21BCE0965
Niraianbu porchezhian
Assignment 4

What is Burp Suite?

Burp Suite is a powerful and versatile cybersecurity tool specifically designed for web application security testing. It serves as a comprehensive solution for identifying and mitigating security vulnerabilities in web applications. Developed by PortSwigger, Burp Suite comes in two versions: Burp Suite Community (free) and Burp Suite Professional (paid, with advanced features).

Why Choose Burp Suite?

Burp Suite is the tool of choice for web application security testing for several reasons:

- Wide Range of Use: It covers a broad spectrum of web security testing tasks, including manual and automated testing, making it suitable for both beginners and experts.

- User-Friendly Interface: Its intuitive user interface simplifies the testing process and facilitates efficient vulnerability identification.

- Powerful Scanner: The tool includes an automated scanner capable of detecting various vulnerabilities, such as SQL injection, cross-site scripting (XSS), and more.

- Proxy Functionality: Burp Suite acts as a proxy, enabling the interception, inspection, and modification of HTTP requests and responses between your browser and the target web application.

- Extensibility: Users can enhance and customize its functionality through the use of extensions.

- Regular Updates: PortSwigger consistently updates Burp Suite to keep it aligned with evolving web application security standards and threats.

Key Features of Burp Suite:

Burp Suite boasts a range of essential features for effective web application security testing:

- Proxy: Intercept and modify HTTP requests and responses for detailed analysis.

- Scanner: Automatically scan web applications for vulnerabilities like SQL injection, XSS, CSRF, and more.

- Intruder: Conduct automated attacks on web applications for identifying vulnerabilities through methods like brute-forcing and fuzzing.

- Repeater: Perform manual testing by reissuing and modifying individual requests.

- Sequencer: Analyze the quality of randomness in tokens or session identifiers.

- Decoder: Decode and encode data in various formats, such as Base64 and URL encoding.

- Comparer: Identify differences between two responses, aiding in the detection of issues like information leakage.

- Extender: Support for custom extensions to expand Burp Suite's capabilities.

- Collaborator: Detect out-of-band vulnerabilities and interactions with external systems.

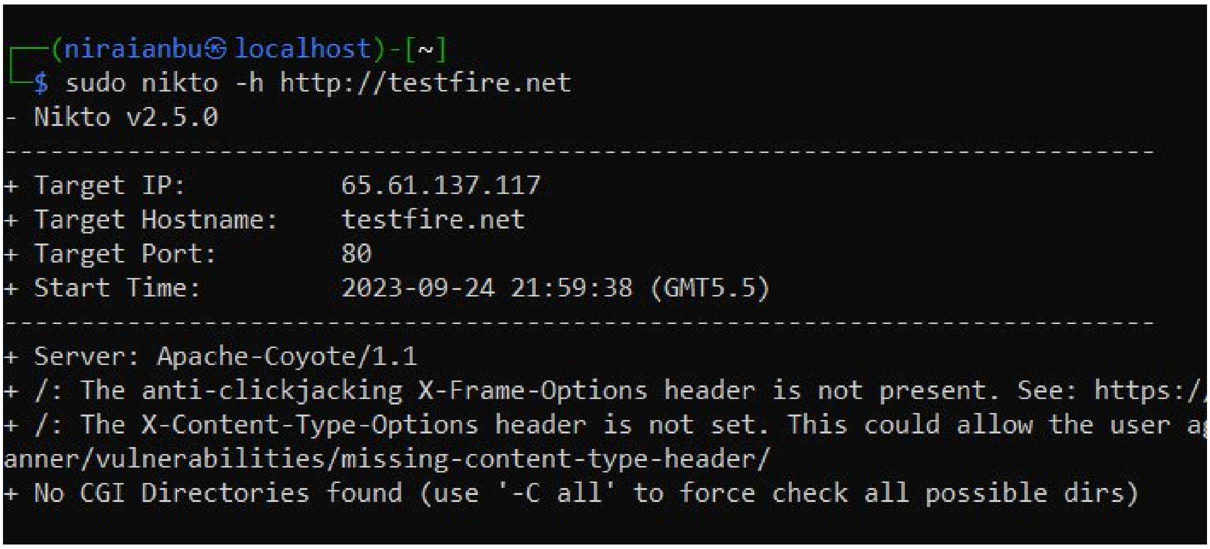
- Scanner Checks: A library of built-in security checks for various vulnerabilities.

