A purple triangle with a white tree and a red circle

Description automatically generated

**UNIVERSITI MALAYSIA TERENGGANU**

**SEMESTER 1 2023/2024**

**CYBER SECURITY CSF3233**

**LAB 8**

**PREPARED FOR:**

**MUHAMMAD ABDUL AALIM AHMAD ROSLI**

**PREPARED BY:**

**ARUN MUGILAN A/L SARGUNAN S63746**

**REFLECTION QUESTIONS:**

1. What are the most important steps you would recommend for securing a new Web Application?

* Robust Password Policies: Implement stringent password requirements and encourage the use of multi-factor authentication (MFA) to enhance security.
* Least Privilege Principle: Grant users the minimum necessary access based on their roles to limit potential risks.
* Secure Session Management: Employ secure session practices, such as using secure cookies and session tokens, to safeguard user sessions.

1. How would you perform a security test on a web application for unauthenticated tests on log-in page scenarios?

* Understanding Technology Stack: Gain a comprehensive understanding of the technologies, components, and data flows involved in the login process.
* Code Analysis: Inspect the code of the login page, analyzing HTML, JavaScript, and CSS for vulnerabilities or potential exposure of sensitive information.
* Testing for Common Vulnerabilities: Conduct tests to identify common vulnerabilities and observe the application's behavior during unauthenticated login scenarios.

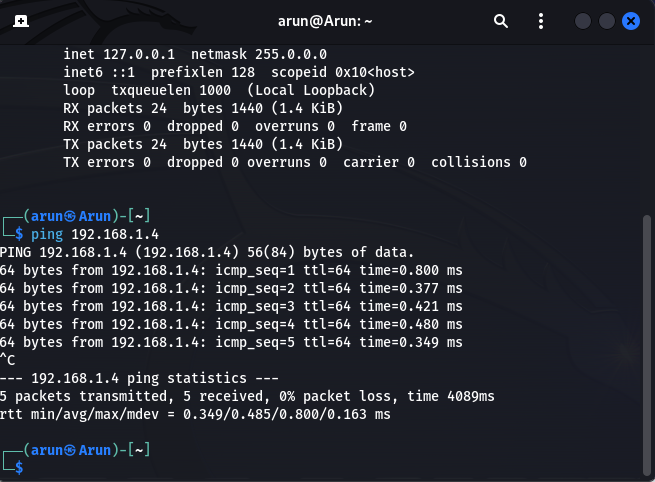
1. How does a web application firewall (WAF) detect and prevent attacks?

* Matching Known Attack Patterns: WAFs identify and prevent attacks by scrutinizing incoming traffic against databases of malicious signatures, blocking any matches with known attack patterns.
* Regular Signature Updates: The effectiveness of WAFs relies on regularly updating signature databases with the latest threat intelligence, ensuring timely protection against emerging threats.

1. List the challenges for the successful deployment and monitoring the web intrusion detection

* detection
* False positives and negatives
* Choosing the right IDS
* Effective replacement and configuration
* Resource constraints
* Tuning and customization
* User adoption and training

Task 1



A screenshot of a computer

Description automatically generated

A screenshot of a computer

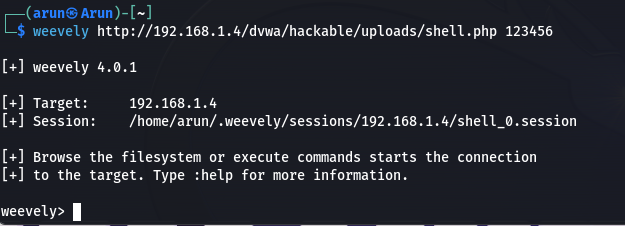
Description automatically generated

A screen shot of a computer

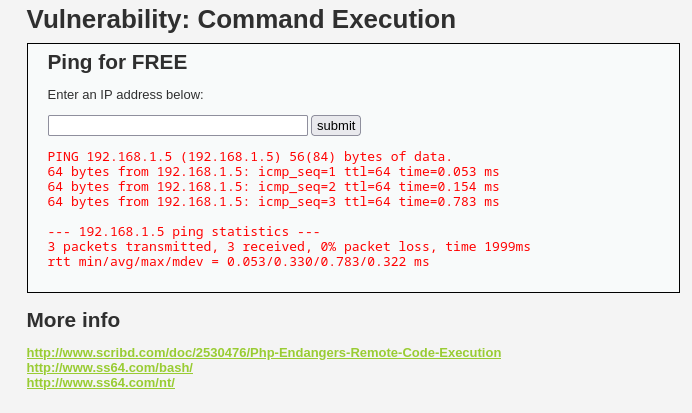
Description automatically generated

A screen shot of a file upload

Description automatically generated



Task 2



A screenshot of a computer

Description automatically generated

Task 3

A computer screen shot of a computer screen

Description automatically generated

5. It seems that we got some juicy information here. What information did you think you get? Maybe some of the questions below can be answered easily. Write your answer in your lab report.

a. What is the table name for keeping the user details?

* + Accounts

b. What are the fields of the identified table?

* + (username , password , mysignature)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated