Subject: Security Testing

SENG 8061

Final Project

Threat Modeling

SUBMITTED TO
PR. PREETHI ARATTU

Name	Student ID
Shivani Shaileshkumar Varu	8941914

Executive Summary Report

Recently, SQA Workout Inc. completed an in-depth security assessment of its web application, which is essential for ensuring the safety of customers' confidential information while maintaining the integrity of our online services. The assessment has found several security vulnerabilities that can be used to get private information or tamper with data.

The assessment's most important findings include high-risk vulnerabilities like SQL Injection and Directory Listing. These vulnerabilities could allow third parties to obtain private information without authorization, compromising user privacy as well as the security of the operations of a company.

As a result of these results, we created a number of mitigation solutions that improved the security of the web-based application. These include restricting the way we manage user data input, disabling unused features that could provide attackers information, and increasing our monitoring systems to faster detect and address suspicious activity. Other identified vulnerabilities, while presenting a medium level of risk, will also be addressed with appropriate security measures. This includes improving error messages to prevent giving away technical details and removing any non-essential scripts or applications that could be used as entry points for attacks.

In conclusion, the identified security issues must be addressed immediately and effectively. SQA Workout Inc. can maintain its reputation as a trustworthy service provider and guarantee a secure atmosphere for customers by implementing the recommendations for security measures into action. Our security measures will be regularly updated and monitored to keep up with the latest threats and maintain the highest standards of web application security.

Technical Report

1) Directory Listing

Vulnerability Description:

The Directory Listing vulnerability in SQA Workout Inc.'s online application is a major security vulnerability. It makes it possible for attackers to see a complete index of every resource within a directory. It can leak important files that should be kept hidden, such as data files, backup source code, or in-development apps. SQA Workout Inc. and its users may be badly affected by this vulnerability.
Attackers can be able to gain private data without authorization if this vulnerability is exploited, which can end up in data breaches, a compromise of private information, and damage to the company's reputation. An attacker can take advantage of this issue by scanning the web application server for directories that have Directory Listing enabled. After that, they could look through the directory index to find sensitive files. Attackers can use this information to launch more attacks, like SQL injection, unauthorized access, or data extraction once these files have been located. This vulnerability damages systems, allows attackers several ways to obtain personal data, and allows them to use directory listings to locate other vulnerabilities that might be exploited for theft.

DREAD Analysis

- Damage Potential (8/10): If exploited, this vulnerability could lead to unauthorized access to sensitive data, including user health and workout data, and proprietary company information. This could severely damage the company's reputation and user trust.
- Reproducibility (9/10): This vulnerability could be easily reproduced if Directory Listing is enabled on the server. Tools and techniques for exploiting Directory Listing vulnerabilities are well-documented and readily available.
- Exploitability (7/10): Exploiting this vulnerability requires some technical skill to navigate the server's directory structure and identify sensitive files. However, information on how to exploit Directory Listing vulnerabilities is widely available.
- Affected Users (9/10): The application's users, including regular customers and personal fitness trainers, may be affected by potential content and video issues.
- Discoverability (8/10): The vulnerability could be discovered through automated scanning tools or manual inspection of the web application's response to certain requests.

DREAD rating=5(D+R+E+A+D)=5(8+9+7+9+8)=8.2, Risk: High

Mitigation and Suggestions:

- The most straightforward way to mitigate this vulnerability is to disable Directory Listing on the server. This can usually be done through the server's configuration files.
- Place an index file (index.html) in each directory to prevent the server from listing the directory's contents when a user navigates to it.
- Use access controls to restrict who can view certain directories. This could involve requiring authentication or checking the user's permissions before serving content.

- A robots.txt file can be used to instruct web robots not to crawl specific directories, although this method is not foolproof.

