

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

Full Name (Members)	Rico, Justroilon C.
Section\Sem\Year	IT42S2 / 2nd Sem / 4th Year

Intended Learning Outcomes

At the end of this activity, the student is expected to:

1. Determine the vulnerabilities of a website;
2. Apply some security measure to avoid the website vulnerability; and
3. Use a software to scan some web vulnerabilities.

Instructions

1. Do not change the format of this template.
2. Satisfy the given activity by providing the copy of the screenshots and other requirements needed as part of your output.
3. Format your document to **DOCS format**.
4. File Name : Use this format : LASTNAME_FIRSTNAME

5. Submit your document in this google drive link :
https://drive.google.com/drive/folders/1hYRwJmb5Clf2GC4jU0TBvvk0decYo_k1?usp=sharing

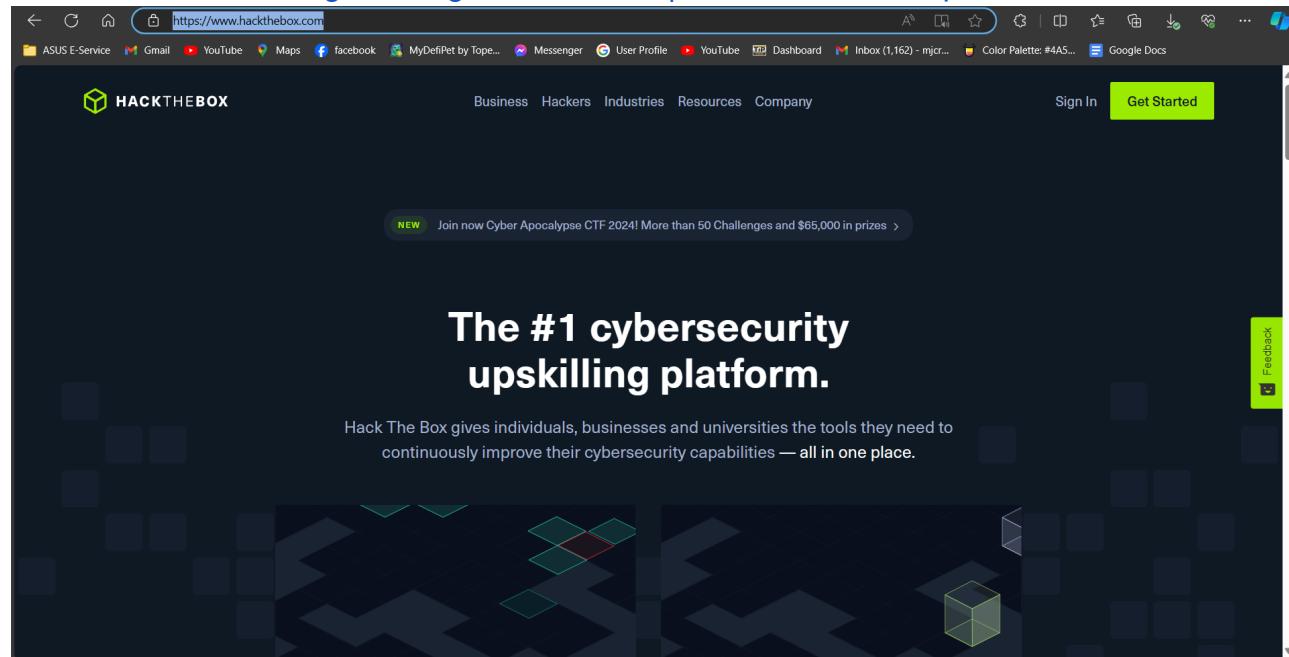
I. Requirements :

- 1.1. Search for five (5) Websites and analyze their Vulnerabilities and Security Measure.
- 1.2. Provide the Screenshot of the website homepage.
(write the URL at the top of the screenshot)
- 1.3. List all Vulnerabilities (sample scan proof and its interpretation, clear screenshot)
- 1.4. Software used in scanning (clear screenshot).

