We Test Pens Incorporated

COMP90074 - Web Security Assignment 3
Jiahao Chen
1118749

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

Report delivered: 30/05/2023

1. Threats identified using STRIDE

S: Spoofing

Threat 1: Phishing Attacks

Attackers may build a fake website that looks like the site of Bank of UniMelb, which could trick users into providing sensitive information.

Threat 2: Impersonation of Branch Managers

Attackers may perform operations which require higher permissions if they have access to a branch manager’s account.

T: Tampering

Threat 1: Connection Tampering

Since users can get access to the system from their own laptop or computer, attackers could alter the data during transmission.

Threat 2: Code Injection

If the system does not properly sanitize user inputs, attackers may inject malicious code into the system.

R: Repudiation

Threat 1: Lack of Multi-Factor Authentication (MFA)

Users may repudiate their transactions and claim that their accounts were compromised. Besides, attackers could have access to users’ accounts easier.

Threat 2: Lack of Log Monitoring

It is difficult to discover malicious actors if no log monitoring is implemented since they can simply deny their actions.

I: Information Disclosure

Threat 1: Insecure Transmission

If the data is not encrypted during transmission or the encryption mechanism is weak, attackers can steal sensitive information.

Threat 2: Lack of Access Controls

If access controls are not properly implemented, it could be easier for attackers to have access to data which needs higher permissions.

D: Denial of Service

Threat 1: Account Lockouts

If attackers try multiple incorrect login attempts, users could be locked out of their accounts and cannot use the bank services.

Threat 2: Distributed Denial of Service (DDoS)

Since the system is open to personal devices, attackers could perform DDoS attack to make it unavailable to users.

E: Elevation of Privilege

Threat 1: Privilege Elevation

The system could have internal bugs which lead users to have some higher permissions. Similarly, branch managers may obtain higher administrative permissions. Note that this may not directly because of external attacks, but due to development errors.

Threat 2: Insecure Direct Object References (IDOR)

Users may be able to have access to resources owned by other accounts. Attackers can exploit this to find if there is sensitive information.

2. Threat actors

S: Spoofing

Threat 1: Phishing Attacks

Phishing attacks could be performed by external cybercrime organizations. Since the website is public, it is easy to mimic and build a similar one to steal sensitive information.

Threat 2: Impersonation of Branch Manager

It is possible that external organizations may steal branch managers’ credentials. Besides, it could be easier for a bank staff to steal a branch manager’s credentials, especially if the bank system has a high standard of security. Malicious bank clients could therefore perform unauthorized attacks or even expose the branch manager to legal liabilities.

T: Tampering

Threat 1: Connection Tampering

It is likely that cybercrime organizations may target on a user and tamper the connection between the user and the bank. The user could suffer from huge loss.

Threat 2: Code Injection

Threat actors can be either external organizations or internal staffs. Note that developers of the system may identify weaknesses of the system much easier.

R: Repudiation

Threat 1: Lack of Multi-Factor Authentication (MFA)

Cybercrime organizations or bank staffs may steal a branch manager’s credentials and perform operations requiring higher permissions. Since MFA is not implemented, it is hard to know if the branch manager’s account is compromised because attackers can deny their actions.

Threat 2: Lack of Log Monitoring

All kinds of threat actors can exploit this vulnerability to perform malicious operations. It is difficult to identify the attackers and their activities since no log is kept.

I: Information Disclosure

Threat 1: Insecure Transmission

Cybercrime organizations may intercept users’ transmission and steal their credentials. They could afterward perform transactions using the stolen accounts.

Threat 2: Lack of Access Controls

Bank staffs may attempt to gain higher permissions for illegal access to sensitive data or operations. Meanwhile, external cybercriminals may seek for higher permissions using stolen accounts.

D: Denial of Service

Threat 1: Account Lockouts

A single user block may be a prank or a targeted attack from someone who has malicious intentions towards the user. For widespread user lockouts, it may be launched by cybercrime organizations. Note that the usernames need to be first obtained.

Threat 2: Distributed Denial of Service (DDoS)

Since DDoS could require a huge number of resources and the consequence is only making the system unavailable, threat actors are more likely includes cybercrime organizations or state-sponsored actors.

E: Elevation of Privilege

Threat 1: Privilege Elevation

Any bank client or staff who found this vulnerability may become a threat actor and perform actions beyond their permissions to benefit themselves.

Threat 2: Insecure Direct Object References (IDOR)

Any bank client or staff this vulnerability may become a threat actor and steal other accounts’ information.

3. Threats remediations

S: Spoofing

Threat 1: Phishing Attacks

Since phishing attacks may not be directly related to a type of internal vulnerability of the website, the remediation could focus on informing and educating customers on identifying potential phishing scams. Besides, it is essential to implement an SSL certificate to help users judge if the website is legitimate.

Threat 2: Impersonation of Branch Manager

It is essential to implement multi-factor authentication (MFA) for branch manager logins. Besides, it is necessary to have a log monitoring the system to detect malicious activities.

T: Tampering

Threat 1: Connection Tampering

All data should be encrypted in transit, for example, using AES or TLS. Moreover, for dangerous operations such as closing accounts, it is better to requiring users to go to a branch with their photo IDs.

Threat 2: Code Injection

All user inputs should be rigorously validated and sanitized. In addition, it is necessary to have access control and monitor unauthorized activities.

R: Repudiation

Threat 1: Lack of Multi-Factor Authentication (MFA)

It is essential to implement an MFA method, such as SMS or email-based codes. Third-party authenticator apps could also be taken into consideration. Meanwhile, it is necessary to inform users the importance of MFA and how to enable it.

Threat 2: Lack of Log Monitoring

Auditing and log management should be implemented. It could include real-time analysis on the activities and raise alerts when abnormal activities are detected. For example, the ELK stack is a good choice for implementing such mechanisms.

I: Information Disclosure

Threat 1: Insecure Transmission

Ensure that all data are encrypted during transmission, using AES or TLS. Moreover, MFA may alleviate the loss to some extent if credentials are leaked.

Threat 2: Lack of Access Controls

The principle of least privilege (PoLP) can be applied when developing the system to ensure that different users only have access to the needed data.

D: Denial of Service

Threat 1: Account Lockouts

Implement CAPTCHA to prohibit automated login attempts. Meanwhile, users could be notified when someone is attempting to login to their accounts. Moreover, an IP address should be blocked if it performs too many requests.

Threat 2: Distributed Denial of Service (DDoS)

Rate limiting and load balancing are necessary for dealing with DDoS. However, DDoS mitigation service could be considered as they could directly provide professional supports, especially if the time is limited to develop a protection mechanism.

E: Elevation of Privilege

Threat 1: Privilege Elevation

Access controls should be implemented across the system to separate privileges. Meanwhile, the log could be helpful to monitor if there is any privilege elevation.

Threat 2: Insecure Direct Object References (IDOR)

Ensure that access controls are also implemented at object level, for example, having an access control list (ACL). Meanwhile, the log could be used to identify IDOR.