DETECTING VULNERABLE OAUTH 2.0 IMPLEMENTATIONS IN ANDROID APPLICATION

ADVISOR: TETSUTARO UEHARA AND SONGPON TEERAKANOK

RITSUMEIKAN UNIVERSITY

ABSTRACT

OAuth 2.0, a prevalent authorization framework, can be vulnerable to cross-site request forgery (CSRF) attacks, thus requiring developers' due diligence during implementation in Android applications. A key countermeasure includes a state parameter in the URL during the login transition. However, lacking state parameter doesn't necessarily imply an inherent vulnerability to CSRF attacks. To investigate this further, we developed an Android application to analyse other Android applications using OAuth 2.0 with Google accounts, focusing primarily on the utilisation of the state parameter in CSRF attack prevention.

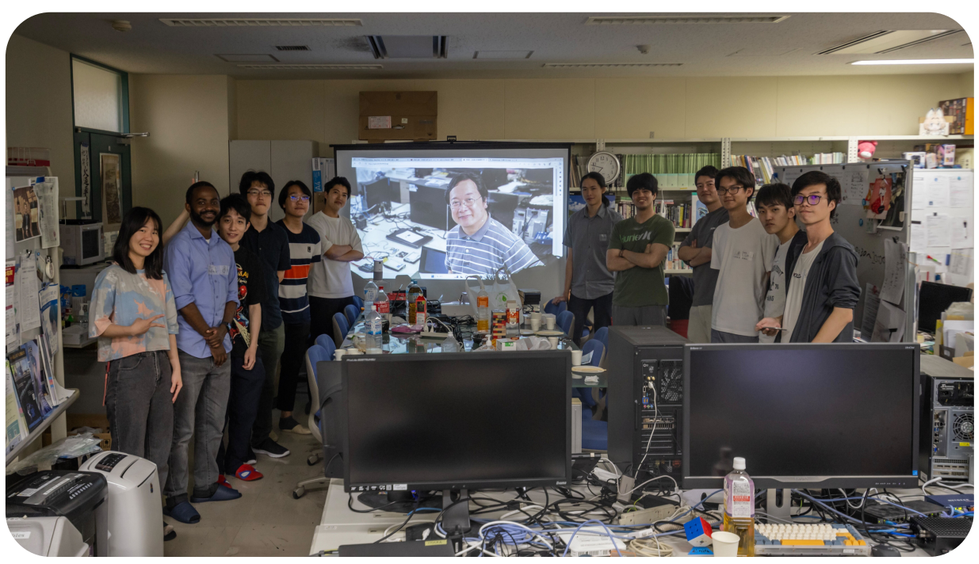
Our investigation involves assessing the login procedures of applications via both the Chrome application and the default browser. Through this, we aim to identify the presence or absence of the state parameter and the authorization code, critical components in a robust CSRF defence strategy. Our findings allow us to evaluate if Android applications using OAuth 2.0 have basic protections against CSRF attacks. The results of our research could protect users by identifying and discouraging the use of Android applications that employ OAuth 2.0 for social login yet remain vulnerable to CSRF attacks.

PERIOD

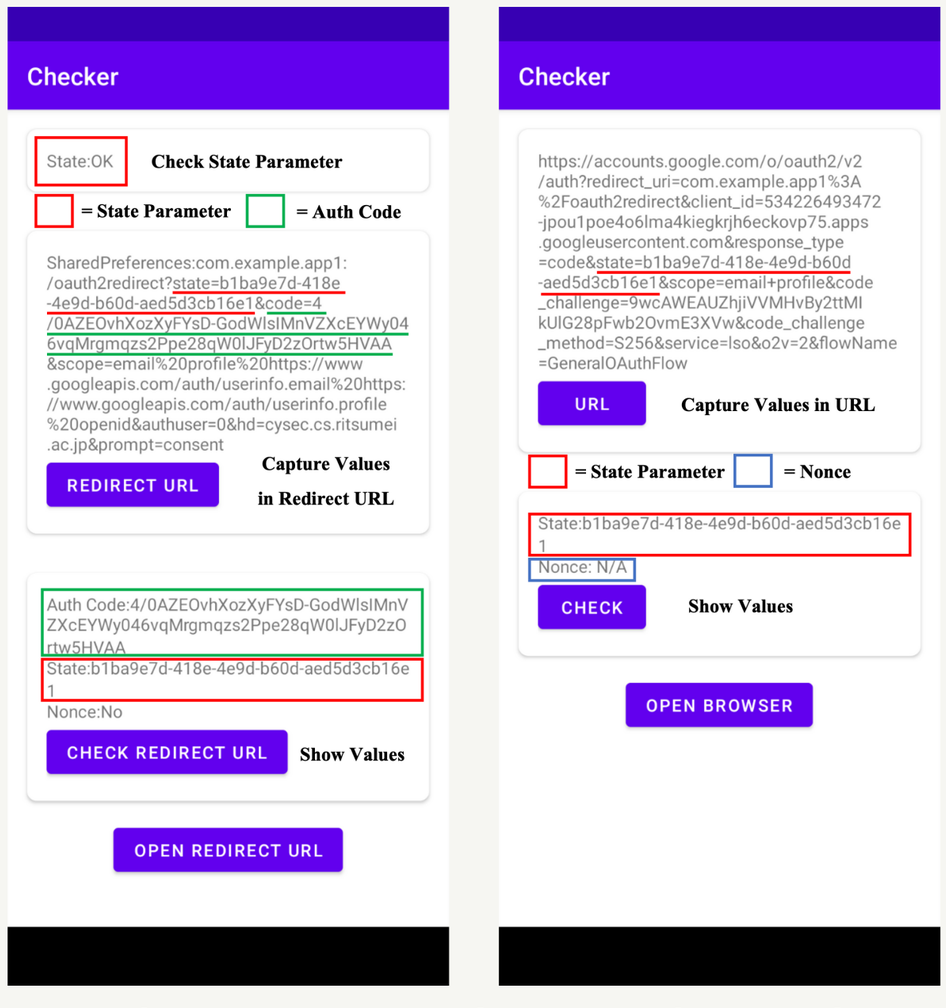
17 May - 21 July 2023 (2 Months)

TECHNICAL TOOLS

- Android Studio
- Java
- Gradle
- OAuth 2.0 Protocol



RESULT



The URL, State, and Nonce values, and the State and Auth Code values in the redirect URL.

WORKFLOW