Phase 5: Fix the Mobile Application XSS Security Vulnerability in Application

Yingwei Liu

Liberty University

Abstract

This article emphasizes the correction of the SQLi vulnerabilities that provided in Phase 3. This article will provide the vulnerabilities that we discovered in the phase 3. Then, I will try to fix the code of the vulnerable code and re-run the testing steps. Also, evidence of the final fuzzing activity and lack of vulnerabilities found. After fixed all the vulnerabilities, I will try to discuss the process of this vulnerability’s correction.

Keywords: SQLi, vulnerabilities, correction.

Phase 5: Fix the Mobile Application XSS Security Vulnerability in Application

This article will present the code snippets of before and after vulnerable code sections in the top of the report. 2. Evidence of the final fuzzing activity and lack of vulnerabilities found. 3. A discussion of the SQLi class of vulnerability and a recommendation of how to fix that vulnerability, across all code, efficiently and effectively.

# Vulnerable Code

This section will present the Vulnerable code of the Mobile App.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

### Fix the errors.

This section focuses on the correction of the errors that has been detected in the Mobile App. First vulnerabilities of Android Phone are unsecured Wi-Fi connections and unauthorized certificate.

So, the certificate authority is an important act that validates the identities of entities. According to the windows, “A certification authority (CA) is responsible for attesting to the identity of users, computers, and organizations. The CA authenticates an entity and vouches for that identity by issuing a digitally signed certificate. The CA can also manage, revoke, and renew certificates.” (2016) In order for the Android to build connection with burp suit, it requires to generate a certificate authority. The SQLi vulnerabilities is exists in the android application during the account login period.

Text

Description automatically generated

The sqli can result data leak from the system database. Especially, the android application involves a lot of important information of the user. If the source code from the login page of the application does not provide valid authentication, it can easily make the attacker take another users login information and login into the database. Just like Android Developers Guides, “One of the main principles of SQL databases is the schema: a formal declaration of how the database is organized. The schema is reflected in the SQL statements that you use to create your database. You may find it helpful to create a companion class, known as a contract class, which explicitly specifies the layout of your schema in a systematic and self-documenting way.” (Android)Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

It is very crucial for developers to consider the SQL injection attack for the App application. First, it requires to prevent invalid source code. Second, the authentication of the user information is fundamental steps in this process. Just like the John 3:16 states, “For God so loved the world, that he gave his only begotten Son, that whosoever believeth in him should not perish, but have everlasting life.” (Bible) In addition, this article presented the code snippets of before and after vulnerable code sections in the top of the report. Evidence of the final fuzzing activity and lack of vulnerabilities found. A discussion of the SQLi class of vulnerability and a recommendation of how to fix that vulnerability, across all code, efficiently and effectively.

References

Microsoft (2016). Certification Authority. Retrieved from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831574(v=ws.11)

Android Developer. Save data using SQLite. Retrieved from https://developer.android.com/training/data-storage/sqlite#DbHelper

Bible. John 3:16. Retrieved from https://www.kingjamesbibleonline.org/Bible-Verses-About-Security/.