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/1hYRwJmb5CIf2GC4jU0TBvvk0decYo_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)

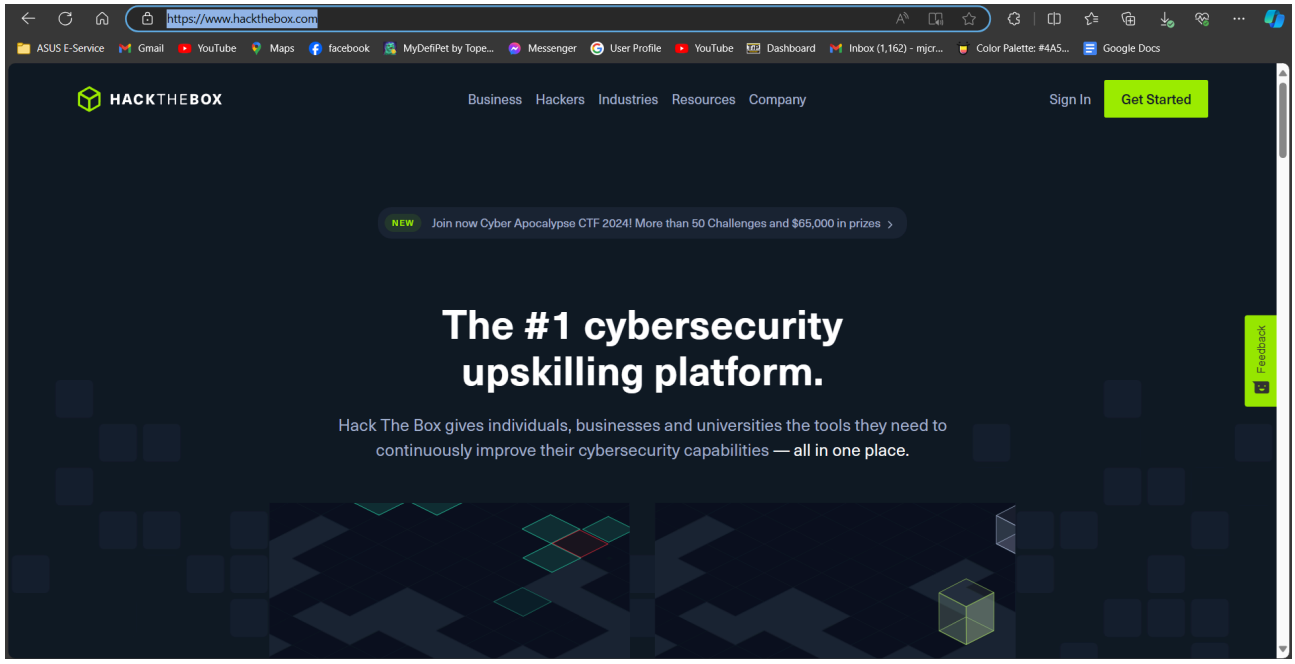
1.3. List all Vulnerabilities (sample scan proof and its interpretation, clear screenshot)

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]

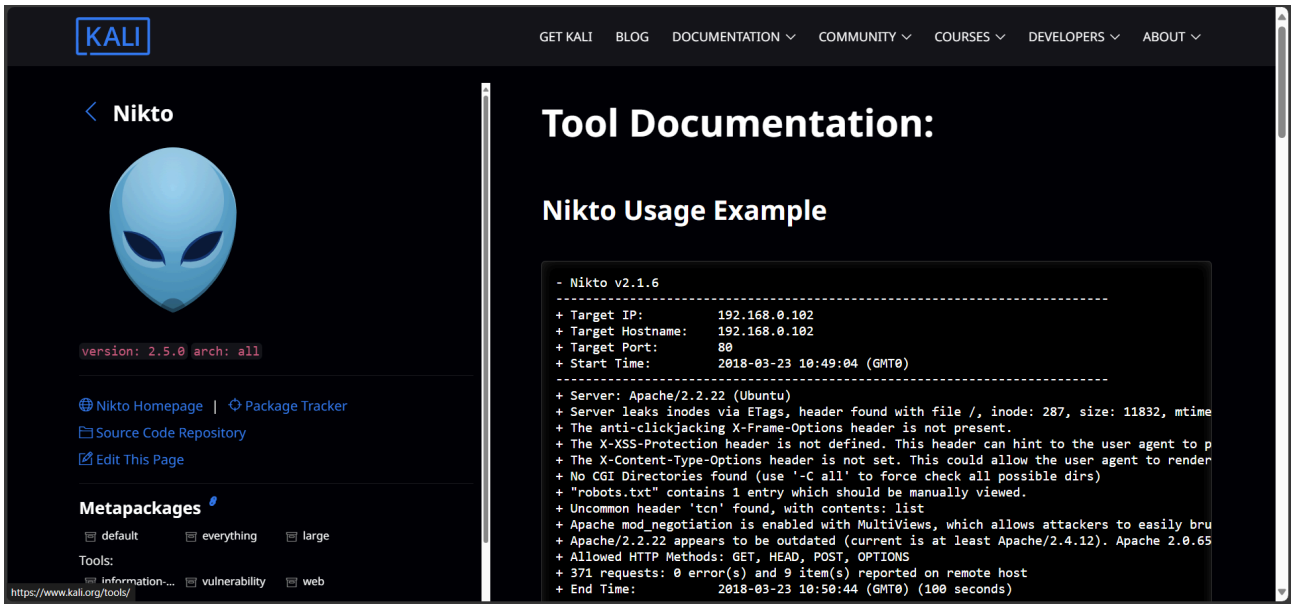



```
┌──(kali㉿kali)-[~]
└─$ nikto -h www.hackthebox.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.18.21.126, 104.18.20.126, 2606:4700::6812:157e, 2606:4700::6812:147e
+ Target IP:          104.18.21.126
