We Test Pens Incorporated
COMP90074 - Web Security Assignment 3
Jiaxuan Feng
965867r

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

Report delivered: 6/6/2021

S: Spoofing

Threat 1: Attacker authenticates as other users after brute-forcing password

Threat identified

An attacker can use brute force method to figure other users' password, and log into the application as the targeted user. With this threat, an attacker can take over a victim's account, and perform actions on this user's behalf without permission.

Threat actor

The threat actor could be an external attacker or a user of this web application, targeting one specific user.

Threat remediation

Remediations for this threat would be to:

1. Require users to set complex password.
2. The website can introduce a lockout mechanism (i.e. lockout one account after 5 times wrong password input).

Threat 2: Attacker authenticates as developer

Threat identified

For the developer login functionality, its function for verifying is saved in the client side of this web application. An attacker can figure out the mechanism and successfully pretend to be a developer. With it, an attacker may destroy this web application.

Threat actor

The threat actor could be an attacker who is an authenticated user

Threat remediation

Remediations for this threat would be to:

1. Remove the developer login function in the client side. It is not necessary to have this functionality.
2. Let the server to verify whether a user is a developer, instead of verifying on the client side.

Threat 3: Attacker pretends to be admin

Threat identified

In this website, some pages and functions can only be accessed by administrators, but an attacker can pretend to be an admin and can successfully access such sensitive content.

Threat actor

The threat actor could be an attacker who is an authenticated user.

Threat remediation

Remediations for this threat would be to:

1. Remove the admin page in the client side. It is not necessary to have this functionality.
2. Let the server to verify whether a user is an admin by his username or id, instead of through a request sent by a user.

T: Tampering

Threat 1: Attacker change other users' password

Threat identified

When using change password functionality, an attacker can pretend to be another legitimate user and change this user's password. This will lead to the attacker take over other user's account, and then perform actions on this user's behalf without any permission.

Threat actor

The threat actor could be an attacker who is an authenticated user of this web application, targeting one specific user, because in this threat, the attacker needs to know username of the victim.

Threat remediation

Remediations for this threat would be to:

1. Ensure that users do not disclose their usernames to others.
2. For the website design, make sure that every parameter (old password, new password, username) is not null in a request, and only when both old password and username are correct, this functionality can be processed.

Threat 2: Attacker change a user's role saved in the system

Threat identified

On the website, there are different roles, such as branch manager, admin, and general users. There is a function which can change a user's role, which should only be accessed by administrators, but an attacker may apply some strategy to use it.

Threat actor

The threat actor could be an external attacker, bank client, internal employee.

Threat remediation

1. Remove this part of functionalities in the client side. Move it into a separate admin application for admin users.

R: Repudiation

Threat 1: Attacker deny his own transaction action

Threat identified

When an attacker has transacted money to other account, but he denied his action and asked for a refund. Due to there is no detailed record of this attacker's action on the server. It is hard to verify that.

Threat actor

bank client, internal employee.

Threat remediation

1. Add extra authentication process for transaction actions, such as digital signatures.

Threat 2: Attacker denies that he takes actions on behalf of other users

Threat identified

Due to many factors, such as password leakage or brute force method, an attacker has taken over another user's account, and takes actions on behalf of this user. But there is no evidence that these actions are taken by the attacker instead of the real user.

Threat actor

External attacker.

Threat remediation

1. Add extra authentication process when taking sensitive actions.
2. Record IP address, cookies, browser ID to record where an action request is from.

I: Information Disclosure

Threat 1: Sensitive information over HTTP

Threat identified

The message sent and received on this website are all through HTTP, and these messages from many functionalities will contain sensitive information. For example, the change password function will pass username and password through HTTP, and this can lead to many issues, such as account take over.

Threat actor

External attackers, or internal employee. Those people who may use same local network as the victim or bank employees.

Threat remediation

1. Ensure HTTPS is enabled and enforced using HSTS.
2. Use a fully switched network.
3. Encrypt messages.

Threat 2: User's profile can be viewed by other users

Threat identified

There is user profile page. In this page, it will show this user's information, which may include account, name, or phone number. If this can be viewed by other people, it can cause information disclosure.

Threat actor

External attacker, bank client, or internal employee.

Threat remediation

1. Add extra authentication process when viewing user profile.

Threat 3: Sensitive information left in Client-side code

Threat identified

The code of some sensitive functionalities can be viewed on the client-side browser. This kind of information can help an attacker to take over the system.

Threat actor

External attacker, bank client.

Threat remediation

1. Make sure every developer is familiar with the whole system and know what kind of information must not be left.
2. Try to let the server handle a case, instead of on a local browser.

D: Denial of Service

Threat 1: Lack of rate limiting on the login page

Threat identified

There is no rate limiting mechanism implemented on both the general login page and developer login page. Because login function usually needs to query a database and cost more time, no limited login request will cause the denial of service on the website.

Threat actor

External attackers, or bank client.

Threat remediation

1. Introduce an IP address lockout mechanism, such as after 5 times wrong input, lockout this IP address for a period.

Threat 2: Lack of rate limiting for User Profile page request

Threat identified

User profile page shows details of a user, and these data need to enquiry the database on the server. An attacker can keep requesting this page and lead to a denial of service.

Threat actor

Bank clients.

Threat remediation

1. Use cache mechanism. If this user's profile has not been changed since last request, it will show the information saved in local browser.

E: Elevation of Privilege

Threat 1: Attacker promote his account as administrator

Threat identified

An attacker can use promote function, which can be found in the client side of this application. As a result, this attacker will have right to view sensitive pages and information, which should not be accessed by general users.

Threat actor

The threat actor could be an attacker who is an authenticated user of this web application, because only authenticated user can try to access the admin page.

Threat remediation

Remediations for this threat would be to:

1. Remove the admin function from the client side, develop a separate web application for administrators.
2. Make sure only the server can verify a user's role by this user's id or username, instead of told by a user himself in a request sent to the server.

Threat 2: Attacker promote his account as branch manager

Threat identified

In this web application, a branch manager can communicate with their clients, see their accounts, and freeze them. An attacker may break into the system and promote himself as a branch manager, which will cause damage to those users who are assigned as clients to this attacker's account.

Threat actor

External attacker, internal employee, or bank client

Threat remediation

1. When an account is created, the role should be unchangeable, so that no general accounts can be promoted.
2. Develop a different application for branch manager, and this application should not be public, so that even an attacker has a branch manager account, he still cannot perform a manager's action.