2) SQL Injection

Vulnerability Description:

SQL injection is a vulnerability that allows attackers to modify SQL queries in web applications, possibly impacting factors including URL parameters, POST data, and cookie values. The attacker could get unauthorized access to personal information, therefore causing user confidentiality violations, financial loss, and reputational damage, as well as interrupting the service. An attacker can take use of this vulnerability by executing malicious SQL queries and injecting them into user input fields, perhaps circumventing login processes or utilizing search boxes to retrieve sensitive data. The vulnerability allows an attacker to obtain sensitive customer data, access network systems, interrupt services, and possibly damage the company.

DREAD Analysis:

- Potential Damage (9/10): There is a significant risk of damage because there is a chance that private user information may be taken, and the service may be interrupted.
- Reproducibility (8/10): SQL Injection attacks are rather simple to execute because they are well-documented and freely available tools make them accessible.
- Exploitability (7/10): Although technical knowledge is required, information on SQL Injection attacks is publicly available.
- Affected Users (8/10): All users of the application could potentially be affected, both regular customers and personal trainers.
- Discoverability (6/10): The vulnerability might not be immediately obvious but could be discovered by those specifically looking for such weaknesses.

DREAD rating=5(D+R+E+A+D)=5(9+8+7+8+6)=7.6 Risk : High

Mitigation and Suggestions:

- Use prepared statements to ensure safe handling of user-supplied input in SQL statements.
- Implement strict validation on user inputs and parameters to ensure conformity to expected format.
- Limit privileges on database accounts used by web applications to limit potential SQL Injection attack damage.
- Implement a Web Application Firewall to filter out SQL Injection attempts and common exploits.
- Detect signs of a breach and alert personnel when anomalous activity is detected.

3) Possible Server Path Disclosure

Vulnerability Description:

A potential vulnerability has been identified in SQA Workout Inc.'s web application due to the presence of a fully qualified path name to the system's root. This typically occurs when the application generates an error. Fully qualified server path names can provide an attacker with knowledge of the web server's file system structure, which is a prerequisite for many other types of attacks. This vulnerability could

have a significant impact on SQA Workout Inc. and its users. If an exploited attacker could gain knowledge of the file system structure, they could potentially access sensitive files or data. A web application vulnerability can provide an attacker access to user data and allow them to obtain confidential information. The server path disclosure exposes server file system structure, backup source code, and under-developed apps, potentially identifying system vulnerabilities.

DREAD Analysis:

- Damage Potential (7/10): If exploited, this vulnerability could lead to unauthorized access to sensitive data, including user health and workout data, and proprietary company information.
- Reproducibility (8/10): This vulnerability could be easily reproduced if Directory Listing is enabled on the server.
- Exploitability (3/10): Exploiting this vulnerability requires some technical skill to navigate the server's directory structure and identify sensitive files.
- Affected Users (0/10): This vulnerability does not currently affect any users.
- Discoverability (2/10): The vulnerability could be discovered through automated scanning tools or manual inspection of the web application's response to certain requests.

DREAD rating=5(D+R+E+A+D)=5(7+8+3+0+2)=4 Risk : Medium

Mitigation and Suggestions:

- Adopt a standard error handling approach that prevents the display of fully qualified path names.
- Make sure error messages don't unintentionally release too much information or be inconsistent, as this can be a security risk.
- Use generic error pages and error-handling algorithms to suggest customers of possible issues without exposing sensitive information.

4) Test Application Found on Server

Vulnerability Description:

A test script was discovered on SQA Workout Inc.'s web application server, posing a security risk. The script includes secret source code, usernames, passwords, and fixed authentication session IDs, among other sensitive data. It is a risky technique because attackers could exploit this data to get to the website's security or retrieve other private information. There could be significant consequences for SQA Workout Inc. from this vulnerability. An attacker may be able to obtain sensitive information if they manage to get their hands on the test script. It can result in loss of confidential resources, illegal access to user data, and damage to the company's reputation.

DREAD Analysis:

- Damage Potential (4/10): If exploited, this vulnerability could lead to unauthorized access to sensitive data, including user health and workout data, and proprietary company information.
- Reproducibility (3/10): This vulnerability could be easily reproduced if the test script is accessible on the server.
- Exploitability (2/10): To find the test script and navigate the server's directory structure, exploiting this vulnerability requires a certain level of technical expertise.

