**CYB 240 Project Two**

Douglas Few

Southern New Hampshire University

February 18, 2022

**Vulnerability One**

One of the vulnerabilities identified during security testing was broken access control. Access control is the process of preventing users from having any privileges other than those that they need in order to perform their job duties (OWASP, *A01:2021 – Broken Access Control* 2022). Associate this with the principle of least privilege, which states that no user should have any privileges other than those that are absolutely necessary (CISA, 2022). Access control becomes broken when the principle of least privilege is not followed. Access control can also be broken when users are permitted to view or make changes to the accounts of other users, or by elevation of privilege that allows a standard user to perform the actions of an administrator.

Overloading users with privileges creates an area of concern when dealing with patient medical records because it allows users who should otherwise not be able to view those records to do so. This is an issue because if those users have access to making changes to information on the database, they could potentially alter the data so that it will no longer be accurate. This will cause inaccuracies during later doctor visits, which could lead to legal issues down the line. Too much access could also allow users to edit payment details on the transaction server, causing discrepancies relating to client payments. This, too, could lead to legal issues if a client ends up overpaying due to a discrepancy.

In order to prevent the risk of broken access control, I would recommend following the recommendations laid out in OWASP proactive control C7: Enforce Access Controls (OWASP, *C7: Enforce access controls* 2022). Specifically, all access requests should go through checks that verify that the access is truly needed by the requesting user. If the access is not strictly necessary for the user to be able to complete their job, then the request should be denied. These steps should be taken in order to adhere to the principle of least privilege. Finally, all access events should be logged so that every attempted login can be audited and examined. This will allow the security team to potentially identify a malicious user if an unauthorized access attempt is detected.

**Vulnerability Two**

Another risk identified was broken authentication, now known by OWASP as Identification and Authentication Failure (OWASP, *A07:2021 – identification and authentication failures* 2022). This failure occurs when there is a weak method, or no method at all, of verifying the user’s identity when they sign in to an account. Oftentimes, this is caused by the lack of security measures that mandate passwords of a certain strength or the use of multi-factor authentication. It can also occur when a website leaves the session identifier exposed, either by showing it in the website URL or by reusing the same identifier after a successful login.

Due to the sensitive information being stored on the transaction server and SQL database, being able to verify that a person accessing that information is a legitimate user is imperative. While proper authentication is required to access the database, no such requirement seems to have been made for the transaction server. This means that patient payment information and/or insurance information can be made easily available to unauthorized individuals.

In order to protect users against the risks of failed identification and authentication, the recommendations outlined in OWASP proactive control C6: Implement Digital Identity should be followed (OWASP, *C6: Implement Digital Identity* 2022). By requiring strong passwords that meet certain criteria, we can make it much more difficult for an attacker to brute force their way into a user’s account. Passwords should be a minimum of 8 characters and should contain a mixture of capital and lowercase letters, numbers and special characters (#, %, &, @). Coupled with the password requirements, users should use a form of multi-factor authentication that allows for every login attempt to be verified. An authentication request will either be sent to the user’s email or texted to them, and this will allow us to be confident that each login request is legitimate.

Along with these requirements, password storage on our end should be more secure. That is to say that user passwords stored in the database should be encrypted so that they cannot be displayed in plaintext. By hashing user passwords in the database, even if an attacker were to gain access to the database, they would not be able to decipher user credentials due to the aforementioned encryption.

**Value of a Security Practitioner**

During the software development life cycle, a security practitioner equipped with knowledge of the fundamental security design principles is better able to identify issues and vulnerabilities that could disrupt the flow of (or even end) an organization. Being unable to identify security issues could lead to injection attacks and denial of service attacks that a knowledgeable practitioner would know how to avoid. By taking steps preemptively, an organization can focus on warding off threats rather than combating attacks that have already been made.

References

CISA. (2022). *Least privilege*. CISA. Retrieved January 28, 2022, from https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege

OWASP. (2022). *A01:2021 – Broken Access Control*. A01 Broken Access Control - OWASP Top 10:2021. Retrieved January 28, 2022, from https://owasp.org/Top10/A01\_2021-Broken\_Access\_Control/

OWASP. (2022). *A07:2021 – identification and authentication failures*. A07 Identification and Authentication Failures - OWASP Top 10:2021. Retrieved January 28, 2022, from https://owasp.org/Top10/A07\_2021-Identification\_and\_Authentication\_Failures/

OWASP. (2022). *C6: Implement Digital Identity*. OWASP Top Ten Proactive Controls 2018 | C6: Implement Digital Identity | OWASP Foundation. Retrieved January 28, 2022, from https://owasp.org/www-project-proactive-controls/v3/en/c6-digital-identity

OWASP. (2022). *C7: Enforce access controls*. OWASP Top Ten Proactive Controls 2018 | C7: Enforce Access Controls | OWASP Foundation. Retrieved January 28, 2022, from https://owasp.org/www-project-proactive-controls/v3/en/c7-enforce-access-controls