- Session Handling: Manage and maintain session information during testing.

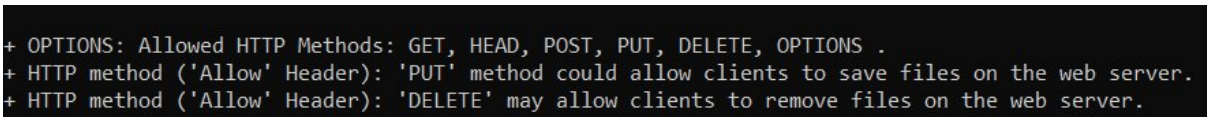
- Target Scope: Define the scope of your testing, specifying which parts of the application to include or exclude.

- Reporting: Generate detailed reports summarizing findings and vulnerabilities.

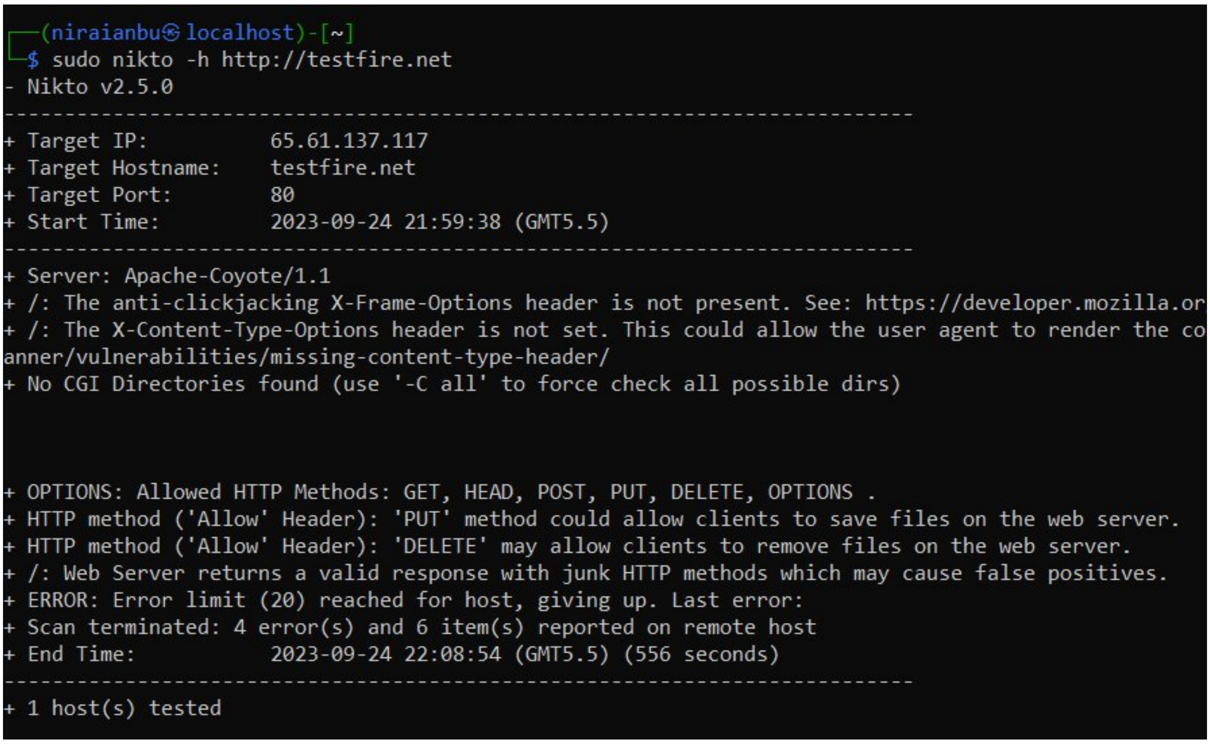
Testing Vulnerabilities on testfire.net:



```
┌──(niraianbu㉿localhost)-[~]
└─$ sudo nikto -h http://testfire.net
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2023-09-24 21:59:38 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:/
+ /: The X-Content-Type-Options header is not set. This could allow the user a
anner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```



```
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
```



```
┌──(niraianbu㉿localhost)-[~]
└─$ sudo nikto -h http://testfire.net
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2023-09-24 21:59:38 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.or
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the co
anner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)


+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 4 error(s) and 6 item(s) reported on remote host
+ End Time:           2023-09-24 22:08:54 (GMT5.5) (556 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```