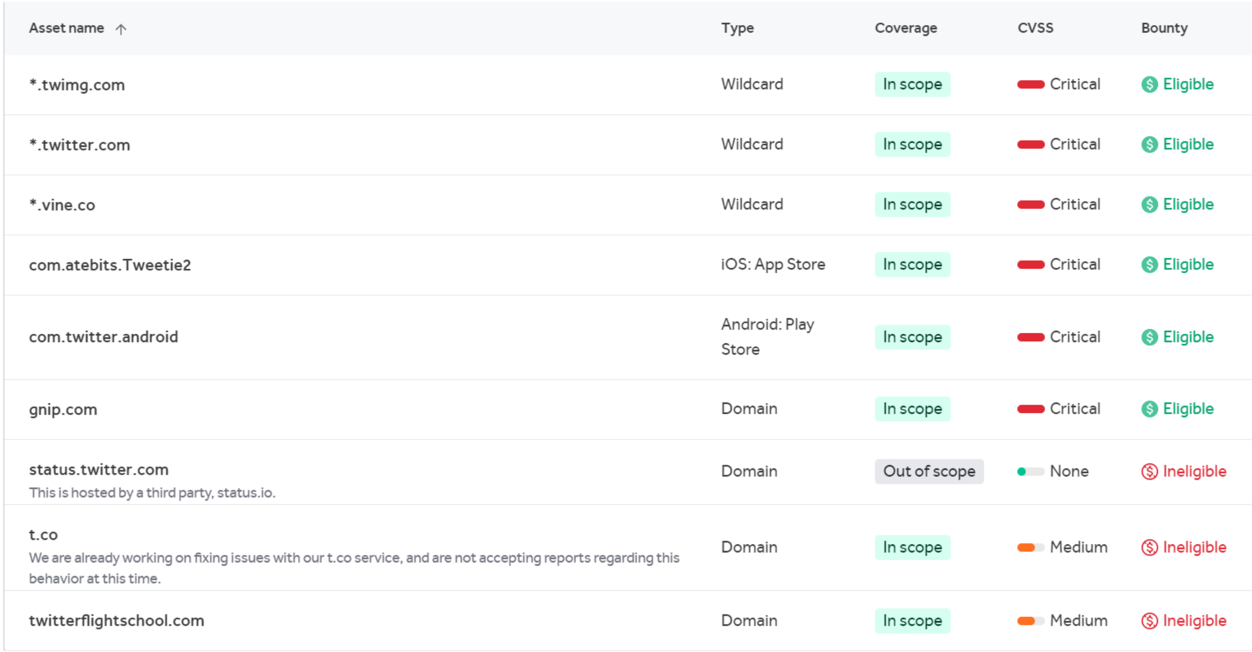
10 days
Average time to bounty

9 months
Average time to resolution

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

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

Assignments of Scope



Asset name ↑	Type	Coverage	CVSS	Bounty
*.twimg.com	Wildcard	In scope	Critical	Eligible
*.twitter.com	Wildcard	In scope	Critical	Eligible
*.vine.co	Wildcard	In scope	Critical	Eligible
com.atebits.Tweetie2	iOS: App Store	In scope	Critical	Eligible
com.twitter.android	Android: Play Store	In scope	Critical	Eligible
gnip.com	Domain	In scope	Critical	Eligible
status.twitter.com This is hosted by a third party, status.io.	Domain	Out of scope	None	Ineligible
t.co We are already working on fixing issues with our t.co service, and are not accepting reports regarding this behavior at this time.	Domain	In scope	Medium	Ineligible
twitterflightschool.com	Domain	In scope	Medium	Ineligible

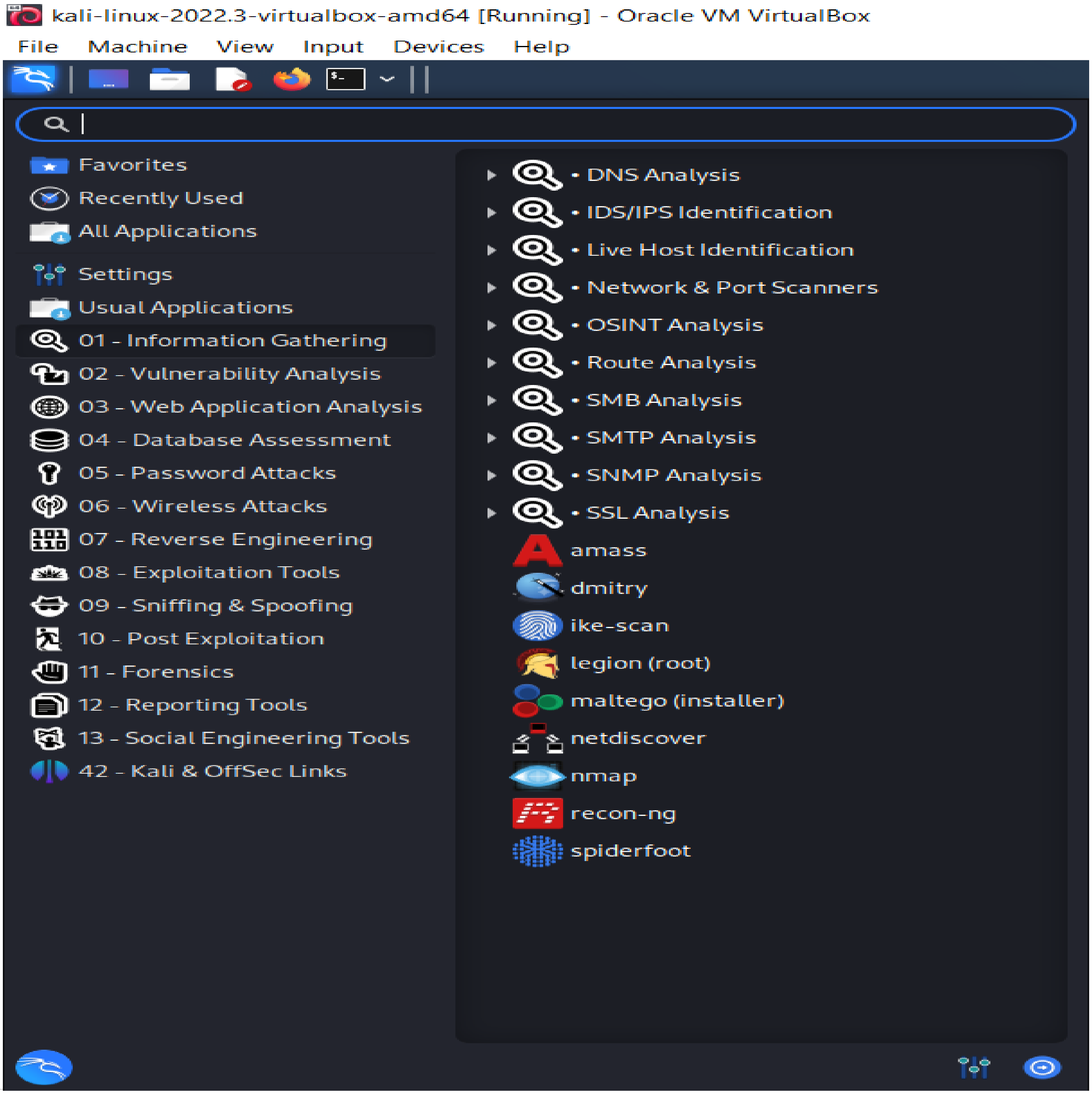
- *.twimg.com
- *.twitter.com
- *.vine.co
- com.atebits.Tweetie2
- com.twitter.android
- gnip.com
- status.twitter.com
  This is hosted by a third party, status.io.

- t.co
  We are already working on fixing issues with our t.co service, and are not accepting reports regarding this behavior at this time.

- twitterflightschool.com

Information gathering

It is the process of collecting data from many sources for a range of purposes. Learning to create efficient information-gathering techniques will benefit studying in a variety of ways. Effective information collecting involves making better use of time, fostering critical thinking through the use of shifting/sorting strategies, and enlarging one's perspective and topic knowledge through the investigation of new sources. Additionally, obtaining knowledge may be useful for a number of purposes, but the major advantage in terms of academic studies is that one will become aware of more varied sources, viewpoints, and techniques that can improve one's academic work.



Subdomains for Hunting

Sub-domain enumeration is the process of listing sub-domains for one or more domains. In the process of reconnaissance, it's a crucial phase. Sub-domain enumeration can reveal several domains and sub-domains that are included in a security assessment, which increases the chance of finding vulnerabilities.

Finding applications using cryptic, abandoned sub-domains may reveal serious bugs.

