**CIPHER'S WORLD**

TASK 1: ATTACK ON ANDROMEDA™

1. What city did the attack originate from?

Ans:- IP Address: 117.11.88.124, City: Tianjin

1. What’s the attacker’s user agent?

Ans:- Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

1. What's the name of the malicious web shell uploaded?

Ans:- image.php

1. Which directory is used by the website to store the uploaded files?

Ans:- /reviews/upload.php

TASK 2: WEB VULNERABILITY ASSESSMENT

1. Reconnaissance:

For reconnaissance of the domain spider.nitt.edu, We can use **WHOIS lookup** using online tools or command-line utilities to gather registration details and nameservers. Use DNS enumeration with tools like **dig** and **nslookup** to retrieve various DNS records. For discovering subdomains, we can use enumeration tools such as **Sublist3r** and **Amass**. Next to perform website fingerprinting with browser extensions like **Wappalyzer** or **BuiltWith** to identify the technologies used. We run **nmap** for port scanning to detect open ports and services on the domain.

2.Enumeration:

To identify potential attack vectors, we can begin with directory and file enumeration using tools like **dirb** or **gobuster** to uncover hidden paths. Service enumeration with **nmap** or **Nikto** will help identify running services and their versions, which can reveal outdated software. Use **Burp Suite** or **OWASP ZAP** to explore web application structures, including input fields and endpoints. Identify content management systems with tools like **wpscan** or **whatweb**, and assess SSL/TLS configurations using SSL Labs SSL Test or testssl.sh for potential weaknesses.

3.Vulnerability Testing:

To test for common web vulnerabilities, we used **sqlmap** to identify SQL injection points by scanning URL parameters and forms. For Cross-Site Scripting (XSS) vulnerabilities, we employed **Burp Suite** to inject test scripts into various input fields. We also conducted security misconfiguration assessments using **Nikto** to detect issues such as default credentials and directory listings, and checked SSL/TLS configurations with **SSL Labs SSL Test**. Each test was carefully documented, including the rationale and results for each vulnerability checked.