+ Target Hostname:    www.hackthebox.com
+ 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: h
ttps://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 differe
nt fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-heade
r/
+ Root page / redirects to: https://www.hackthebox.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

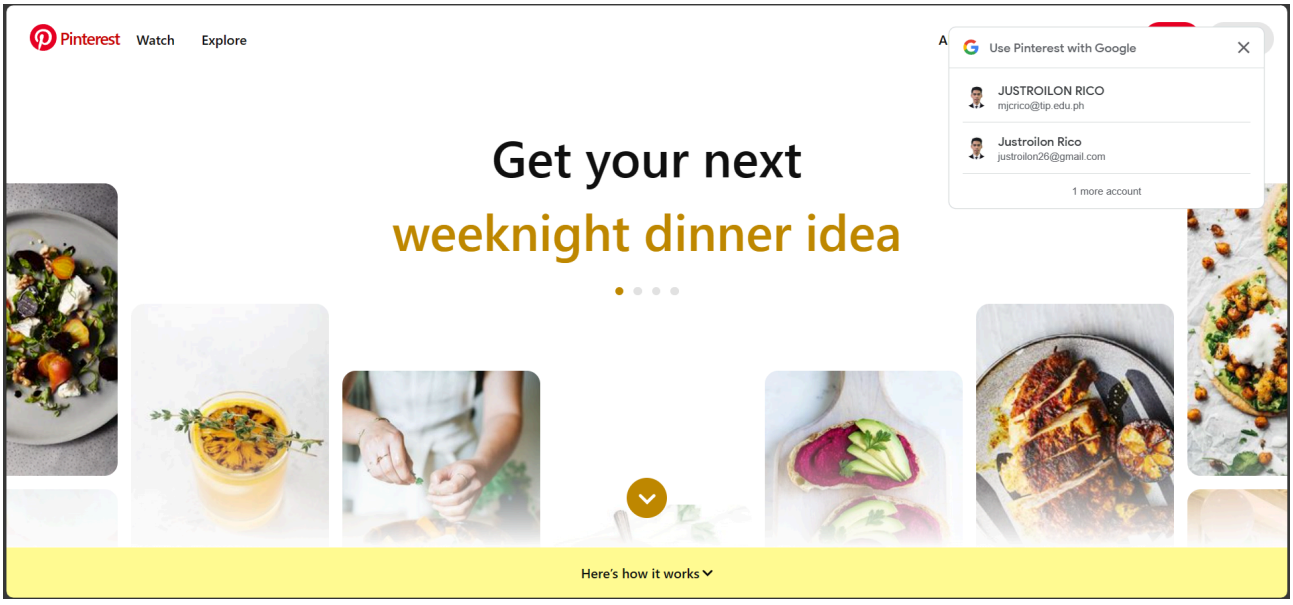
- Port 80 is the standard port for websites, and it can have a lot of different security issues. These holes can allow an attacker to gain either administrative access to the website, or even the web server itself.