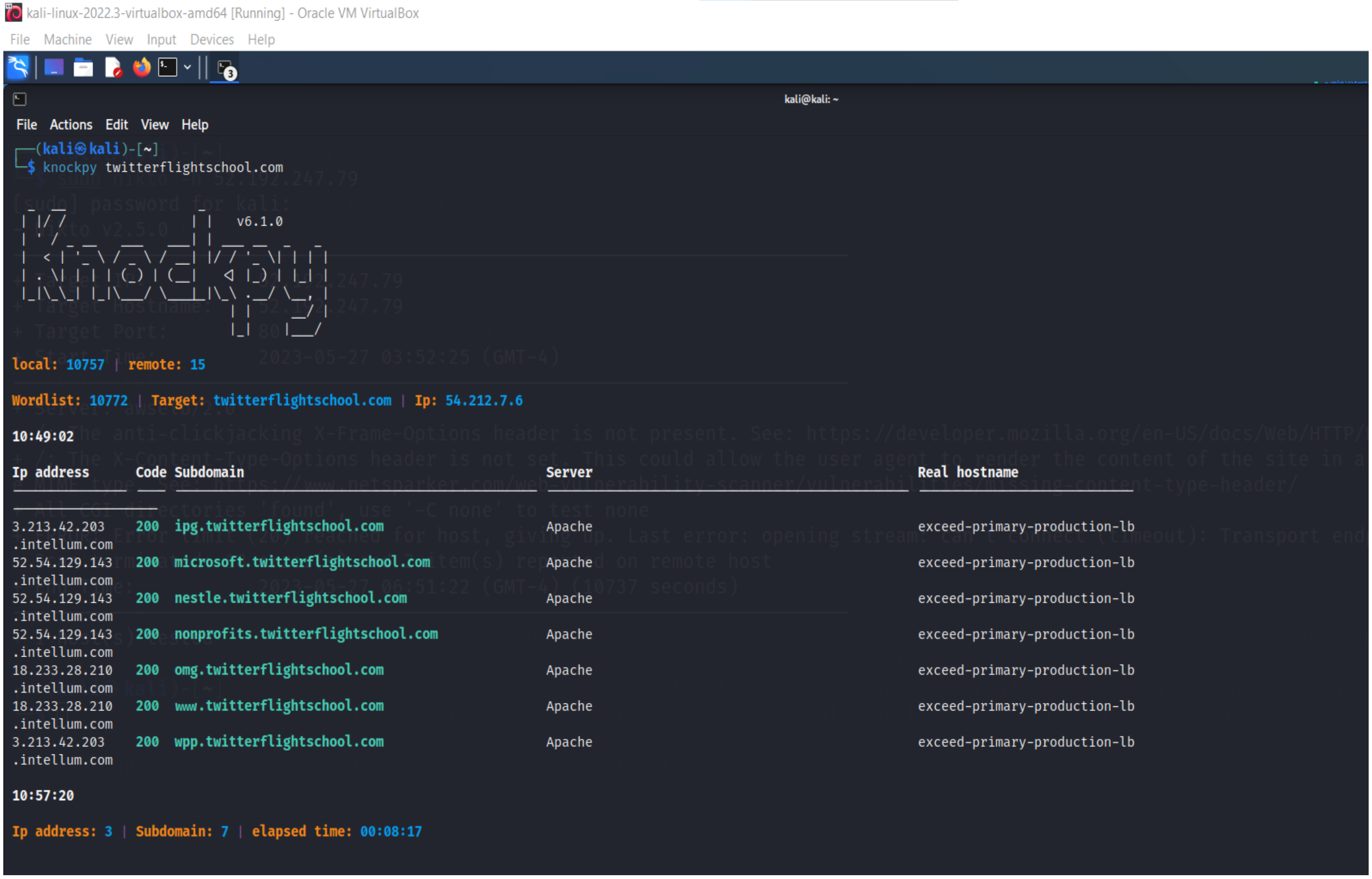
Within a single company, the same vulnerabilities are routinely discovered across many domains and applications.

What is Knockpy?

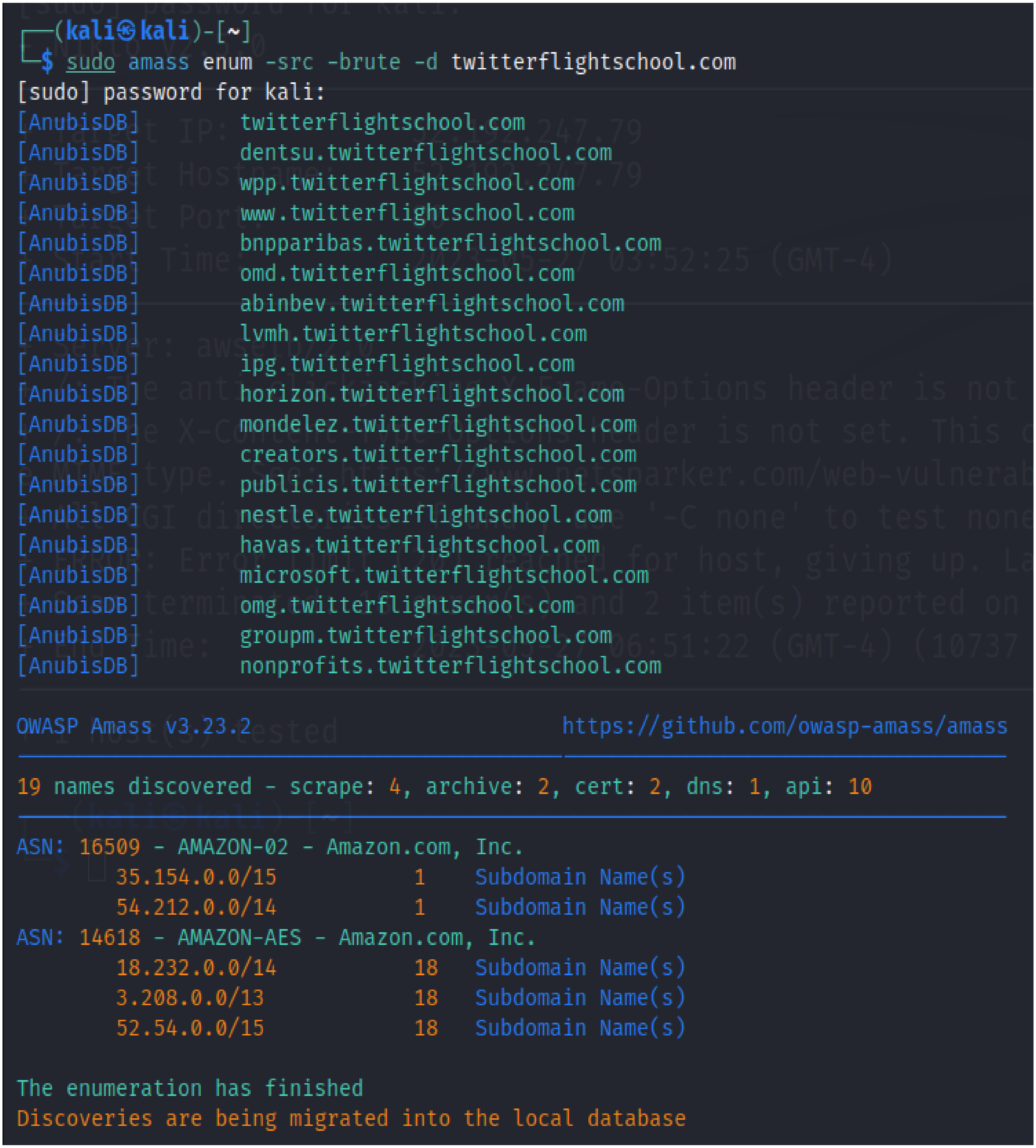
With only a few lines of code, knockpy's python version of the knockoffs framework makes it simple to use knockoff-based inference. The modular design of Knockpy makes it simple for researchers and analysts to add features on top of it.

