**Phase 3 – Identify Vulnerability in Mobile App (USING API)**

**Yingwei Liu**

**Liberty University**

Abstract

This article will need to perform the vulnerability scanners testing manually. I will use the other modules of burp, besides scanner. Using a mobile debug proxy and burp suite, fuzz the API interface and discover 3 SQLi vulnerabilities. In this article, I will be presented 1. Testing setup and configuration. 2. Evidence of the fuzzing activity and vulnerabilities found. 3. A discussion of each vulnerability, explanation of how it is triggered, in the context of the application, and the implications of that vulnerability.

Keywords: API, Vulnerability

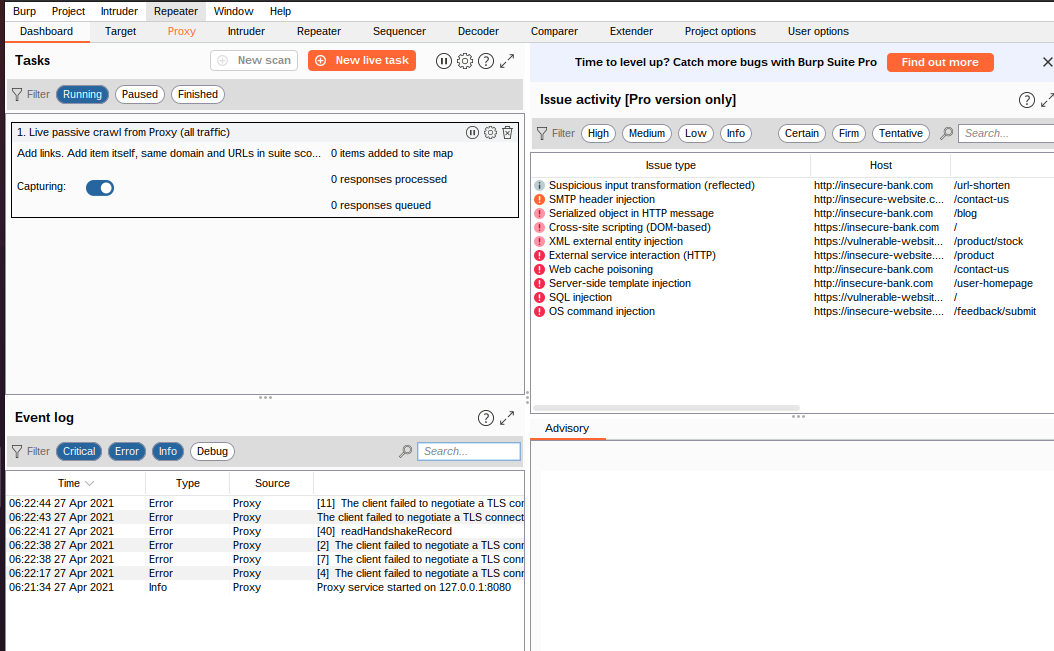
Identify Vulnerability in Mobile App

In this article, I will be presented 1. Testing setup and configuration. 2. Evidence of the fuzzing activity and vulnerabilities found. 3. A discussion of each vulnerability, explanation of how it is triggered, in the context of the application, and the implications of that vulnerability.

# Testing Setup and Configuration

When people design or building a mobile app, it may result several situations call for the developers to monitor the API. Especially, when the developer wants to identify the app’s performance and vulnerabilities. In this testing session, I will apply the Burp Suits as the vulnerability scan software that allows me to monitor the app’s API and received the user’s request. In order to use the Burp Suit for API monitoring, I will need a computer system that download burp suit and a Mobile device.

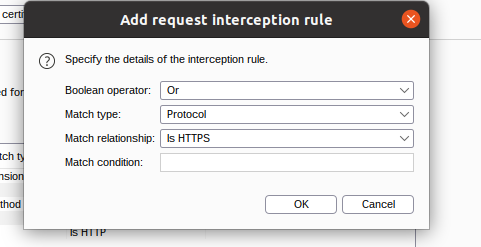
Configuring Burp Suit



## Add HTTP protocol

## 

Add HTTPS

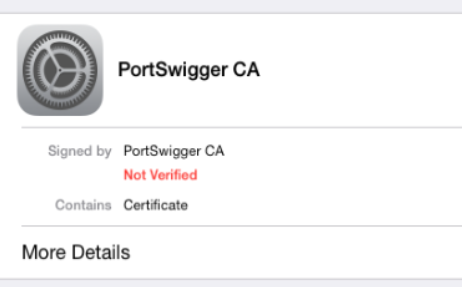


## Installing certificate in the iOS device

## In your iOS device, go to the “Settings” menu.

1. **Tap the “Wi-Fi” option from the "Settings" menu.**

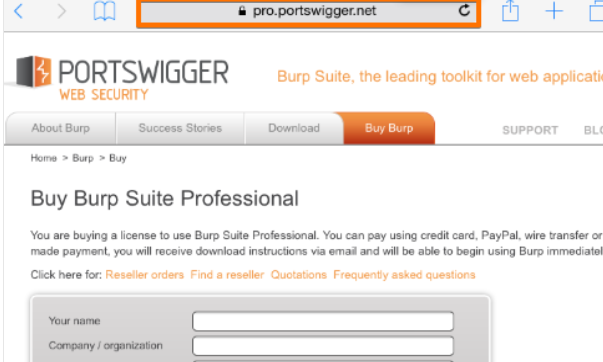
**If your device is not already connected to the wireless network you are using, then switch the "Wi-Fi" button on, find your network in the list, and tap it to connect. Enter your network password if prompted.**



On some versions of iOS you may need to go to "Enable Full Trust for the PortSwigger CA".

You can configure this setting at Settings > General > About > Certificate Trust Settings.

You should now be able to visit any HTTPS URL via Burp without any security warnings.



After you have completed the installation of the certificate in your device, you can start the monitoring and manipulation processes. Go back to the Burp Suite software and select the “Proxy” tab, followed by the “Intercept” tab. Make sure that the Intercept button is activated. Once you open the application, you can start the interception process. The following picture demonstrates what happens when you manipulate a request from an application when searching for the keyword *kereta dorong* via the iPhone.

According to the Genesis 11:6, “And the Lord said, “Behold, they are one people, and they have all one language, and this is only the beginning of what they will do. And nothing that they propose to do will now be impossible for them.”

References

Bible. Retrieved from https://www.openbible.info/topics/technology.

.