Vulnerability testing Tool:

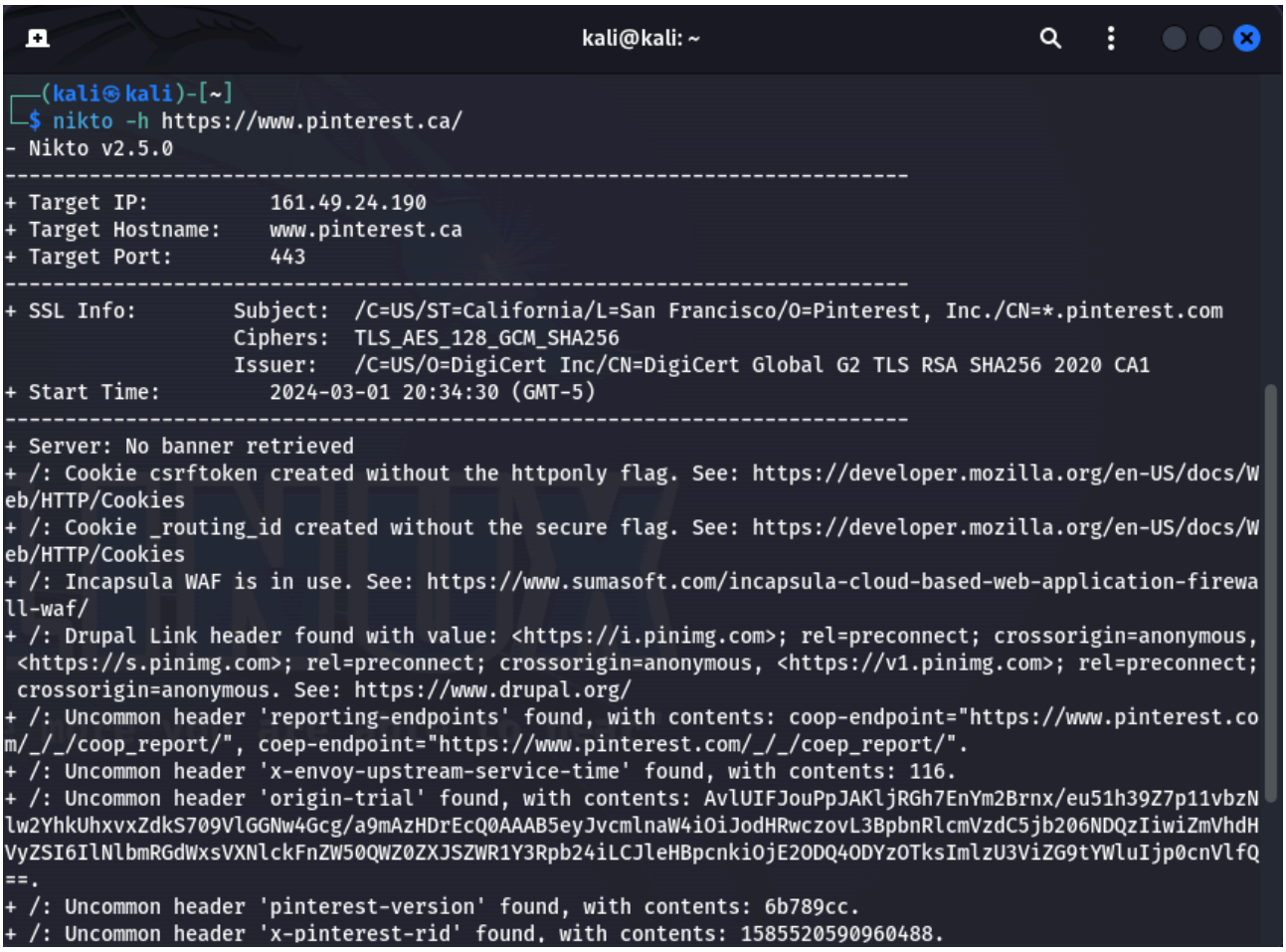
Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form



Pinterest
[(29) Pinterest]

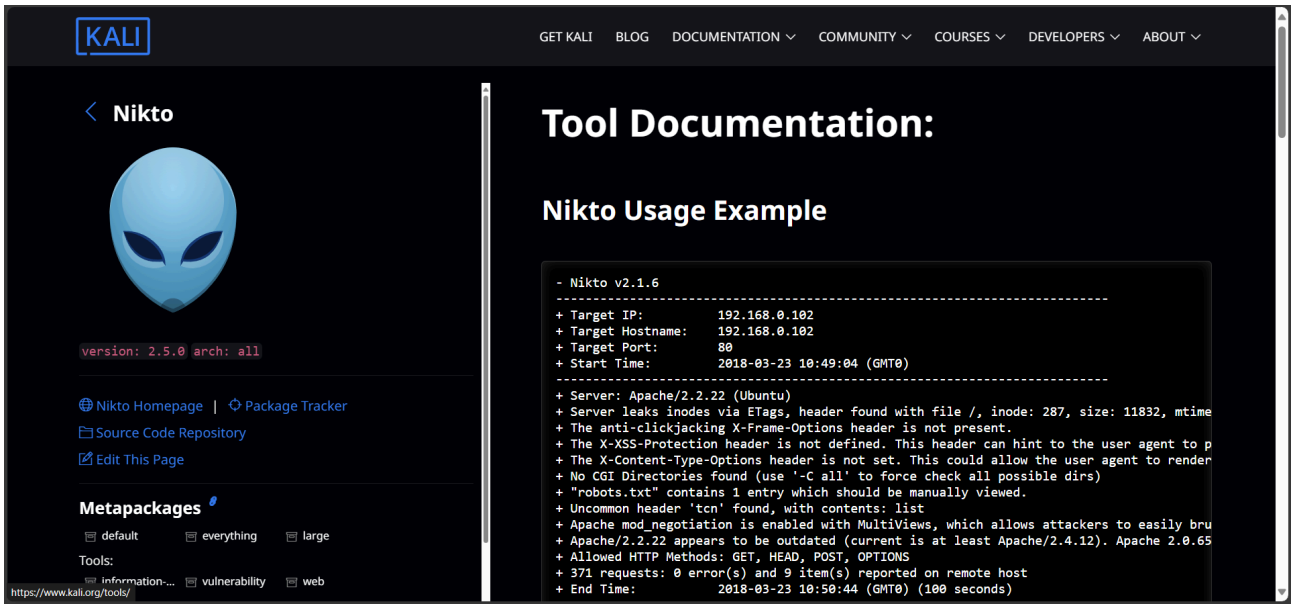


Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form