- searching subdomain by knockpy,

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
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ knockpy twitterflightschool.com
  _  __                 _
 | |/ /                | |   v6.1.0
 | ' / _ __   ___   ___| | ___ __  _   _
 |  < | '_ \ / _ \ / __| |/ / '_ \| | | |
 | . \| | | | (_) | (__|   <| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/

local: 10757 | remote: 15

Wordlist: 10772 | Target: twitterflightschool.com | Ip: 54.212.7.6

10:49:02

Ip address      Code Subdomain                                       Server                                   Real hostname
_______________ ____ _______________________________________________ ________________________________________ ______________________
_______________
3.213.42.203    200  ipg.twitterflightschool.com                     Apache                                   exceed-primary-production-lb
.intellum.com
52.54.129.143   200  microsoft.twitterflightschool.com               Apache                                   exceed-primary-production-lb
.intellum.com
52.54.129.143   200  nestle.twitterflightschool.com                  Apache                                   exceed-primary-production-lb
.intellum.com
52.54.129.143   200  nonprofits.twitterflightschool.com              Apache                                   exceed-primary-production-lb
.intellum.com
18.233.28.210   200  omg.twitterflightschool.com                     Apache                                   exceed-primary-production-lb
.intellum.com
18.233.28.210   200  www.twitterflightschool.com                     Apache                                   exceed-primary-production-lb
.intellum.com
3.213.42.203    200  wpp.twitterflightschool.com                     Apache                                   exceed-primary-production-lb
.intellum.com

10:57:20

Ip address: 3 | Subdomain: 7 | elapsed time: 00:08:17
```



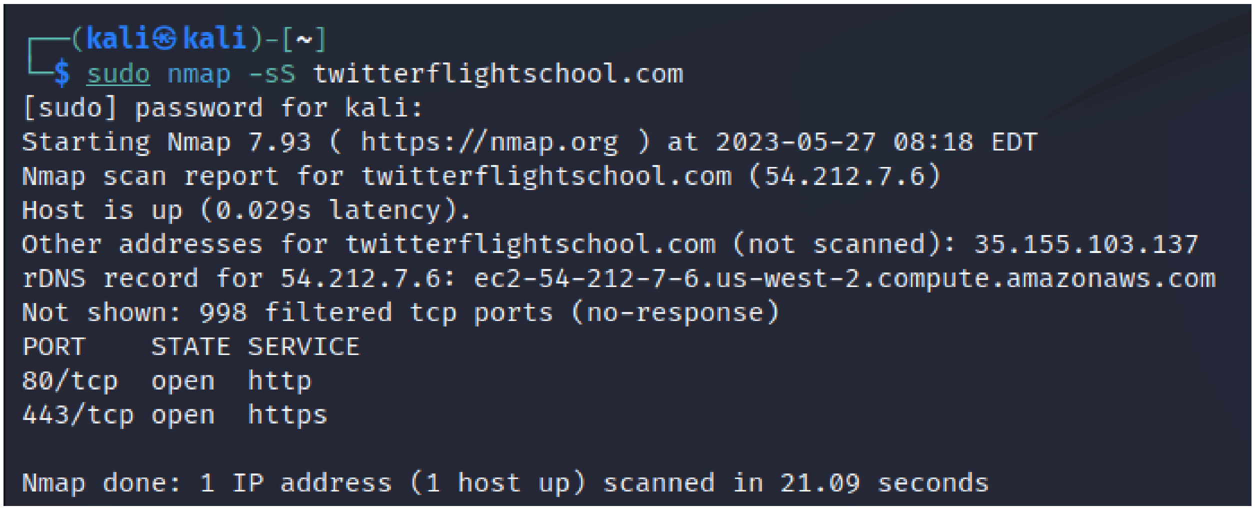
```
┌──(kali㉿kali)-[~]
└─$ sudo amass enum -src -brute -d twitterflightschool.com
[sudo] password for kali:
[AnubisDB]        twitterflightschool.com
[AnubisDB]        dentsu.twitterflightschool.com
[AnubisDB]        wpp.twitterflightschool.com
[AnubisDB]        www.twitterflightschool.com
[AnubisDB]        bnpparibas.twitterflightschool.com
[AnubisDB]        omd.twitterflightschool.com
[AnubisDB]        abinbev.twitterflightschool.com
[AnubisDB]        lvmh.twitterflightschool.com
[AnubisDB]        ipg.twitterflightschool.com
[AnubisDB]        horizon.twitterflightschool.com
[AnubisDB]        mondelez.twitterflightschool.com
[AnubisDB]        creators.twitterflightschool.com
[AnubisDB]        publicis.twitterflightschool.com
[AnubisDB]        nestle.twitterflightschool.com
[AnubisDB]        havas.twitterflightschool.com
[AnubisDB]        microsoft.twitterflightschool.com
[AnubisDB]        omg.twitterflightschool.com
[AnubisDB]        groupm.twitterflightschool.com
[AnubisDB]        nonprofits.twitterflightschool.com

OWASP Amass v3.23.2                            https://github.com/owasp-amass/amass
────────────────────────────────────────────────────────────────────────────────
19 names discovered - scrape: 4, archive: 2, cert: 2, dns: 1, api: 10
────────────────────────────────────────────────────────────────────────────────
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        35.154.0.0/15           1     Subdomain Name(s)
        54.212.0.0/14           1     Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
        18.232.0.0/14           18    Subdomain Name(s)
        3.208.0.0/13            18    Subdomain Name(s)
        52.54.0.0/15            18    Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

- ## 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

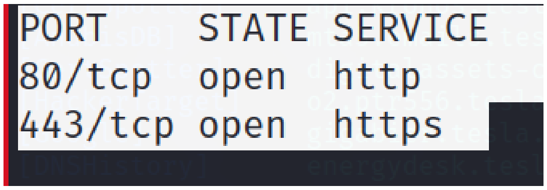
The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS twitterflightschool.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-27 08:18 EDT
Nmap scan report for twitterflightschool.com (54.212.7.6)
Host is up (0.029s latency).
Other addresses for twitterflightschool.com (not scanned): 35.155.103.137
rDNS record for 54.212.7.6: ec2-54-212-7-6.us-west-2.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 21.09 seconds
```

open ports are,

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https



```
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

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.

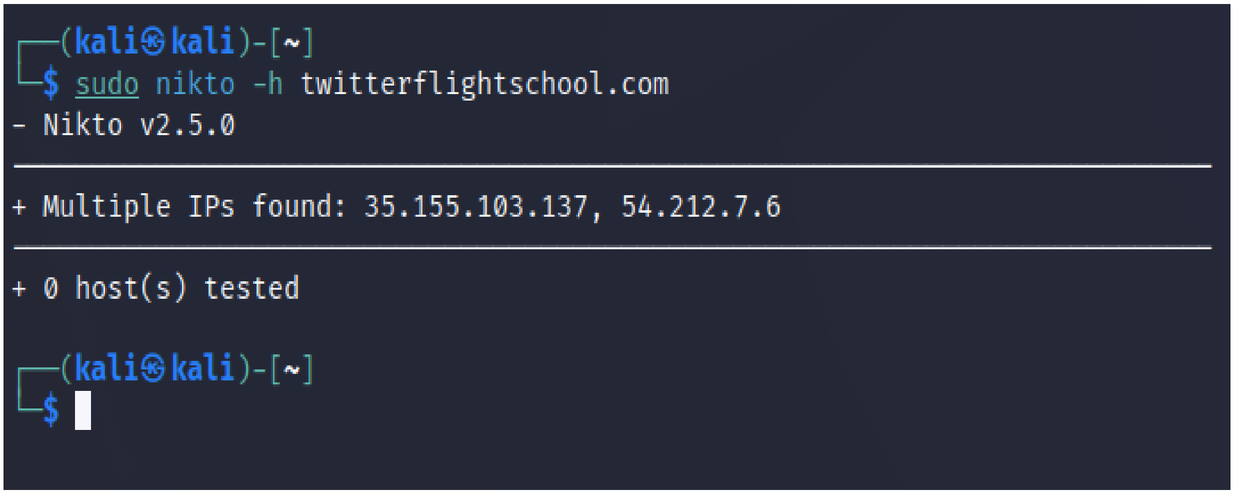
Using Nmap to List Open Ports

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.

