Exercise 3 - Define Different Web Application Software Vulnerabilities

A Cyber Security Analyst needs to be familiar with different types of software vulnerabilities and be able to rectify these vulnerabilities to mitigate a cyber security attack.

In this exercise, the different types of software vulnerabilities will be discussed.

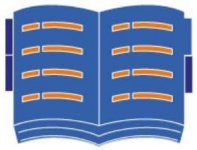
Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Web Application Software Vulnerabilities

Your Devices

This exercise contains supporting materials for CySA+.



Improper Error Handling

Web applications generate error conditions during normal operation.

These errors may include the following:

- Out of memory
- Database unavailable
- Network timeout
- Null pointer exceptions

When a web application handles these generated errors incorrectly, it may lead to several security risks for the web site. These security risks include that the website will reveal sensitive information to the malicious, which may result in the exploitation of the website.

Dereferencing

Dereferencing refers to the code in an application that dereferences a null pointer and thereby raising a NullPointerException. A Null Pointer Error normally results from the programming code being violated and which can result in general instability of the program.

If a malicious user intentionally triggers a null pointer dereference, it may result that the application reveals debugging information of the application, which can be useful in the subsequent attacks and exploits.

Insecure Object Reference

This type of software vulnerability refers to when a user's credentials are not validated, and the user is given direct access to the requested resource without authentication. The main reason for this type of software vulnerability to be exploited is as the user's session is not encrypted, it may be intercepted by a cyberattacker. These types of exploits can be circumvented by the use of hash values.

Race Condition

A Race condition vulnerability in a software application exists when a certain criterion needs to be met before an operation can be executed. A window of vulnerability exists while the application waits for the criteria that needs to be met, or the assumption of the criteria is not met. This may result in unexpected behavior.

Broken Authentication

A software vulnerability where an application's functions related to authentication and session management are implemented incorrectly. This may lead to a cyber attacker compromising passwords, keys, and session tokens. These vulnerabilities can then be used to impersonate the captured user data for the exploit.

Sensitive Data Exposure

Several web applications and Application Programming Interfaces (API) don't protect sensitive data, which, if the web application is compromised, may lead to exposure of this. For example, credit card details of Personal Identifiable Information (PPI). To prevent this vulnerability from being exploited, sensitive data needs to be encrypted in rest and in transit.

Insecure Components

Components of a web application need to be configured securely to prevent exploitation. Insecurely configured components may include open cloud storage components and misconfigured HTTP headers. Securing these components may include patching/upgrading software and ensuring the operating system is up to date with updates.

Insufficient Logging and Monitoring

If there is insufficient logging and monitoring of a web application, it may lead to the exploitation as there will be no way that the Cyber Security Analyst will be able to view actions that have been performed, meaning data breaches will only be detected after they have occurred. Logging and monitoring is essential to ensure that the application is secure and not being accessed by unauthorized users.

Weak or Default Configurations

When a web application is installed, it is normally configured with default settings. This includes default administrator passwords, or being configured to use default ports. If these default settings are not changed when the application is configured, it may result that the application will be compromised by an attacker that has in-depth knowledge of these default configurations.

Use of Insecure Function: strcpy

If the insecure function strcpy is used in a specific code, it may lead to the exploit in the specific application. The reason is the strcpy is an insecure function that may cause a buffer overflow attack on the specific web application.