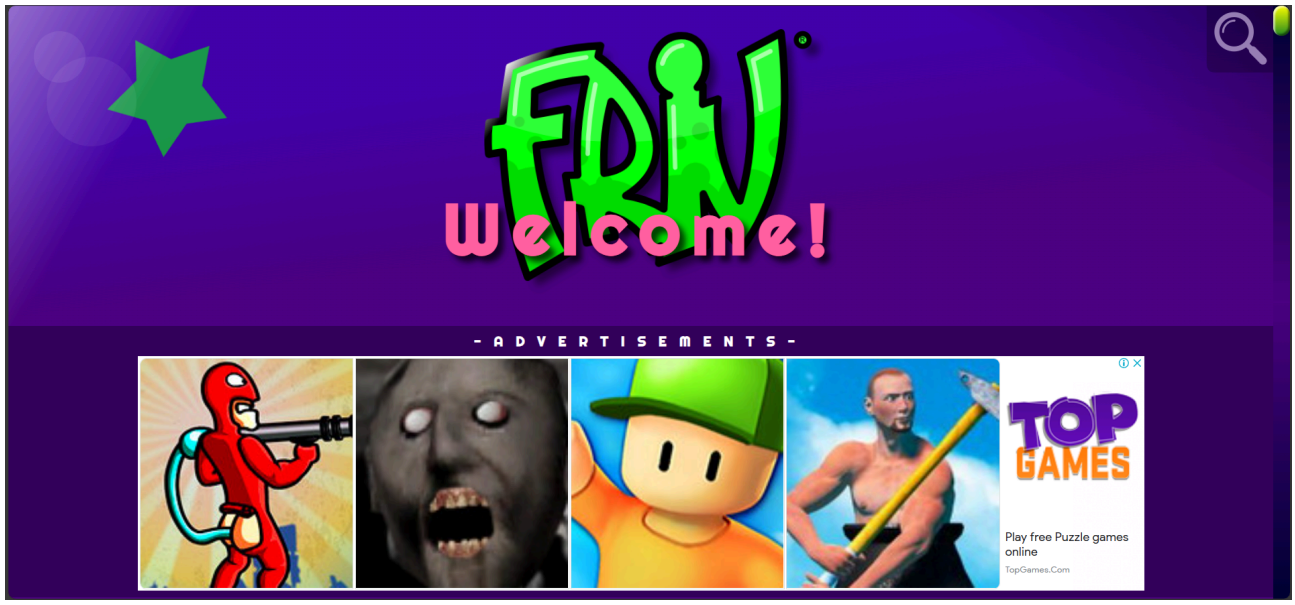
- port 443 is part of the HTTPS protocol, being one of the paths that allow access to data packets. This port is vulnerable to SQL injections, cross-site scripting, DDoS attacks, and cross-site request forgery.