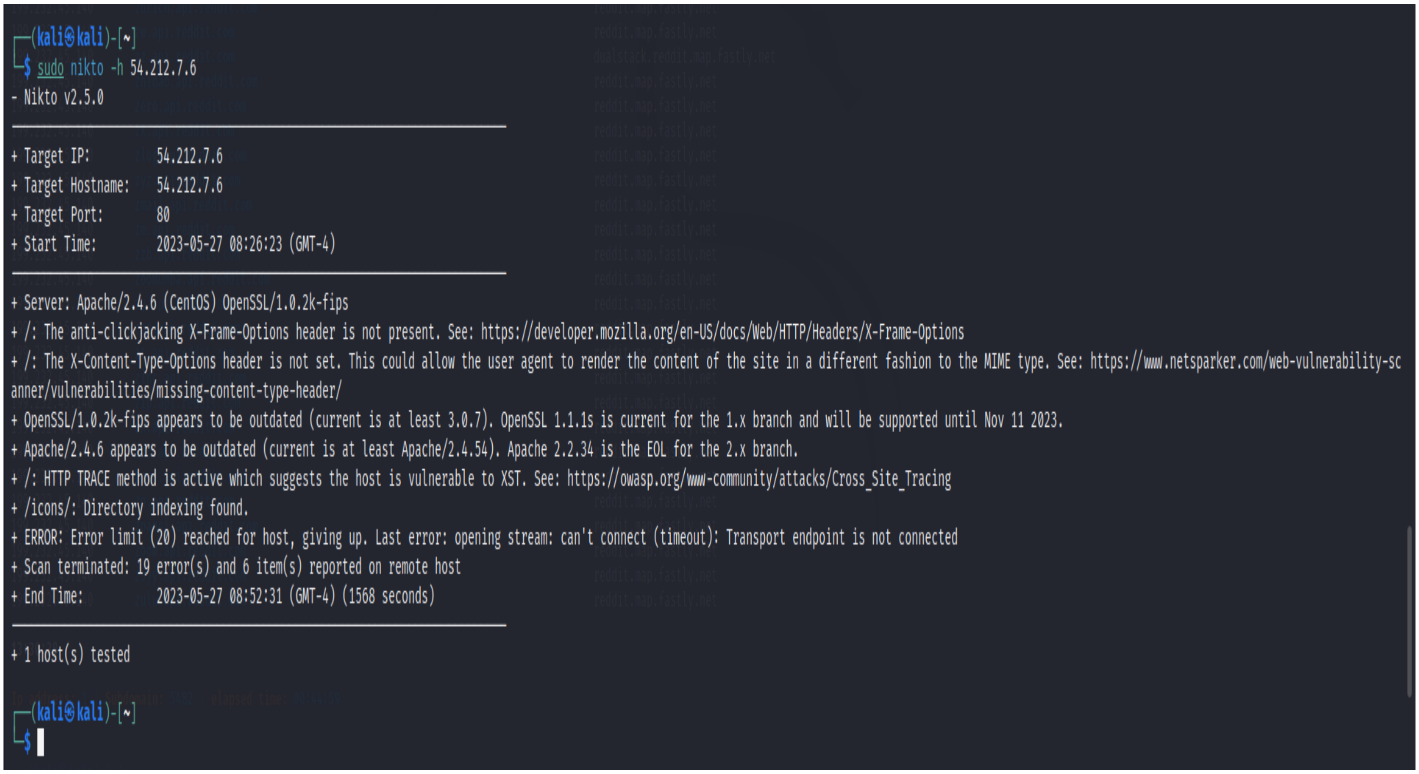
Checking for Vulnerabilities using NIKTO

vulnerabilities are scanned by Nikto. But not any found vulnerability

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.



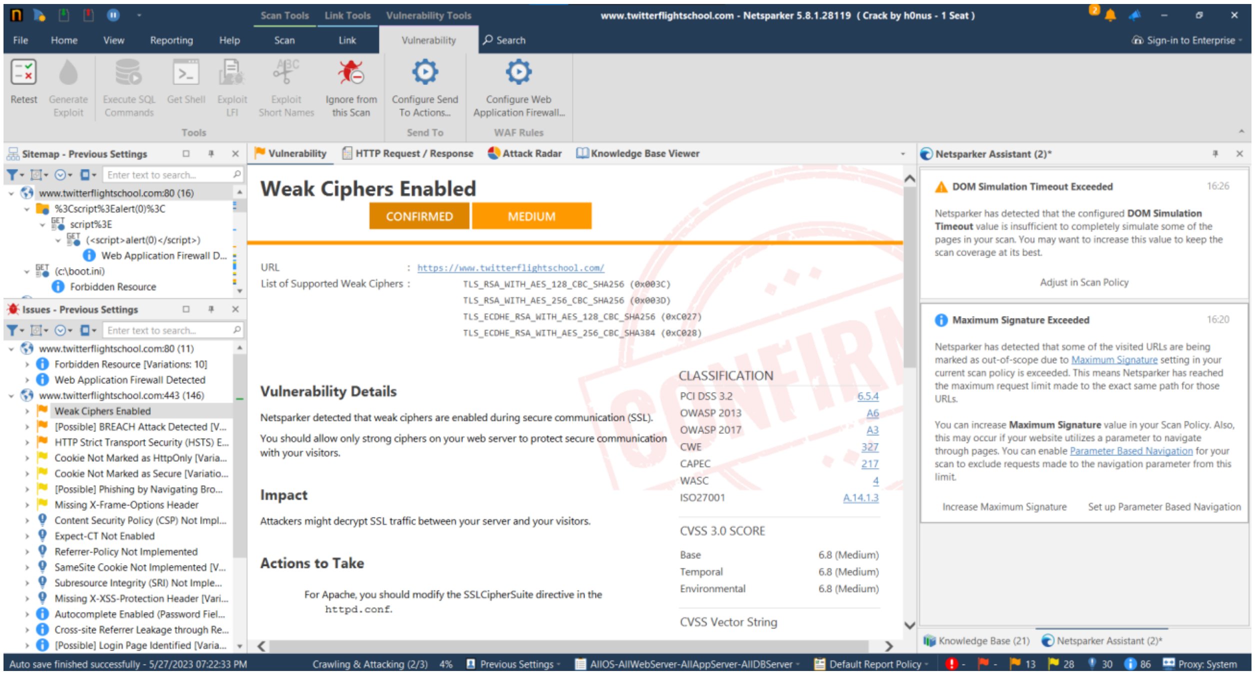
```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h twitterflightschool.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 35.155.103.137, 54.212.7.6
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 54.212.7.6
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          54.212.7.6
+ Target Hostname:    54.212.7.6
+ Target Port:        80
+ Start Time:         2023-05-27 08:26:23 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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-sc
anner/vulnerabilities/missing-content-type-header/
+ OpenSSL/1.0.2k-fips appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /icons/: Directory indexing found.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Transport endpoint is not connected
+ Scan terminated: 19 error(s) and 6 item(s) reported on remote host
+ End Time:           2023-05-27 08:52:31 (GMT-4) (1568 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```

Scanned Vulnerabilities Using Netsparker

1) Weak Ciphers Enabled



www.twitterflightschool.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

Sitemap - Previous Settings

```
www.twitterflightschool.com:80 (16)
  %3Cscript%3Ealert(0)%3C
    script%3E
      (<script>alert(0)</script>)
        Web Application Firewall D...
  (c:\boot.ini)
    Forbidden Resource
```

Issues - Previous Settings

```
www.twitterflightschool.com:80 (11)
  Forbidden Resource [Variations: 10]
  Web Application Firewall Detected
www.twitterflightschool.com:443 (146)
  Weak Ciphers Enabled
  [Possible] BREACH Attack Detected [V...
  HTTP Strict Transport Security (HSTS) E...
  Cookie Not Marked as HttpOnly [Varia...
  Cookie Not Marked as Secure [Variatio...
  [Possible] Phishing by Navigating Bro...
  Missing X-Frame-Options Header
  Content Security Policy (CSP) Not Impl...
  Expect-CT Not Enabled
  Referrer-Policy Not Implemented
  SameSite Cookie Not Implemented [V...
  Subresource Integrity (SRI) Not Imple...
  Missing X-XSS-Protection Header [Vari...
  Autocomplete Enabled (Password Fiel...
  Cross-site Referrer Leakage through Re...
  [Possible] Login Page Identified [Varia...
```

Weak Ciphers Enabled

CONFIRMED MEDIUM

URL : https://www.twitterflightschool.com/

List of Supported Weak Ciphers :

```
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
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`.

CLASSIFICATION	
PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE	
Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

DOM Simulation Timeout Exceeded 16:26

Netsparker has detected that the configured **DOM Simulation Timeout** value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.

Adjust in Scan Policy

Maximum Signature Exceeded 16:20

Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Increase Maximum Signature   Set up Parameter Based Navigation

Auto save finished successfully - 5/27/2023 07:22:33 PM   Crawling & Attacking (2/3) 4%   Previous Settings   AllOS-AllWebServer-AllAppServer-AllDBServer   Default Report Policy   13   28   30   86   Proxy: System

Risk type : Medium

URL : https://www.twitterflightschool.com/

List of Supported Weak Ciphers :

TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
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.