- Affected Users (0/10): This vulnerability does not currently affect any users.
- Discoverability (0/10): The vulnerability could be discovered through manual inspection of the web application's response to certain requests.

DREAD rating=5(D+R+E+A+D) =5(4+3+2+0+0) =1.8 Risk : Low

Mitigation and Suggestions:

- The test application should be removed from the server. Developers and administrators should be informed to remove test applications from servers when they are no longer needed.
- While the test applications are in use, be sure to protect them using HTTP basic authentication.
- Contact your security or network operations team and request they investigate the issue.

5) Cross Side Scripting

Vulnerability Description:

Customers or fitness trainers can be able to view websites that contain malicious code because of the XSS vulnerability. It can result in unwanted access to sensitive user information, including financial details, schedules of exercise, and health tracking data. Additionally, it might enable an attacker to pretend to be customers or fitness trainers, disrupting the application's functionality and damaging the company's reputation. The vulnerability makes it possible for sensitive data to be easily accessed, app services to be interrupted, and the company's reputation to be damaged. Additionally, it offers chances for delay, impersonation, and malware to infect users' devices.

Assessing the vulnerability using DREAD:

- Damage Potential (9/10): The potential damage is high. If an attacker successfully exploits this vulnerability, they could steal sensitive customer data, impersonate customer or trainers, disrupt the app's services, or spread malware to users' devices.
- Reproducibility (7/10): XSS attacks are well-documented, and tools are readily available, making them relatively easy to reproduce.
- Exploitability (1/10): While some technical skill is required to exploit XSS vulnerabilities, information on how to perform such attacks is widely available.
- Affected Users (5/10): All users of the application could potentially be affected, both regular customers and personal trainers.
- Discoverability (0/10): The vulnerability might not be immediately obvious but could be discovered by those specifically looking for such weaknesses.

DREAD rating=5(D+R+E+A+D) =5(9+7+1+5+0) =4.4 Risk: Medium

Mitigations and suggestions to fix this vulnerability:

- Implement secure programming practices to ensure effective filtering of user-supplied data.
- Encode all user-supplied data before it is sent to the client to prevent scripts from being delivered to end users in an executable format.

- Identify and address any vulnerabilities through frequent security audits and penetration tests.
- Reduce the impact of potential XSS vulnerabilities by putting in place a Content Security Policy (CSP).

6) Database Server Error Message

This vulnerability occurs in the web application displays critical database server error messages that suggest an unhandled exception was triggered in the code. When user input is received by an application that it was not prepared for and is unable to handle, an unhandled exception occurs. Web applications with vulnerabilities that could provide attackers access to private user information without authorization can be found through error messages. This could include workout routines, health tracking information, and payment information. Additionally, it could disrupt app services and damage the company's reputation. The vulnerability allows an attacker to obtain unauthorized access to the database, steal data, interrupt activities, or perform other malicious activities by bypassing the app's security and gaining access to sensitive data while disrupting the apps.

Assessing the vulnerability using DREAD:

- Damage Potential (7/10): If exploited, this vulnerability could lead to unauthorized database access, compromising sensitive user data and potentially leading to service disruption.
- Reproducibility (5/10): Can be replicated with certain conditions.
- Exploitability (3/10): Requires technical understanding of web application's internal workings.
- Affected Users (7/10): A successful exploit could impact both regular customers and personal fitness trainers, potentially affecting all users of the application.
- Discoverability (0/10): This vulnerability may not be easily discoverable without deliberate probing and testing for unhandled exceptions.

DREAD rating=5D+R+E+A+D=57+5+3+7+0=4.4 Risk: Medium

Mitigations and suggestions:

- Implement robust error-handling methods that manage unexpected user input without revealing sensitive information.
- Specify acceptable data types and input ranges to prevent invalid data from triggering exceptions.
- Use proper input validation to minimize user errors and potential attack vectors.