- Cross-Origin-Embedder-Policy (COEP): is a security header that allows a web page to control 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



Friv

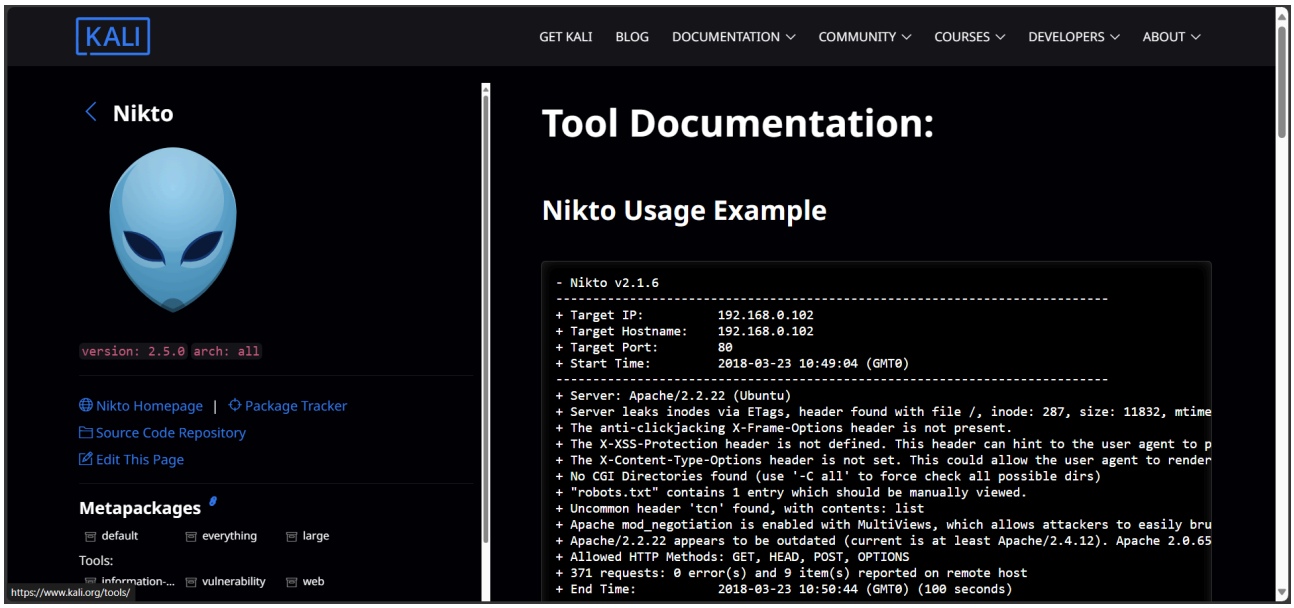
[Friv® | FRIV.COM : The Best Free Games! [Jogos | Juegos]]



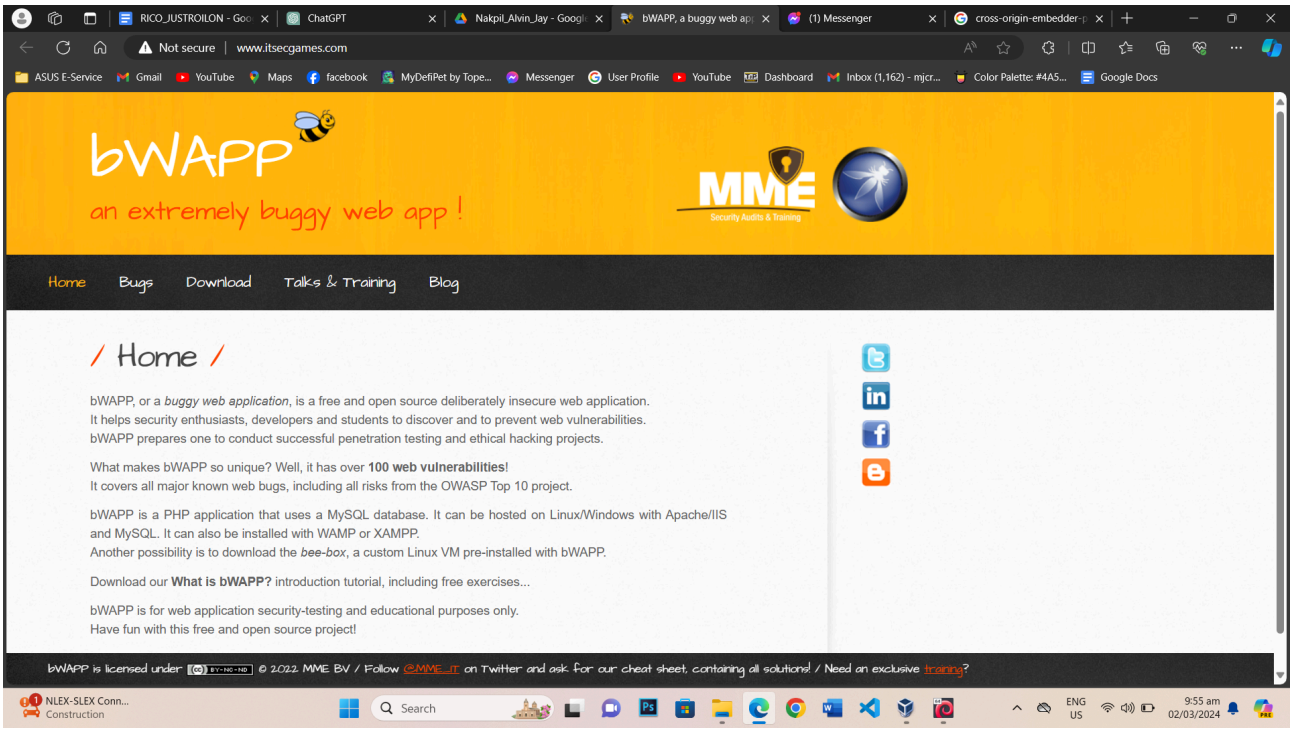
Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

- 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



