We Test Pens Incorporated
COMP90074 - Web Security Assignment 3
Yichen Guan
ID:**********

THREAT MODELLING REPORT FOR Bank of UniMelb Pty. Ltd. - WEB APPLICATION

Report delivered: 12/06/2022

1. Threats identified using STRIDE

S: Spoofing

Threat 1: Attackers might pretend to be the victim by identity theft

Threat identified:

Attackers might steal the victim's identity information by phishing or social engineering. Attackers could use this information to bypass Bank identity verification and impersonate a victim to open a new account.

Threat actor:

The actor could be an external attacker who tries to use the victim's account to launder money.

Threat remediation:

1: Raise security awareness.

2: Do not easily download attachments in emails.

Threat 2: Attackers might obtain the victim’s password.

Threat identified

Attackers might Install malicious software such as keyloggers on the victim's computer to obtain passwords. Attackers could use that password to log in to the victim's account and transfer money.

Threat actor:

The actor could be an external attacker who tries to steal the victim's money.

Threat remediation:

1:The system uses the verification code to complete the login authorization through real-time verification.

2:Abnormal address login reminder.

T: Tampering

Threat 1: Attackers might capture and modify the network packet.

Threat identified:

Attackers could perform a man-in-the-middle attack to maliciously tamper with the victim's transfer amount or different accounts.

Threat actor:

The actor could be a bank client with hacking skills who wants to steal money from victim clients.

Threat remediation:

1:No connection to public free Wi-Fi.

2:Banking systems require complex encryption algorithms for network packets.

Threat 2: Attackers might maliciously modify web application content

Threat identified:

An attacker could perform an XSS attack by inserting malicious javascript code in the client profile textbox.

Threat actor:

The actor could be a bank client who tries to steal sensitive information.

Threat remediation:

1: Strictly restrict or filter client input.

2: Use Content Security Policy

R: Repudiation

Threat 1: The branch manager might delete the log file.

Threat identified:

The branch managers might use their permissions to browse client information and download client data without the client's authorisation. Finally, managers delete browsing and download the history log file.

Threat actor:

The actor could be the branch manager trying to sell clients' sensitive information for money.

Threat remediation:

1: Apply the Principle of Least Privilege.

Threat 2: Attackers might fill up the disk space on which the log file is being stored.

Threat identified:

After attackers perform unauthorized operations, they found out that the log file cannot be deleted. So they fill the disk space through methods such as injection and destroy the disk to achieve the purpose of delete the log file.

Threat actor:

The actor could be the external attacker who gain benefits by performing bank-busting operations.

Threat remediation:

1:Redundant backup of important data.

2:Perform abnormal flow monitoring

I: Information Disclosure

Threat 1: The branch manager leaks the client’s information.

Threat identified:

The branch managers might steal clients' private information at their job’ s convenience.

Threat actor:

The actor could be a branch manager who tries to steal sensitive information and sell it for money.

Threat remediation:

1: Apply the Principle of Least Privilege to the high-privileged account.

2: Any operations should be recorded and stored.

Threat 2: Attackers might capture the network packet.

Threat identified:

Attackers could perform a man-in-the-middle attack to obtain some sensitive information stored in the package, or the attacker could steal the client's cookies

Threat actor:

The actor could be an external attacker who tries to steal the victim's sensitive information.

Threat remediation:

1:No connection to public free Wi-Fi.

2:Banking systems should apply complex encryption algorithms for network packets.

D: Denial of Service

Threat 1: The attacker makes a large number of requests to consume the resources of the server.

Threat identified:

The attacker sends a large number of request packets at the same time, which consumes the bandwidth of the server and makes the server unable to work.

Threat actor:

The actor could be an external attacker trying to blackmail the bank for money.

Threat remediation:

1:Perform abnormal traffic monitoring.

2:Fix firewall vulnerabilities

Threat 2: Service failure due to branch manager wrong operation.

Threat identified:

The branch manager's wrong operation results in deleting the client's account. Clients whose account was deleted cannot complete normal transfer operations.

Threat actor:

The actor could be branch managers who have Insufficient professional skills.

Threat remediation:

1:Regular training of bank staff.

2: Apply the Principle of Least Privilege and separation of responsibility.

E: Elevation of Privilege

Threat 1: Horizontal privilege escalation

Threat identified:

An attacker exploits insecure direct object references via a hidden parameter to access other customers' data by switching the variable's value.

Threat actor:

The actor could be a bank client attempting to steal other clients' data.

Threat remediation:

1: Execute the privilege check before retrieving the object information

Threat 2: Vertical privilege escalation

Threat identified:

Attacker gains advanced privileges bypassing weak authentication such as client-side authentication.

Threat actor:

The actor could be a bank client who attempts to gain higher privileges to perform more unauthorized operations for money.

Threat remediation:

1: Move the validation operation to the server-side.

2: Banks should use a multi-factor authentication approach.