TEAM Squad NOC Proof-Of-Concept Document

1. SQL Injection (SQLi)

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| The fields in the login page might be exploitable by  SQLi | SQLi is a common attack vector that makes use of malicious SQL codes for backend database manipulation, accessing information not intended to be available for unauthorised users. | Severity - Critical | * Attackers being able to gain access to a user account. (Confidentiality impact) * Attackers being able to access confidential / sensitive data they should not have access to. (Integrity Impact) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: Make use of special characters, such as “ ‘ “, to find out if a field is exploitable. If it is exploitable, able to make use of SQL codes such as, “**‘ OR 1=1 --** ”, to gain access to an account.

Post-Exploitation Activity: If the query gets through to the web application server, attackers would be able to gain access to a user account, and exploit it in many different ways such as accessing and stealing confidential data they should not be able to access.

Consequences: Attackers can obtain sensitive data by logging into an user account with the SQL code and carry out further reconnaissance on the web application that could be detrimental to the web application.

Prepared by: Agreed by:

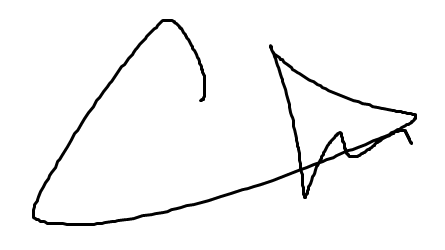
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

2. Broken Authentication

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| Cookies can be viewed in the application tab in the Chrome Browser  There is a cookies can also be obtained with a “document.cookie” command in the console | Cookies can be stolen by attackers and hence exploited by impersonating other online users | Severity - Critical | * Confidentiality and Integrity of user account tied to cookie can be affected (Confidentiality Impact, Integrity Impact) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: Make use of the stolen user cookie and use it as the cookie value for the web application the attacker is on. Thus, allowing for attackers to gain access to the victim’s authorised session.

Post-Exploitation Activity: Attackers will be able to gain access to the session that the victim has signed into, thus, accessing all the information that the victim’s account can access on the web application.

Consequences: Attackers can use the cookie to steal any information relating to the user that has the cookie tied to the user account. Attackers can also make use of the cookie to be able to gain access to an authorised session.

Prepared by: Agreed by:

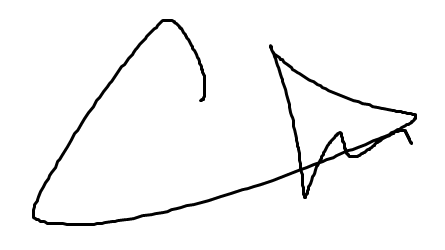
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

3. Broken Access Control

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| User is able to access / carry out actions that they do not have access to | Users are able to view, modify and delete different values, while also able to access information they do not have access to | Severity - Critical | * Confidential files/entries can be viewed, modified or deleted without authorization (Confidentiality Impact, Integrity Impact, Availability Impact) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: Attacker can modify the URL by replacing the ID section of the URL with the ID of the entry; Attacker can view admin-only pages

Post-Exploitation Activity: Attacker will be able to view, modify and delete user entries.

Consequences: Attacker can Modify the URL to cause entries integrity issues as the attacker is allowed to edit or delete the entry. The Attacker can also take this chance to view entries and administrative pages, allowing the possibility to identify sensitive information.

Prepared by: Agreed by:

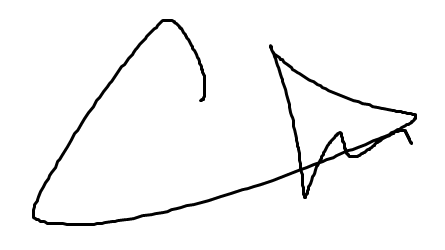
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

4. Security Misconfiguration

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| Certain controls can be inaccurately configured, hence, left insecure | This misconfiguration could be exploited by attackers by leaving settings to its default configurations, thus, allowing for the unauthorised access of data to the attackers. | Severity - Medium | * Confidential information can be revealed. (Confidentiality impacts) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: One attack that attackers can carry out is adding a different file path behind the URL of the web application.

Post-Exploitation Activity: Attackers might be able to access confidential information that is contained inside the web application that should not be accessible by them.

Consequences: Confidentiality of data will be impacted. Additionally, If the file extensions appended behind the URL reveals any sensitive security vulnerability information, the whole web application can be compromised as attackers can identify vulnerable points to attack. Personal identifiable Information (PII) can also be lost if stored in these files that are exposed to the public.

Prepared by: Agreed by:

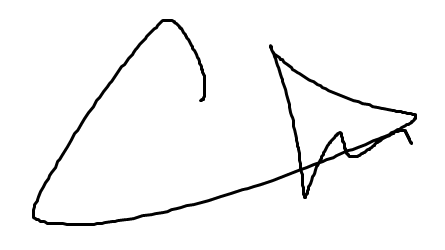
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

5. Cross-Site Scripting (XSS)

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| Client-side scripts can be injected into the web application by the attackers through entry points | XSS can be classified into 3 categories, stored XSS, reflected XSS, and DOM-based XSS  Stored XSS stores the injected scripts in the database and can allow attackers to exploit it such that users using the same webpage will view the same script injected by the attacker.  Reflected XSS does not store the script in the database and just reflects it once the script is injected in the entry points.  DOM-based XSS does not store the attack payload on the website but the code in the client side will be executed differently | Severity - High | * Cookies values of different user accounts can be stolen by the attackers. (Confidentiality impact) * Website can be defaced (Availability impact) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: Attackers can do a simple alert script on one webpage of the web application that could pop-up the cookie value of a current authenticated user.

