5 A financial web application allows users to transfer funds through a form that inputs the recipient's account number and the amount to be transferred. The backend process for this transaction is handled by the following SQL statement in a PHP script:

php

Copy code

$sql = "INSERT INTO transactions (sender\_account, recipient\_account, amount) VALUES ('$sender', '$recipient', '$amount');";

(a) Highlight a potential vulnerability in the SQL statement above and explain how it might be exploited.

(2 marks)

(b) An attacker aims to exploit this vulnerability to transfer funds without proper authorization. What input could an attacker use for the $recipient and $amount variables to achieve this? Provide a hypothetical but plausible SQL injection example.

(3 marks)

(c) Detail THREE (3) security measures the web application developers can implement to prevent the exploitation of the vulnerability identified in Q5(a).

(6 marks)

(d) Explain the importance of auditing and monitoring transaction logs in detecting unauthorized transactions that might result from exploiting this vulnerability.

(2 marks)

(e) Consider the SQL statement and its context within the financial application. Discuss how ensuring ACID (Atomicity, Consistency, Isolation, Durability) properties in database transactions could mitigate potential impacts of the attack.

(3 marks)

# Considering the potential vulnerabilities in web applications:

[http://www.securedoc.com/login?error=<script>alert('Hacked!');</script](http://www.securedoc.com/login?error=%3cscript%3ealert('Hacked!');%3c/script)>

## Identify the vulnerability exploited in the scenario where the following URL is accessed:

(2 marks)

## What defensive strategies should CyberSafe Solutions implement to mitigate the risk of this vulnerability? Provide a brief explanation for each strategy.

(2 marks)

## Describe how an attacker could leverage the vulnerability identified in Q2(b)(i) to compromise user data or system integrity.

(2 marks)

# Identify which firewall that is suitable to do the following tasks.

## Deny all HTTP POST requests from certain country IP addresses.

## (Deny packet based on the packet’s destination address of 192.168.2.1.

## (iii) Deny email messages that contain an .exe files attachment.

## (iv) Compared to the firewall’s state table to determine if the packet’s state based on certain values in the TCP headers contradicts its expected state.

(4 marks)

(g) Identify the OSI layer that the firewall corresponds to for each task in Q4(f)(i) to (iv).

(4 marks)

(f) Determine the appropriate type of firewall for executing the tasks listed below:

(i) Filter out and block VoIP (Voice over IP) calls from identified spam numbers.

(ii) Block access to specific URLs on a corporate network, regardless of the protocol used to access them.

(iii) Prevent access to the network based on the MAC address of the device attempting to connect.

(iv) Analyze and block SQL injection attacks targeting web applications hosted within the network.

(4 marks)

(g) For each task in Q4(f)(i) to (iv), identify the corresponding OSI layer that the firewall operates on.

(4 marks)

# Reflecting on the following code segment used in a web application for file access:

# php

# Copy code

# $file = $\_GET['file'];

# include("/var/www/html/userdata/" . $file);

# (a) Identify the vulnerability present in this code.

# (1 mark)

# (b) Explain the potential risk if an attacker inputs a specially crafted value for the file parameter, assuming there are no safeguards against such manipulation.

# (2 marks)

# (c) Provide TWO (2) specific examples of how an attacker might exploit this vulnerability.

# (2 marks)

# (d) Suggest TWO (2) methods to secure this code against the identified vulnerability.

# (4 marks)

# (e) True or False: The vulnerability in this code snippet is mitigated by default in the latest versions of web servers, making it a non-issue for modern web applications.

# (1 mark)EGEGFEFGGGF

"INTRODUCTION TO INTERNET SECURITY

Evolution of Web Applications: Functions and advantages of web applications, Web Application Security: Services, Mechanisms and Attacks, Key issues, problem factors, security perimeter, Web security applications of the future"

"METHOD OF CONFIRMATION

User Access Handling: Authentication, Session Management, Access Control.

User Input Handling: Multiple inputs, boundary validation, multiple validation steps"

"METHOD OF CONFIRMATION

Attack control: Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks, Managing the Application."

"MESSAGE INTEGRITY

Authentication Technology,

Design Weaknesses in authentication mechanisms: Bad Passwords, Brute-Force Login, Verbose Failure Messages, Vulnerable Transmission of Credentials, Password Change Functionality, Forgotten Password Functionality, “Remember Me” Functionality, User Impersonation Functionality, Incomplete Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords."

"MESSAGE INTEGRITY

Implementation Flaws in Authentication: Fail-Open Login Mechanisms, Defects in Multistage Login Mechanisms, Insecure Storage of Credentials."

"TYPES OF INTERNET SECURITY THREATS

Hacking, Denial Of Service, Buffer Over Flow, Trojan Horse, Social Engineering, Malware, Viruses, Worms and Botnets

"

"TYPES OF INTERNET SECURITY THREATS

SQL Injection: Exploiting a Basic Vulnerability, Injecting into Different Statement Type, Finding SQL Injection Bugs, Fingerprinting the Database, UNION Operator, Extracting Useful Data, Extracting Data with UNION.

Cross site scripting: XSS Vulnerabilities, XSS Attack, Prevent XSS Attacks"

"APPLICATIONS AND SERVICES

Web Application Technology

HTTP Protocol: HTTP Request, HTTP Responses, URLs, Cookies, HTTPS, HTTP Proxies, HTTP Authentication

"

"APPLICATIONS AND SERVICES

Web Functionality: Server-Side Functionality, Client-Side Functionality, State and Sessions."

"INTERNET SECURITY INFRASTRUCTURE

Firewall System

"

"INTERNET SECURITY INFRASTRUCTURE

Internet and Network Security Monitoring System

Digital signature"

"INTERNET SECURITY RISK MANAGEMENT

Securing Authentication: Strong Credentials, Validate Credentials, Prevent Information Leakage"

"INTERNET SECURITY RISK MANAGEMENT

Prevent Brute-Force Attacks, Password Change Function, Account Recovery Function, Log, Monitor, and Notify"

"INTERNET SECURITY RISK MANAGEMENT

Risk Analysis Approach and Technology, Audit System"