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

HackTheBox

[Hack The Box: Hacking Training For The Best | Individuals & Companies](https://www.hackthebox.com)



```
(kali㉿kali)-[~]
└─$ nikto -h www.hackthebox.com
- Nikto v2.5.0
-----
+ Multiple IPs found: 104.18.21.126, 104.18.20.126, 2606:4700::6812:157e, 2606:4700::6812:147e
+ Target IP:          104.18.21.126
+ Target Hostname:    www.hackthebox.com
+ Target Port:        80
+ Start Time:         2024-03-01 20:17:08 (GMT-5)
-----
+ Server: cloudflare
+ /: IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ /: IP address found in the 'set-cookie' header. The IP is "1.0.1.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: 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 type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.hackthebox.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

- Port 80 is the standard port for websites, and it can have a lot of different security issues. These holes can allow an attacker to gain either administrative access to the website, or even the web server itself.

Vulnerability testing Tool:

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

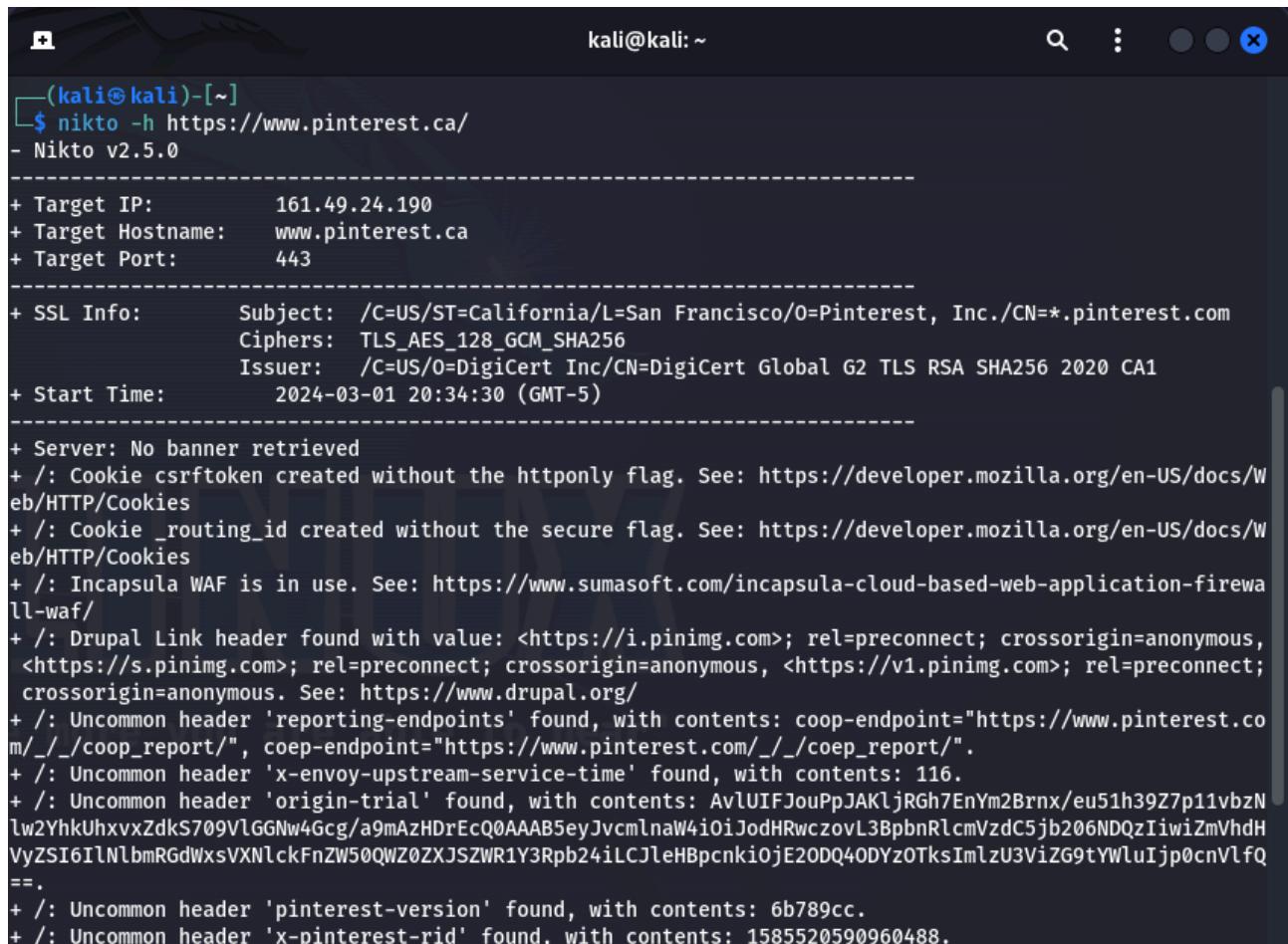
The screenshot shows the Kali Linux website's "Tools" section. On the left, there's a sidebar for the "Nikto" tool, featuring a blue alien head icon, the version information "version: 2.5.0 arch: all", and links to the homepage, package tracker, source code repository, and edit page. Below this is a "Metapackages" section with filters for "default", "everything", and "large". A link to the URL "https://www.kali.org/tools/" is also present. The main content area on the right is titled "Tool Documentation:" and contains a heading "Nikto Usage Example" followed by a terminal window displaying the output of a Nikto scan. The output includes details about the target IP (192.168.0.102), port (80), start time (2018-03-23 10:49:04), and various findings such as Apache version, X-Frame-Options header, and allowed HTTP methods.

```
- Nikto v2.1.6
-----
+ Target IP:      192.168.0.102
+ Target Hostname: 192.168.0.102
+ Target Port:    80
+ Start Time:    2018-03-23 10:49:04 (GMT0)
-----
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 287, size: 11832, mtime
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to p
+ The X-Content-Type-Options header is not set. This could allow the user agent to render
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily bru
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 371 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:        2018-03-23 10:50:44 (GMT0) (100 seconds)
```

Pinterest
[\(29\) Pinterest](#)

The screenshot shows the Pinterest homepage. At the top, there's a navigation bar with the Pinterest logo, "Watch", and "Explore" buttons. The main headline reads "Get your next weeknight dinner idea" with a call-to-action button below it. Below the headline are several food-related images: a salad, a cocktail, hands preparing food, a beetroot dish, and a grilled dish. To the right, a "Use Pinterest with Google" sign-in modal is open, showing two accounts: "JUSTROILON RICO" and "Jstroilon Rico". A yellow banner at the bottom says "Here's how it works ▾".

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form



(kali㉿kali)-[~]\$ nikto -h https://www.pinterest.ca/
- Nikto v2.5.0

+ Target IP: 161.49.24.190
+ Target Hostname: www.pinterest.ca
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Pinterest, Inc./CN=*.pinterest.com
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
+ Start Time: 2024-03-01 20:34:30 (GMT-5)

+ Server: No banner retrieved
+ /: Cookie csrfToken created without the httponly flag. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>
+ /: Cookie _routing_id created without the secure flag. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>
+ /: Incapsula WAF is in use. See: <https://www.sumasoft.com/incapsula-cloud-based-web-application-firewall-waf/>
+ /: Drupal Link header found with value: <<https://i.pinimg.com>>; rel=preconnect; crossorigin=anonymous,
<<https://s.pinimg.com>>; rel=preconnect; crossorigin=anonymous, <<https://v1.pinimg.com>>; rel=preconnect;
crossorigin=anonymous. See: <https://www.drupal.org/>
+ /: Uncommon header 'reporting-endpoints' found, with contents: coop-endpoint="https://www.pinterest.com/_/coop_report/", coop-endpoint="https://www.pinterest.com/_/coep_report/".
+ /: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 116.
+ /: Uncommon header 'origin-trial' found, with contents: AvlUIFJouPpjAKljRGh7EnYm2Brnx/eu51h39Z7p11vbzN
lw2YhkUhvxZdkS709VlGGNw4Gcg/a9mAzHDrEcQ0AAAB5eyJvcmlnaW4iOjodHRwczovL3BpbnRlcwVzdC5jb206NDQzIiwiZmVhdH
VyzSI6IlNlbmRgdWxsVXNlckFnZW50QWZ0ZXJSZWR1Y3RpB24iLCJleHBpcnki0jE20DQ40DYzOTksImlzU3ViZG9tYWluIjp0cnVlfQ
==.
+ /: Uncommon header 'pinterest-version' found, with contents: 6b789cc.
+ /: Uncommon header 'x-pinterest-rid' found, with contents: 1585520590960488.

- port 443 is part of the HTTPS protocol, being one of the paths that allow access to data packets. This port is vulnerable to SQL injections, cross-site scripting, DDoS attacks, and cross-site request forgery.
- Cross-Origin-Embedder-Policy (COEP): is a security header that allows a web page to control the behavior of how its resources are embedded into other websites. When set to "report-only" mode, as indicated by the "Report-Only" directive in the header, the policy is not enforced, but violations are reported to a specified endpoint, allowing website owners to monitor potential issues without breaking functionality.
- X-Content-Type-Options header not set: The X-Content-Type-Options header is not set, which could allow the browser to interpret content differently than the MIME type specified. This could potentially lead to MIME-sniffing attacks.

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

The screenshot shows the Kali Linux website's "Tools" section. On the left, there is a sidebar for the "Nikto" tool, which includes a blue alien head icon, the version information "version: 2.5.0 arch: all", and links to the homepage, package tracker, source code repository, and edit page. Below this is a "Metapackages" section with filters for "default", "everything", and "large". A link to the tools index is also present. The main content area on the right is titled "Tool Documentation:" and contains a section titled "Nikto Usage Example" with a terminal window displaying the output of a Nikto scan. The output shows details about the target IP (192.168.0.102), port (80), and start time (2018-03-23 10:49:04). It also lists various findings such as Apache version, X-Frame-Options header, and allowed HTTP methods.