Post-Exploitation Activity: Attackers can make use of the cookie value to log in to a user account and gain unauthorised access to confidential information. Attackers can deface the website also and make it no longer usable for users.

Consequences: Confidentiality of data can be affected as attackers gain access to data they should not have access to. Availability of the webpage can also be affected.

Prepared by: Agreed by:

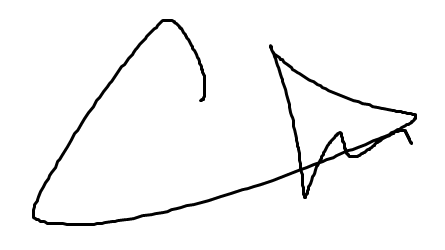
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

6. Using Components with Known Vulnerability

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| Some technology used has versions exposed and some of these versions has some exploits available online | Some vulnerable components can be identified and exploited with automated tools | Severity - High | * The website can be brought down (Availability Impact) * Information stored in the database can be leaked (Confidentiality Impact) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: Attackers can use third party applications to find out what technology the website is using. After gaining all that information, the attacker can find ways to attack using vulnerabilities in that technology.

Post-Exploitation Activity: Attacker may be able to make use of the different exploits available for the different technology used by the website and possibly gain remote access by creating a remote shell session.

Consequences: Web applications can be exploited as information about known vulnerabilities in the technology are open to the public. If left unattended, attackers can make use of these known vulnerabilities to attack the web application, causing the web application to lose its functionality.

Prepared by: Agreed by:

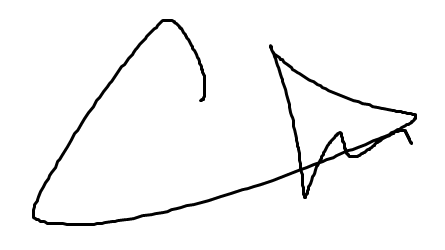
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

7. Insufficient Logging/Monitoring

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| Some Key information is missing and is not logged in the Log Activity Report | Insufficient logging and monitoring is missing security critical information logs that helps detect malicious incidents or breaches | Severity - Low | * Unable to keep track of who did what action (Integrity Impact) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: No logon success or failures recorded when users are trying to log in. Public Ip address of each attempt made is also not captured.

Post-Exploitation Activity: Attackers can keep trying to log in to the website without being locked out or blocked by the firewall as long as they do not send too many requests in a short amount of time.

Consequences: Admins won't be able to know which account the attacker tried to brute force into the website and would not be able to selectively block them from gaining access.

Prepared by: Agreed by:

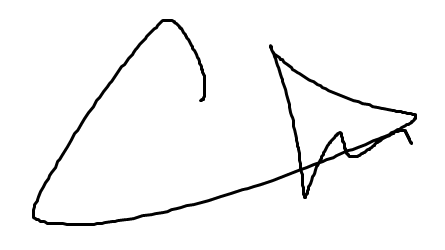
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

8. Sensitive Data Exposure

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| Man-in-the-middle attack can be executed, where data can be read and obtained while in transit | This attack steals clear text data off the server, while in transit or from the user’s client | Severity - Critical | * Data sent to the web application server can be exposed and seen in clear text (Confidentiality impact) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: When a victim makes a HTTPS request to a website, the attacker converts the https request into an http request and the connection between the victim and the website is no longer secure and encrypted

Post-Exploitation Activity: Data sent between victim and website can be seen in clear text

Consequences: Data can be eavesdropped and confidential data can be lost.

Prepared by: Agreed by:

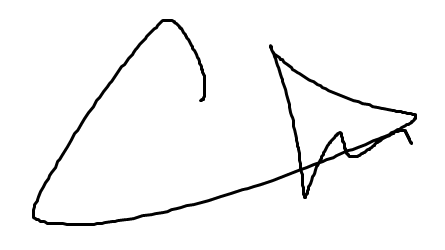
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

9. File Upload Function

| Vulnerability Found | Descriptions | Severity Level | Possible Impacts |
| --- | --- | --- | --- |
| There are many file extension types and if not filtered properly, can result in viruses being uploaded.  There is also no limit on how big a file can be and thus can result in buffer overflow attacks | This attack occurs due to the types of file that is uploaded to the web application.. | Severity - Medium | * Expose sensitive information (Confidentiality Impact) * Crash the web application (Availability Impact) |

**Proposed Exploitation and Post-Exploitation Activity & Consequences**

Exploitation: Attackers can use this function to upload viruses or even file with sizes way too large such that the web application is unable to take on the load.

Post-Exploitation Activity: Attackers have then been able to successfully inject a file that the web server could possibly not be able to handle. Thus, crashing the website and resulting in the website being unavailable to its intended users.

Consequences: Web application could be then infected by the virus or occupied with processing the large file.

Prepared by: Agreed by:

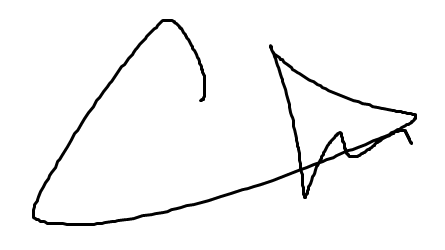
Edward Neo



21/01/2022 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date

Clarence Ow



21/01/2022

Mabel Choi



21/01/2022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature/Name/Date