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

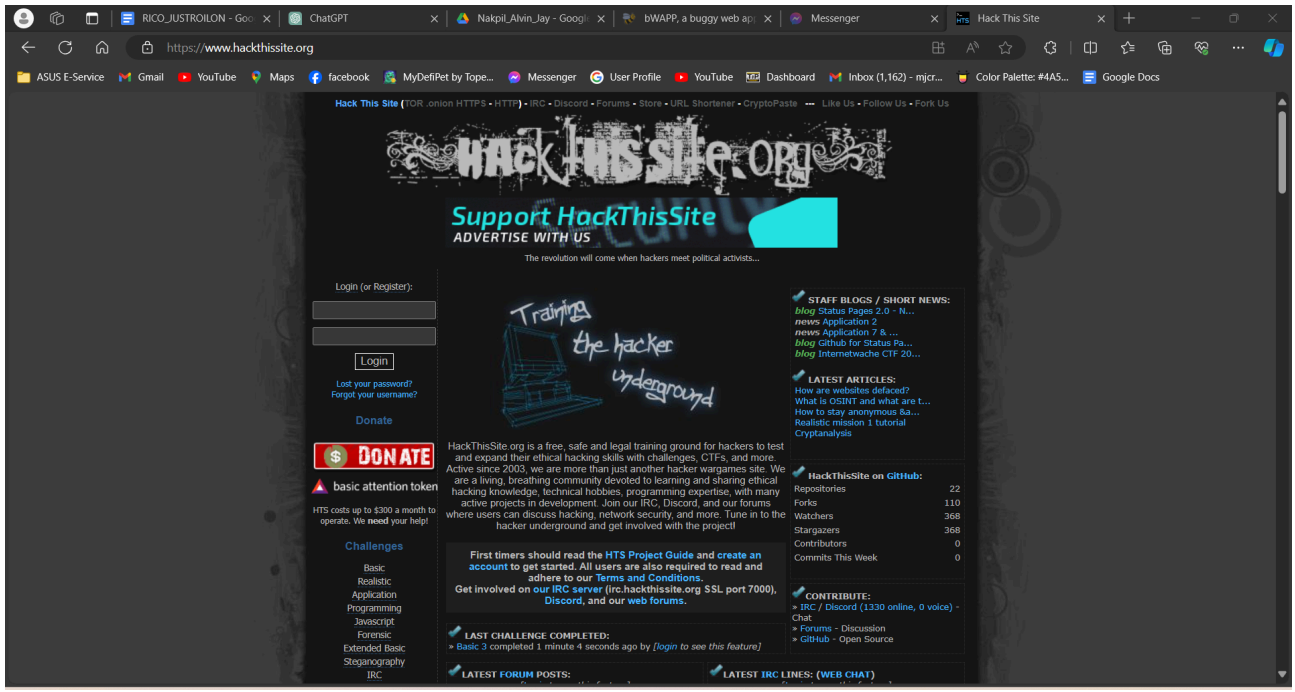


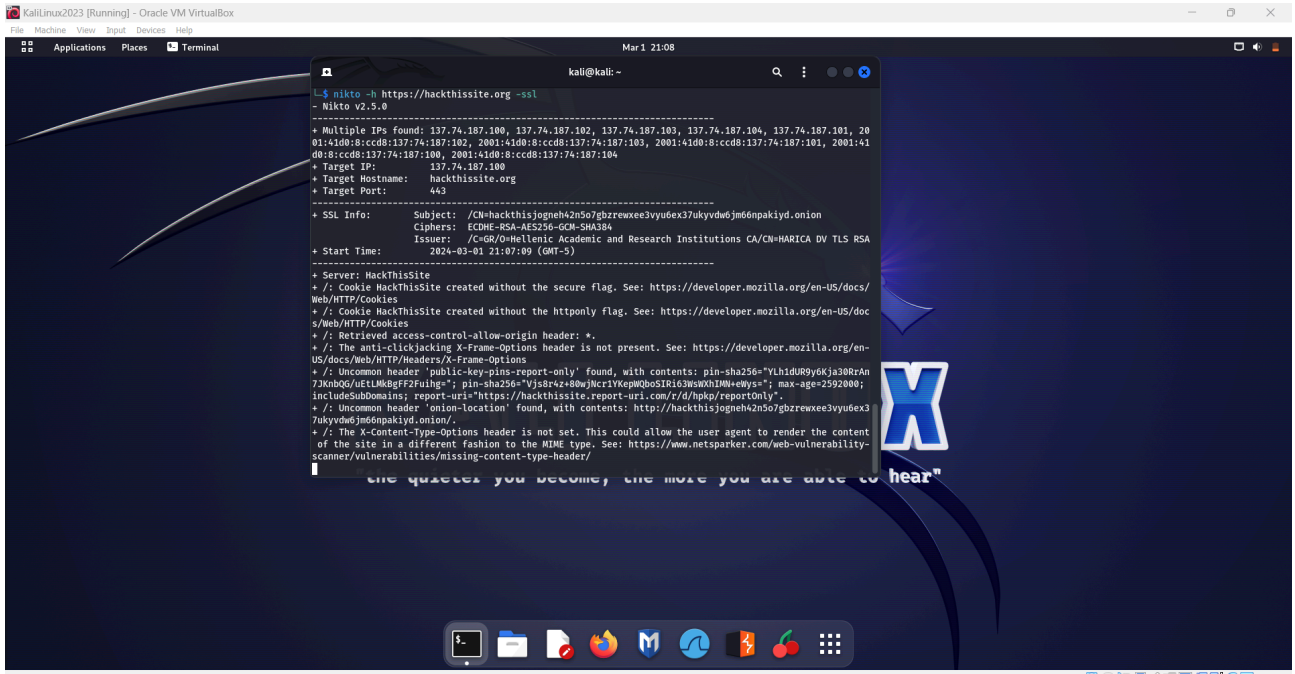
Technological Institute of the Philippines Manila
CBS404A - Cyber Threat Analysis and Modelling
Activity Form

- 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





- 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

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**

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 Best Practices	**Adherence to security best practices (e.g., input validation, password policies)**	**10**
Vulnerability Scanning and Assessment Tool (20 points)		
9. Selection of Scanning Tool	Use of an appropriate vulnerability scanning tool	5

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 of 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)