```
- Nikto v2.1.6
-----
+ Target IP:      192.168.0.102
+ Target Hostname: 192.168.0.102
+ Target Port:    80
+ Start Time:    2018-03-23 10:49:04 (GMT0)
-----
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 287, size: 11832, mtime
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to p
+ The X-Content-Type-Options header is not set. This could allow the user agent to render
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily bru
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 371 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:        2018-03-23 10:50:44 (GMT0) (100 seconds)
```

Friv

[Friv® | FRIV.COM : The Best Free Games! \[Jogos | Juegos\]](#)



Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

```
kali@kali: ~
+ /: 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
+ /7eznt07T.Big5: Uncommon header 'akamai-grn' found, with contents: 0.0c1431a1.1709343328.44267bb6.
+ /7eznt07T.php#: The X-Content-Type-Options header is not set. This could allow the user agent to rende
r the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-v
ulnerability-scanner/vulnerabilities/missing-content-type-header/
^C

(kali㉿kali)-[~]
$ nikto -h https://www.friv.com
- Nikto v2.5.0

Multiple IPs found: 23.105.171.94, 198.7.62.130, 207.244.86.26, 23.105.171.82, 207.244.69.244, 192.96.
201.39, 23.105.171.150
+ Target IP: 23.105.171.94
+ Target Hostname: www.friv.com
+ Target Port: 443

SSL Info: Subject: /CN=www.friv.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Let's Encrypt/CN=R3
Start Time: 2024-03-01 20:43:46 (GMT-5)

Server: nginx
+ /: 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 site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: 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/
```

- Port 443, integral to the HTTPS protocol, serves as a conduit for data packet transmission. Despite its encryption, this port remains susceptible to various threats including SQL injections, cross-site scripting, DDoS attacks, and cross-site request forgery.
- anti-click hijacking x-frame-options: "The X-Frame-Options header is a security measure designed to counteract clickjacking attacks by controlling whether a web page can be embedded within an iframe on another site. By configuring the X-Frame-Options header with values like "DENY" or "SAMEORIGIN", site administrators can reduce the risk of clickjacking incidents where users are deceived into interacting with content from a different website without their awareness."
- TLS and the Strict-Transport-Security HTTP header is not defined: "TLS (Transport Layer Security) and the Strict-Transport-Security (HSTS) HTTP header are essential components of web security. TLS ensures secure communication by encrypting data between clients and servers, while the HSTS header instructs web browsers to only communicate with a website over HTTPS, thereby enhancing protection against various attacks."

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

The screenshot shows the Kali Linux website with the 'Nikto' tool page selected. The main content area displays the 'Tool Documentation:' section, which includes a heading 'Nikto Usage Example' and a code block showing the output of a Nikto scan. The output details the target IP (192.168.0.102), port (80), start time (2018-03-23 10:49:04 GMT), and various findings such as Apache version, X-Frame-Options header, and allowed HTTP methods.