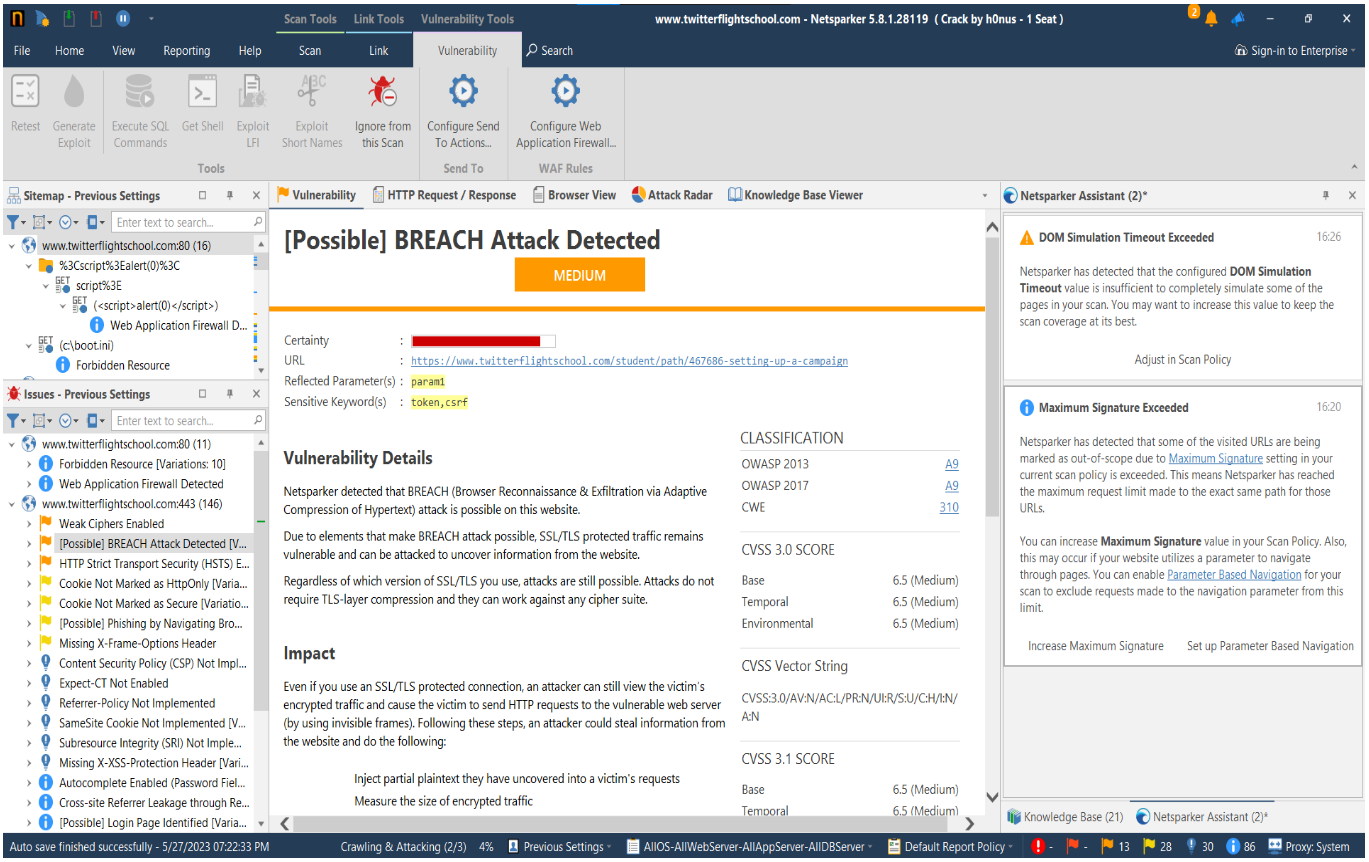
b.In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

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) [Possible] BREACH Attack Detected



www.twitterflightschool.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

Sitemap - Previous Settings

- www.twitterflightschool.com:80 (16)
  - %3Cscript%3Ealert(0)%3C
    - script%3E
      - (<script>alert(0)</script>)
        - Web Application Firewall D...
  - (c:\boot.ini)
    - Forbidden Resource

Issues - Previous Settings

- www.twitterflightschool.com:80 (11)
  - Forbidden Resource [Variations: 10]
  - Web Application Firewall Detected
- www.twitterflightschool.com:443 (146)
  - Weak Ciphers Enabled
  - [Possible] BREACH Attack Detected [V...
  - HTTP Strict Transport Security (HSTS) E...
  - Cookie Not Marked as HttpOnly [Varia...
  - Cookie Not Marked as Secure [Variatio...
  - [Possible] Phishing by Navigating Bro...
  - Missing X-Frame-Options Header
  - Content Security Policy (CSP) Not Impl...
  - Expect-CT Not Enabled
  - Referrer-Policy Not Implemented
  - SameSite Cookie Not Implemented [V...
  - Subresource Integrity (SRI) Not Imple...
  - Missing X-XSS-Protection Header [Vari...
  - Autocomplete Enabled (Password Fiel...
  - Cross-site Referrer Leakage through Re...
  - [Possible] Login Page Identified [Varia...

[Possible] BREACH Attack Detected

MEDIUM

Certainty :
URL : https://www.twitterflightschool.com/student/path/467686-setting-up-a-campaign
Reflected Parameter(s) : param1
Sensitive Keyword(s) : token,csrf

Vulnerability Details

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

Inject partial plaintext they have uncovered into a victim's requests

Measure the size of encrypted traffic

CLASSIFICATION	
OWASP 2013	A9
OWASP 2017	A9
CWE	310

CVSS 3.0 SCORE	
Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE	
Base	6.5 (Medium)
Temporal	6.5 (Medium)

Netsparker Assistant (2)*

DOM Simulation Timeout Exceeded 16:26

Netsparker has detected that the configured **DOM Simulation Timeout** value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.

Adjust in Scan Policy

Maximum Signature Exceeded 16:20

Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Increase Maximum Signature   Set up Parameter Based Navigation

Auto save finished successfully - 5/27/2023 07:22:33 PM   Crawling & Attacking (2/3)   4%   Previous Settings   AllOS-AllWebServer-AllAppServer-AllDBServer   Default Report Policy   ! -   - 13   28   30   86   Proxy: System

Risk type : Medium

URL : https://www.twitterflightschool.com/student/path/467686-setting-up-a-campaign

Reflected Parameter(s) :param1

Sensitive Keyword(s) :token,csrf

- **Vulnerability Details**

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

- **Impact**

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

Inject partial plaintext they have uncovered into a victim's requests
Measure the size of encrypted traffic

- **Remedy**

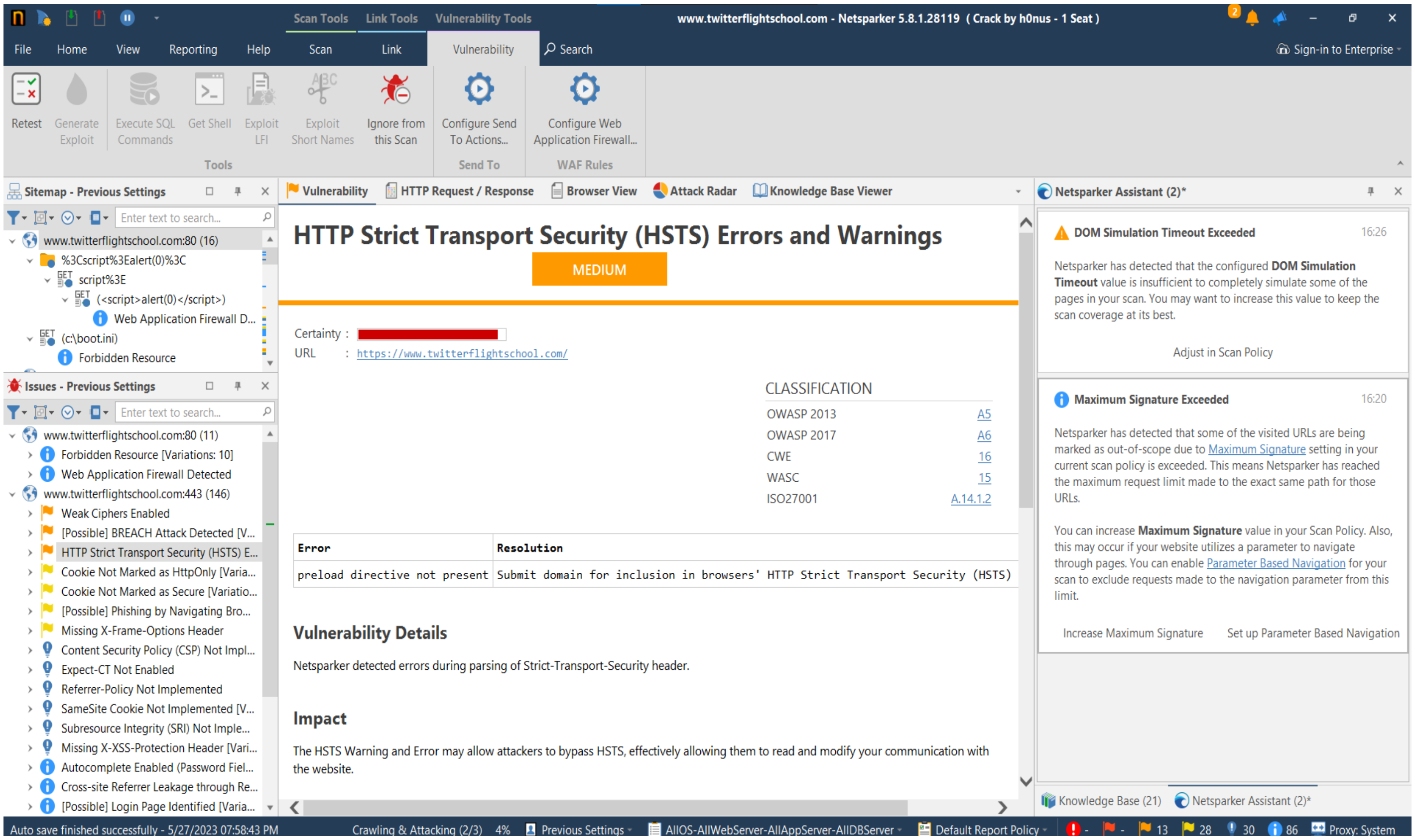
Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

