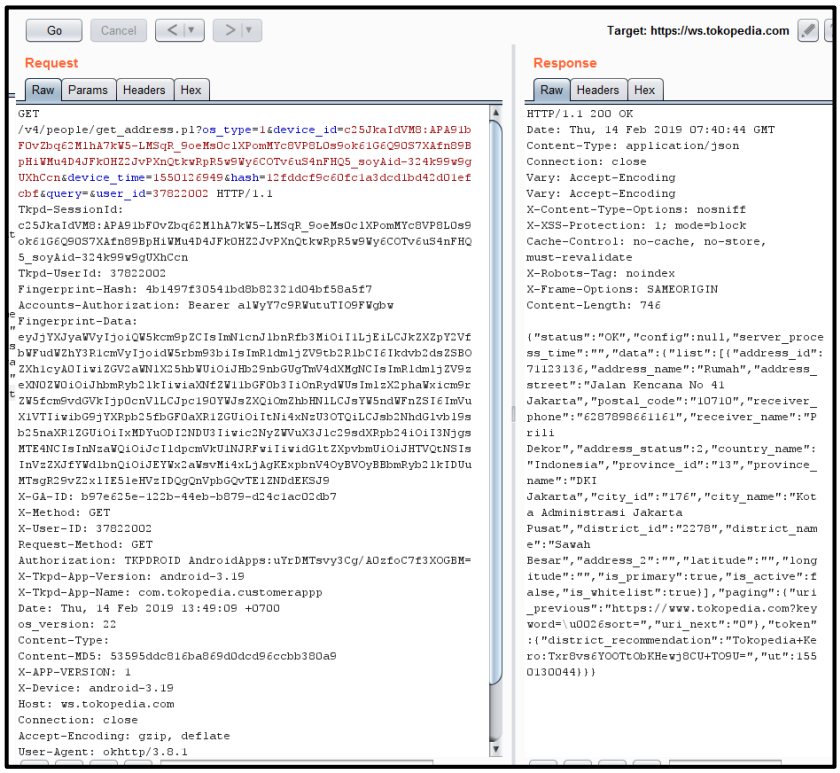
Insecure Direct Object Reference on User's Address Page [Android App]

on 14 February 2019

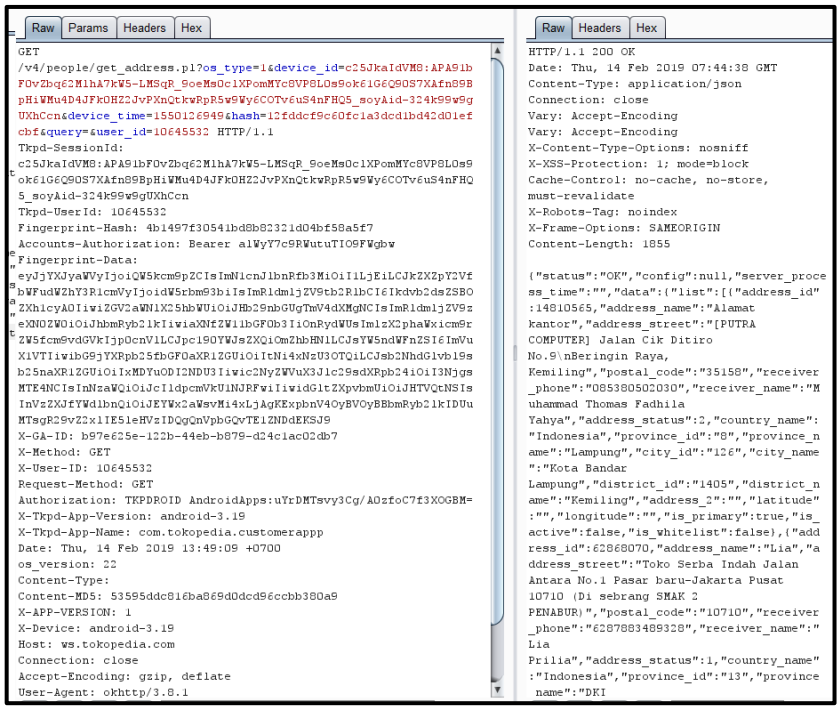
by Muhammad Thomas Fadhila Yahya

Description	**Insecure Direct Object Reference**, also called IDOR. It refers to when a reference to an internal implementation object, such as a file or database key, is exposed to users without any other access control. In such cases, the attacker can manipulate those references to get access to unauthorized data. An attacker can access and dump other user private information like addresses.
Affected Endpoint	**https://ws.tokopedia.com/v4/people/get_address.pl**
Impact	1. Steal user's sensitive information like addresses. 2. Using sensitive information to do phishing.
Steps to Reproduce	1. Open Tokopedia App 2. Login into your Tokopedia account. 3. Open **Akun** 4. Open **Pengaturan** 5. Open **Akun**, and choose **Daftar Alamat** 6. When user access address, it will ask address information through this URL **Pict 1.1** **https://ws.tokopedia.com/v4/people/get_address.pl?os_type=1&device_id=c25JkaldVM8:APA91bF0vZbq62MlhA7kW5-LMSqR_9oeMs0clXPomMYc8VP8L0s9ok61G6Q90S7XAfn89BpHiWMu4D4JFk0HZ2JvPXnQtkwRpR5w9Wy6COTv6uS4nFHQ5_soyAid-324k99w9gUXhCcn&device_time=1550126949&hash=12fddcf9c60fc1a3dcd1bd42d01efcbf&query=&user_id=37822002** 7. Try to intercept the connection to look more detail. 8. In Request body, change user id with other user id **Pict 1.2.** 9. Forward the request and then the address change to others address in response **Pict 1.2.**

POC	List of screenshot



Pict 1.1 Request Intercept



Pict 1.2 Request Modified

Remediation	1. Implement an access control. The user needs to be authorized for the requested information before the server provides it.
References	1. https://www.owasp.org/index.php/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet 2. https://www.owasp.org/index.php/Testing_for_Insecure_Direct_Object_References_(OTG-AUTHZ-004)