```
- Nikto v2.1.6
-----
+ Target IP:      192.168.0.102
+ Target Hostname: 192.168.0.102
+ Target Port:    80
+ Start Time:    2018-03-23 10:49:04 (GMT0)
-----
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 287, size: 11832, mtime
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to p
+ The X-Content-Type-Options header is not set. This could allow the user agent to render
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily bru
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 371 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:        2018-03-23 10:50:44 (GMT0) (100 seconds)
```

bWAPP

[bWAPP, a buggy web application! \(itsecgames.com\)](https://www.itsecgames.com)

The screenshot shows the bWAPP homepage. The top navigation bar includes links for Home, Bugs, Download, Talks & Training, and Blog. The main content area features a yellow banner with the text 'bWAPP' and 'an extremely buggy web app!' along with the MME Security Audits & Training logo. Below the banner, there's a section about what bWAPP is and how it can be used for penetration testing. Social media icons for Twitter, LinkedIn, Facebook, and YouTube are displayed on the right side. At the bottom, there's a footer with a license notice and system status indicators.

bWAPP, or a *buggy web application*, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.

What makes bWAPP so unique? Well, it has over **100 web vulnerabilities!**
It covers all major known web bugs, including all risks from the OWASP Top 10 project.

bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIIS and MySQL. It can also be installed with WAMP or XAMPP.
Another possibility is to download the *bee-box*, a custom Linux VM pre-installed with bWAPP.

Download our [What is bWAPP?](#) introduction tutorial, including free exercises...

bWAPP is for web application security-testing and educational purposes only.
Have fun with this free and open source project!

bWAPP is licensed under [\(CC BY-NC-ND\)](#) © 2022 MME BV / Follow [@MME_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [training?](#)

NLEX-SLEX Conn... Construction

9:55 am 02/03/2024 ENG US

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form



KaliLinux2023 [Running] - Oracle VM VirtualBox
File Machine View Input Device Help
Applications Places Terminal Mar 1 21:01
kali@kali:~

```
+ 0 host(s) tested
  (kali㉿kali)-[~]
  $ nikto -h https://www.itsrgames.com
  - Nikto v2.5.0
  -----
+ 0 host(s) tested
  (kali㉿kali)-[~]
  $ nikto -h https://www.itsecgames.com
  - Nikto v2.5.0
  -----
+ Target IP:      31.3.96.40
+ Target Hostname: www.itsecgames.com
+ Target Port:    443
  -----
+ SSL Info:       Subject: /CN=www.mmevbva.com
                  Cipher: ECDHE-RSA-AES256-GCM-SHA384
                  Issuer: /CN=www.mmevbva.com
+ Start Time:    2024-03-01 20:56:36 (GMT -5)
  -----
+ Server: Apache
+ /: 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 site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: 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://www.mmevbva.com
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

- anti-click hijacking x-frame-options: "The X-Frame-Options header is a security measure designed to counteract clickjacking attacks by controlling whether a web page can be embedded within an iframe on another site. By configuring the X-Frame-Options header with values like "DENY" or "SAMEORIGIN", site administrators can reduce the risk of clickjacking incidents where users are deceived into interacting with content from a different website without their awareness."
- X-Content-Type-Options header is not set: "Not setting the X-Content-Type-Options header may leave a website vulnerable to security risks. This header helps prevent MIME type sniffing attacks by instructing browsers to strictly adhere to the declared content type."

Hack This Site
[Hack This Site](#)

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

The screenshot shows the homepage of HackThisSite.org. It features a header with the site's name and a navigation bar with links like "Hack This Site" (TOR, onion, HTTPS + HTTP), "IRC", "Discord", "Forums", "Store", "URL Shortener", "CryptoPaste", "Like Us", "Follow Us", and "Fork Us". Below the header is a large banner with the text "Support HackThisSite" and "ADVERTISE WITH US". A sub-banner below it says "The revolution will come when hackers meet political activists...". To the left is a "Login (or Register)" form and a "DONATE" button. In the center, there's a drawing of a computer monitor with the text "Training the hacker underground". On the right, there are sections for "STAFF BLOGS / SHORT NEWS", "LATEST ARTICLES", "HackThisSite on GitHub", and "CONTRIBUTE". At the bottom, there are sections for "LAST CHALLENGE COMPLETED" and "LATEST FORUM POSTS".