Served from a server that uses HTTP-level compression (ie. gzip)
Reflects user-input in the HTTP response bodies
Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

- If possible, disable HTTP level compression
- Separate sensitive information from user input
- Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
- Hide the length of the traffic by adding a random number of bytes to the responses.
- Add in a rate limit, so that the page maximum is reached five times per minute.

3) HTTP Strict Transport Security (HSTS) Errors and Warnings


Scan Tools
Link Tools
Vulnerability Tools
www.twitterflightschool.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Scan
Link
Vulnerability
Search
Sign-in to Enterprise
Retest
Generate Exploit
Execute SQL Commands
Get Shell
Exploit LFI
Exploit Short Names
Ignore from this Scan
Configure Send To Actions...
Configure Web Application Firewall...
Tools
Send To
WAF Rules
Sitemap - Previous Settings
Enter text to search...
www.twitterflightschool.com:80 (16)
%3Cscript%3Ealert(0)%3C
script%3E
(<script>alert(0)</script>)
Web Application Firewall D...
(c:\boot.ini)
Forbidden Resource
Issues - Previous Settings
Enter text to search...
www.twitterflightschool.com:80 (11)
Forbidden Resource [Variations: 10]
Web Application Firewall Detected
www.twitterflightschool.com:443 (146)
Weak Ciphers Enabled
[Possible] BREACH Attack Detected [V...
HTTP Strict Transport Security (HSTS) E...
Cookie Not Marked as HttpOnly [Varia...
Cookie Not Marked as Secure [Variatio...
[Possible] Phishing by Navigating Bro...
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Referrer-Policy Not Implemented
SameSite Cookie Not Implemented [V...
Subresource Integrity (SRI) Not Imple...
Missing X-XSS-Protection Header [Vari...
Autocomplete Enabled (Password Fiel...
Cross-site Referrer Leakage through Re...
[Possible] Login Page Identified [Varia...
Vulnerability
HTTP Request / Response
Browser View
Attack Radar
Knowledge Base Viewer
Netsparker Assistant (2)*
Adjust in Scan Policy
Increase Maximum Signature
Set up Parameter Based Navigation
Knowledge Base (21)
Netsparker Assistant (2)*
Auto save finished successfully - 5/27/2023 07:58:43 PM
Crawling & Attacking (2/3) 4%
Previous Settings
AllOS-AllWebServer-AllAppServer-AllDBServer
Default Report Policy
13
28
30
86
Proxy: System

HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM

Certainty :
URL : https://www.twitterflightschool.com/

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS)

Vulnerability Details

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

DOM Simulation Timeout Exceeded 16:26

Netsparker has detected that the configured **DOM Simulation Timeout** value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.

Maximum Signature Exceeded 16:20

Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Risk type : Medium

URL : https://www.twitterflightschool.com/

Error : preload directive not present

Resolution : Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

- **Vulnerability Details**

Netsparker detected errors during parsing of Strict-Transport-Security header.

- **Impact**

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website

- **Remedy**

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

Serve a valid certificate

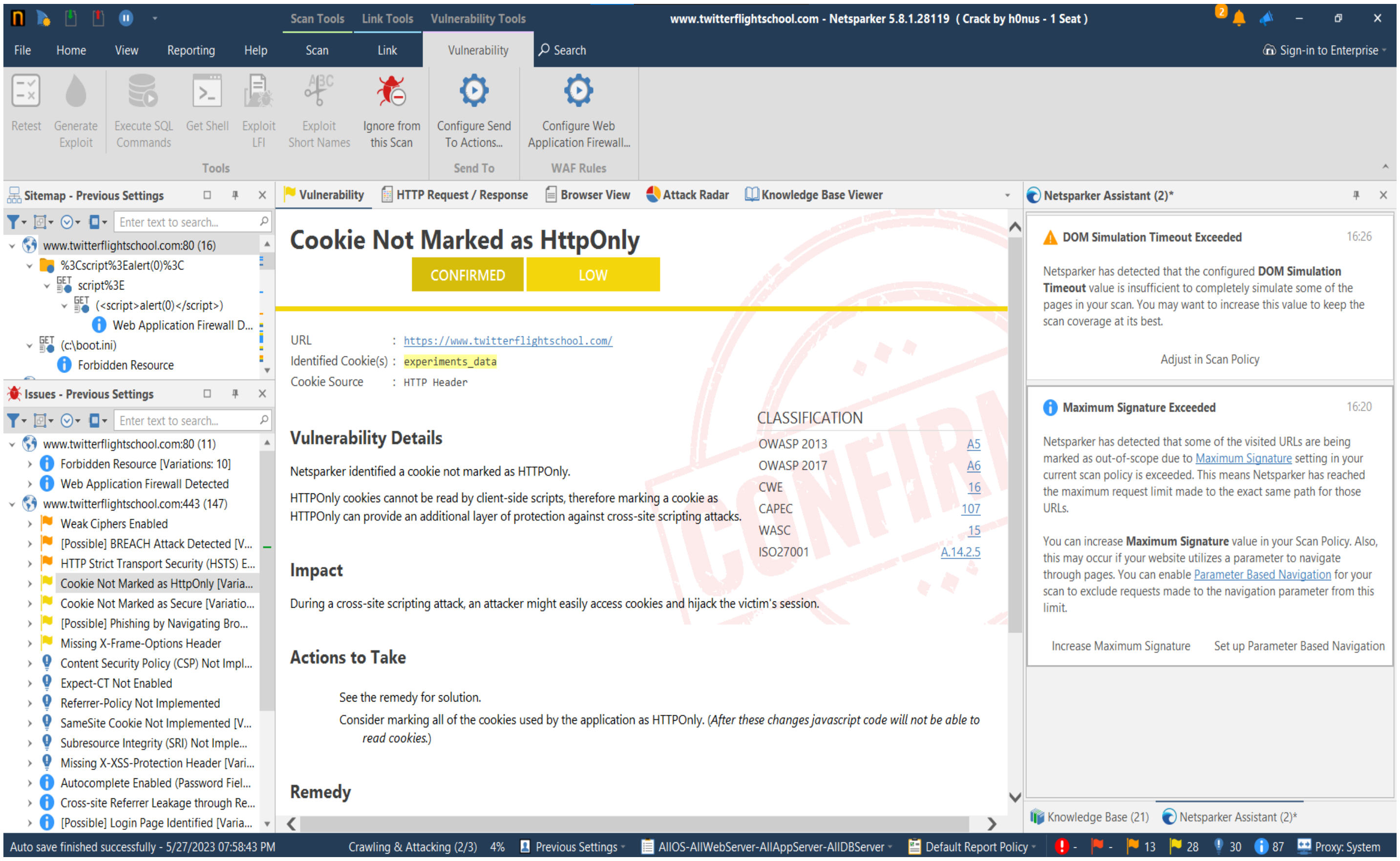
If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists

Serve an HSTS header on the base domain for HTTPS requests:

- The max-age must be at least 31536000 seconds (1 year)
- The includeSubDomains directive must be specified
- The preload directive must be specified
- If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

4) Cookie Not Marked as HttpOnly


Scan Tools
Link Tools
Vulnerability Tools
www.twitterflightschool.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Scan
Link
Vulnerability
Search
Sign-in to Enterprise
Retest
Generate Exploit
Execute SQL Commands
Get Shell
Exploit LFI
Exploit Short Names
Ignore from this Scan
Configure Send To Actions...
Configure Web Application Firewall...
Tools
Send To
WAF Rules
Sitemap - Previous Settings
Enter text to search...
www.twitterflightschool.com:80 (16)
%3Cscript%3Ealert(0)%3C
script%3E
(<script>alert(0)</script>)
Web Application Firewall D...
(c:\boot.ini)
Forbidden Resource
Issues - Previous Settings
Enter text to search...
www.twitterflightschool.com:80 (11)
Forbidden Resource [Variations: 10]
Web Application Firewall Detected
www.twitterflightschool.com:443 (147)
Weak Ciphers Enabled
[Possible] BREACH Attack Detected [V...
HTTP Strict Transport Security (HSTS) E...
Cookie Not Marked as HttpOnly [Varia...
Cookie Not Marked as Secure [Variatio...
[Possible] Phishing by Navigating Bro...
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Referrer-Policy Not Implemented
SameSite Cookie Not Implemented [V...
Subresource Integrity (SRI) Not Imple...
Missing X-XSS-Protection Header [Vari...
Autocomplete Enabled (Password Fiel...
Cross-site Referrer Leakage through Re...
[Possible] Login Page Identified [Varia...
Vulnerability
HTTP Request / Response
Browser View
Attack Radar
Knowledge Base Viewer
Netsparker Assistant (2)*
CONFIRMED
Knowledge Base (21)
Netsparker Assistant (2)*

Cookie Not Marked as HttpOnly

CONFIRMED LOW

URL : https://www.twitterflightschool.com/
Identified Cookie(s) : experiments_data
Cookie Source : HTTP Header

Vulnerability Details

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

CLASSIFICATION	
OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Actions to Take

See the remedy for solution.

Consider marking all of the cookies used by the application as HTTPOnly. *(After these changes javascript code will not be able to read cookies.)*

Remedy

DOM Simulation Timeout Exceeded 16:26

Netsparker has detected that the configured **DOM Simulation Timeout** value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.

Adjust in Scan Policy

Maximum Signature Exceeded 16:20

Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Increase Maximum Signature Set up Parameter Based Navigation

Auto save finished successfully - 5/27/2023 07:58:43 PM Crawling & Attacking (2/3) 4% Previous Settings AllOS-AllWebServer-AllAppServer-AllDBServer Default Report Policy - - 13 28 30 87 Proxy: System

Risk type : Low

- **Vulnerability Details**

  Netsparker identified a cookie not marked as HTTPOnly.

  HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

- **Actions to Take**

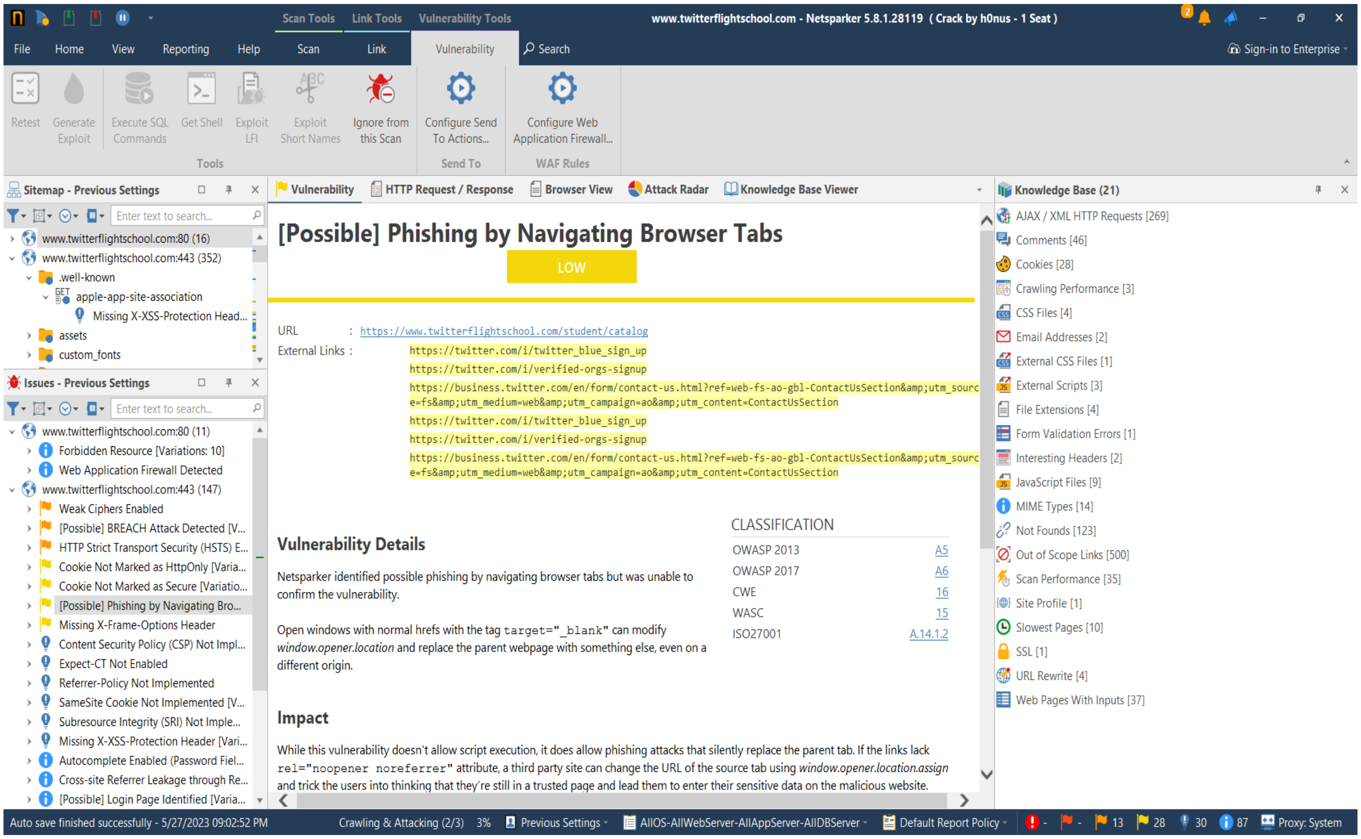
  See the remedy for solution.

  Consider marking all of the cookies used by the application as HTTPOnly. (After these changes javascript code will not be able to read cookies.)

- **Remedy**

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.

5) [Possible] Phishing by Navigating Browser Tabs


Scan Tools
Link Tools
Vulnerability Tools
www.twitterflightschool.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Scan
Link
Vulnerability
Search
Sign-in to Enterprise
Retest
Generate Exploit
Execute SQL Commands
Get Shell
Exploit LFI
Exploit Short Names
Ignore from this Scan
Configure Send To Actions...
Configure Web Application Firewall...
Tools
Send To
WAF Rules
Sitemap - Previous Settings
Enter text to search...
www.twitterflightschool.com:80 (16)
www.twitterflightschool.com:443 (352)
.well-known
apple-app-site-association
Missing X-XSS-Protection Head...
assets
custom_fonts
Issues - Previous Settings
Enter text to search...
www.twitterflightschool.com:80 (11)
Forbidden Resource [Variations: 10]
Web Application Firewall Detected
www.twitterflightschool.com:443 (147)
Weak Ciphers Enabled
[Possible] BREACH Attack Detected [V...
HTTP Strict Transport Security (HSTS) E...
Cookie Not Marked as HttpOnly [Varia...
Cookie Not Marked as Secure [Variatio...
[Possible] Phishing by Navigating Bro...
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Referrer-Policy Not Implemented
SameSite Cookie Not Implemented [V...
Subresource Integrity (SRI) Not Imple...
Missing X-XSS-Protection Header [Vari...
Autocomplete Enabled (Password Fiel...
Cross-site Referrer Leakage through Re...
[Possible] Login Page Identified [Varia...
Vulnerability
HTTP Request / Response
Browser View
Attack Radar
Knowledge Base Viewer
Knowledge Base (21)
AJAX / XML HTTP Requests [269]
Comments [46]
Cookies [28]
Crawling Performance [3]
CSS Files [4]
Email Addresses [2]
External CSS Files [1]
External Scripts [3]
File Extensions [4]
Form Validation Errors [1]
Interesting Headers [2]
JavaScript Files [9]
MIME Types [14]
Not Founds [123]
Out of Scope Links [500]
Scan Performance [35]
Site Profile [1]
Slowest Pages [10]
SSL [1]
URL Rewrite [4]
Web Pages With Inputs [37]
Auto save finished successfully - 5/27/2023 09:02:52 PM
Crawling & Attacking (2/3)
3%
Previous Settings
AllOS-AllWebServer-AllAppServer-AllDBServer
Default Report Policy
13
28
30
87
Proxy: System