The screenshot shows a terminal window on a KaliLinux system. The terminal window title is "kali@kali:~". The command entered is "\$ nikto -h https://hackthissite.org -ssl". The output of the scan is displayed in the terminal. Key findings include:

- + Multiple IPs found: 137.74.187.100, 137.74.187.102, 137.74.187.103, 137.74.187.104, 137.74.187.101, 2001:41d0:8:cc08:137:74:187:102, 2001:41d0:8:cc08:137:74:187:103, 2001:41d0:8:cc08:137:74:187:101, 2001:41d0:8:cc08:137:74:187:104
- + Target IP: 137.74.187.100
- + Target Hostname: hackthissite.org
- + Target Port: 443
- + SSL Info: Subject: /CN=hackthisjognneh42n5o7gbzrwekee3vyu6ex37ukywd6j56npakiyd.onion, Ciphers: ECDHE-RSA-AES256-GCM-SHA384, Issuer: /C=GR/Hellenic Academic and Research Institutions CA/CN=HARICA DV TLS RSA 2048-03-01 21:07:09 (GMT-5)
- + Start Time: 2024-03-01 21:07:09 (GMT-5)
- + Server: HackThisSite
- + Cookie HackThisSite created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
- + Cookie HackThisSite created without the httpOnly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
- + 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 'public-key-pins-report-only' found, with contents: pin-sha256="Vh1duR9yKja0RAn73KnBQqJqUetMkgFfZFuing"; pin-sha256="Vjsb4r+280wNcr1XepW0bo5IR16wsXhIM+Myss"; max-age=259200; includeSubDomains; report-uri="https://hackthissite.org/r/hpkp/reportonly"
- + Uncommon header 'onion-location' found, with contents: http://hacdhkjhognneh42n5o7gbzrwekee3vyu6ex37ukywd6j56npakiyd.onion
- + 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/

- Cookie HackThisSite created without the secure flag: "A cookie named 'HackThisSite' has been created without the 'secure' flag. This flag is a security feature that ensures cookies are only transmitted over secure HTTPS connections, reducing the risk of interception by unauthorized parties."
- public-key-pins-report-only: "Website includes the 'public-key-pins-report-only' header, indicating the use of Public Key Pinning (HPKP) in report-only mode. This mode reports pinning violations to a designated endpoint without enforcing pin validation, allowing administrators to monitor potential issues without immediate impact on users."
- X-Content-Type-Options header is not set: The absence of the X-Content-Type-Options header can leave a website vulnerable to certain types of attacks, such as MIME sniffing, where browsers may interpret content types

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

incorrectly. This header instructs browsers to adhere strictly to the declared content type and not perform MIME type sniffing, thus enhancing security.

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

II. Rubric

Criteria	Description	Points
Website Vulnerability Assessment (40 points)		
1. Identification of Common Vulnerabilities	Accurate identification of common website vulnerabilities (e.g., SQL injection, XSS, CSRF)	10
2. Identification of Critical Vulnerabilities	Accurate identification of critical vulnerabilities that could lead to significant data breaches or system compromise	10
3. Depth of Vulnerability Analysis	Thorough analysis of the website's code and configuration for vulnerabilities	10
4. Documentation of Vulnerabilities	Clear documentation of identified vulnerabilities, including their severity and potential impact	10

Technological Institute of the Philippines Manila
 CBS404A - Cyber Threat Analysis and Modelling
 Activity Form

Security Measures Implementation (40 points)		
5. Application of Security Patches	Successful application of necessary security patches and updates	10
6. Implementation of Access Control	Effective implementation of access controls (e.g., authentication, authorization)	10
7. Encryption Implementation	Adequate use of encryption for sensitive data (e.g., SSL/TLS)	10
8. Security Practices	Adherence to security best practices (e.g., input validation, password policies)	10
9. Selection of Scanning Tool	Use of an appropriate vulnerability scanning tool	5

Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

Vulnerability Scanning and Assessment Tool (20 points)		
10. Scanning Accuracy	Accuracy of vulnerability scanning results	5
11. Interpretation of Scan Results	Ability to interpret and prioritize scan results	5

12. Documentation Scanning Process	Clear documentation of the scanning process, including tools used and results obtained	5
Total Points		100

"I affirm that I have not given or received any unauthorized help on this assignment, and that this work is my own."

(Your E-Signature)