[Possible] Phishing by Navigating Browser Tabs

LOW

URL : https://www.twitterflightschool.com/student/catalog

External Links :

```
https://twitter.com/i/twitter_blue_sign_up
https://twitter.com/i/verified-orgs-signup
https://business.twitter.com/en/form/contact-us.html?ref=web-fs-ao-gbl-ContactUsSection&amp;utm_source=fs&amp;utm_medium=web&amp;utm_campaign=ao&amp;utm_content=ContactUsSection
https://twitter.com/i/twitter_blue_sign_up
https://twitter.com/i/verified-orgs-signup
https://business.twitter.com/en/form/contact-us.html?ref=web-fs-ao-gbl-ContactUsSection&amp;utm_source=fs&amp;utm_medium=web&amp;utm_campaign=ao&amp;utm_content=ContactUsSection
```

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

Vulnerability Details

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"` can modify *window.opener.location* and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"` attribute, a third party site can change the URL of the source tab using *window.opener.location.assign* and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Risk type : Low

URL : https://www.twitterflightschool.com/student/catalog

External Links : https://twitter.com/i/twitter_blue_sign_up

https://twitter.com/i/verified-orgs-signup

https://business.twitter.com/en/form/contact-us.html?ref=web-fs-ao-gbl-ContactUsSection&amp;utm_source=fs&amp;utm_medium=web&amp;utm_campaign=ao&amp;utm_content=ContactUsSection

https://twitter.com/i/twitter_blue_sign_up

https://twitter.com/i/verified-orgs-signup https://business.twitter.com/en/form/contact-us.html?ref=web-fs-ao-gbl-ContactUsSection&amp;utm_source=fs&amp;utm_medium=web&amp;utm_campaign=ao&amp;utm_content=ContactUsSection

- **Vulnerability Details**

  Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

  Open windows with normal hrefs with the tag target="_blank" can modify window.opener.location and replace the parent webpage with something else, even on a different origin.

- **Impact**
  While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack rel="noopener noreferrer" attribute, a third party site can change the URL of the source tab using window.opener.location.assign and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

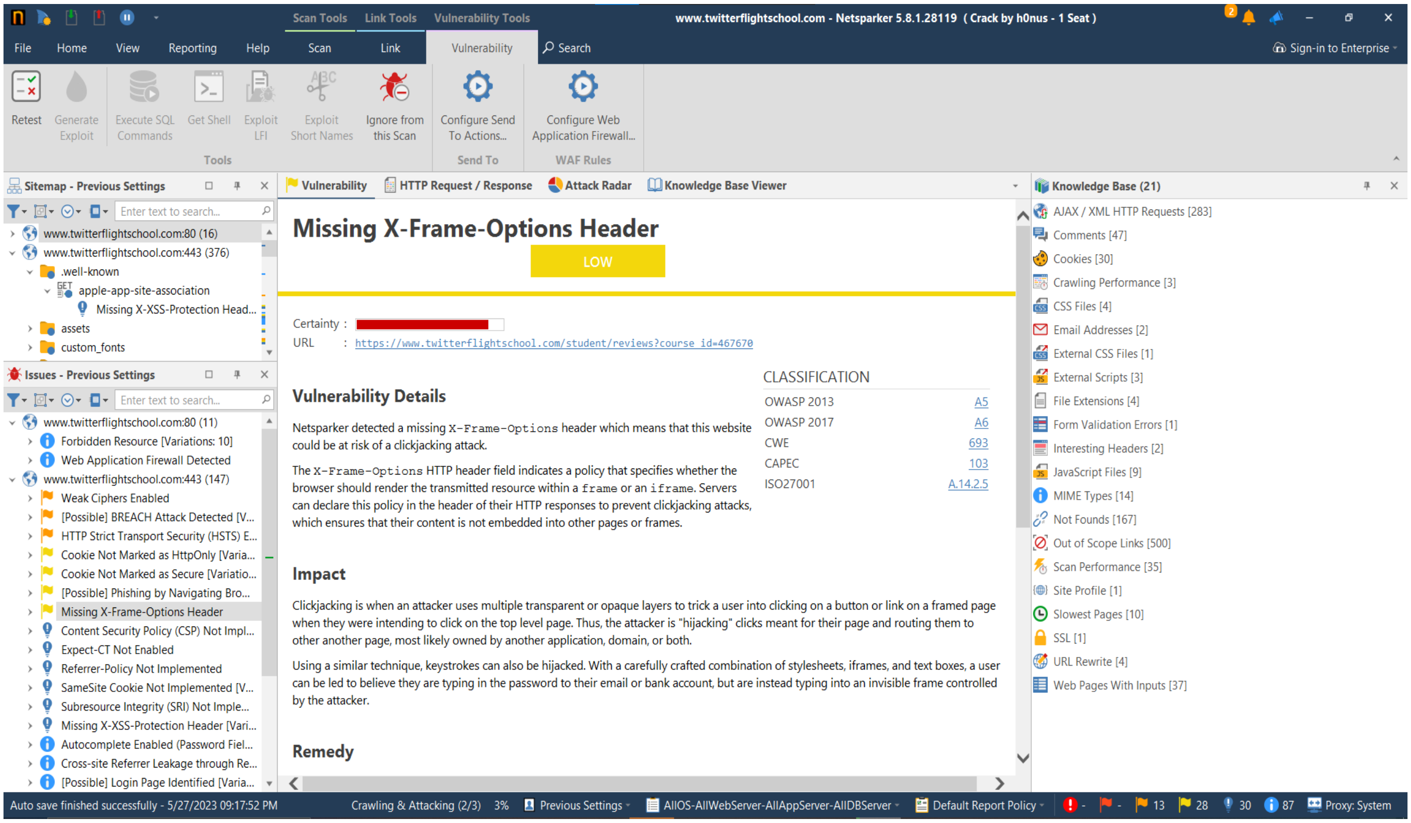
- **Remedy**

  Add rel=noopener to the links to prevent pages from abusing window.opener. This ensures that the page cannot access the window.opener property in Chrome and Opera browsers.

  For older browsers and in Firefox, you can add rel=noreferrer which additionally disables the Referer header.

  <a href="..." target="_blank" rel="noopener noreferrer">...</a>

6) Missing X-Frame-Options Header



Scan Tools
Link Tools
Vulnerability Tools
www.twitterflightschool.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Scan
Link
Vulnerability
Search
Sign-in to Enterprise
Retest
Generate Exploit
Execute SQL Commands
Get Shell
Exploit LFI
Exploit Short Names
Ignore from this Scan
Configure Send To Actions...
Configure Web Application Firewall...
Tools
Send To
WAF Rules
Sitemap - Previous Settings
Enter text to search...
www.twitterflightschool.com:80 (16)
www.twitterflightschool.com:443 (376)
.well-known
apple-app-site-association
Missing X-XSS-Protection Head...
assets
custom_fonts
Issues - Previous Settings
Enter text to search...
www.twitterflightschool.com:80 (11)
Forbidden Resource [Variations: 10]
Web Application Firewall Detected
www.twitterflightschool.com:443 (147)
Weak Ciphers Enabled
[Possible] BREACH Attack Detected [V...
HTTP Strict Transport Security (HSTS) E...
Cookie Not Marked as HttpOnly [Varia...
Cookie Not Marked as Secure [Variatio...
[Possible] Phishing by Navigating Bro...
Missing X-Frame-Options Header
Content Security Policy (CSP) Not Impl...
Expect-CT Not Enabled
Referrer-Policy Not Implemented
SameSite Cookie Not Implemented [V...
Subresource Integrity (SRI) Not Imple...
Missing X-XSS-Protection Header [Vari...
Autocomplete Enabled (Password Fiel...
Cross-site Referrer Leakage through Re...
[Possible] Login Page Identified [Varia...
Vulnerability
HTTP Request / Response
Attack Radar
Knowledge Base Viewer
Knowledge Base (21)
AJAX / XML HTTP Requests [283]
Comments [47]
Cookies [30]
Crawling Performance [3]
CSS Files [4]
Email Addresses [2]
External CSS Files [1]
External Scripts [3]
File Extensions [4]
Form Validation Errors [1]
Interesting Headers [2]
JavaScript Files [9]
MIME Types [14]
Not Founds [167]
Out of Scope Links [500]
Scan Performance [35]
Site Profile [1]
Slowest Pages [10]
SSL [1]
URL Rewrite [4]
Web Pages With Inputs [37]

Missing X-Frame-Options Header

LOW

Certainty :

URL : https://www.twitterflightschool.com/student/reviews?course_id=467670

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

Vulnerability Details

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

Auto save finished successfully - 5/27/2023 09:17:52 PM   Crawling & Attacking (2/3) 3%   Previous Settings   AllOS-AllWebServer-AllAppServer-AllDBServer   Default Report Policy   13   28   30   87   Proxy: System

Risk type : Low

URL : https://www.twitterflightschool.com/student/reviews?course_id=467670

- **Vulnerability Details**

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

- **Impact**

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

- **Remedy**

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.

X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.

X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.