FIELD NOTE / BUG BOUNTY

Leaking Sensitive User Data via IDOR in Tokopedia Endpoint

Petruknisme · 21 Mar, 2018 · 2 min to read

After a long hiatus with busy activities in RL, I decided to write again in this blog about my experience with Bug Bounty from Tokopedia. While testing Tokopedia program, I find an IDOR vulnerability in one of the endpoints that lets me leaking user sensitive information include name, phone number, address and etc. Tokopedia has allowed me to share this finding but with redacted sensitive information.

After digging deeper, I find endpoint which use token and unique id for getting some information from server about user data but lacks of token validation. It means, I can use my valid token for getting other user information.

Summary

Leaking user sensitive information include PII(Personally identifiable information)

Details

> *"Affected Parameter: address_id*
>
> *Affected Endpoint: https://accounts.tokopedia.com/ajax/profile/address/get-address?token=(https://accounts.tokopedia.com/ajax/profile/address/get-address?token=)<unique_token>&address_id=<incremented_id>*
>
> *Vulnerability Type: Insecure Direct Object References(IDOR)*
>
> *Severity: Signifficant/HIGH*
>
> *Impact: Leaking user sensitive information"*

Reproduction Steps

1. Visit tokopedia.com and login to your account
2. Click on the Setting and click on address list : https://www.tokopedia.com/people/(https://www.tokopedia.com/people/)/address
3. After that, you will see adress list. Each address will be assigned with unique(incremented) id.
4. Try to remove one of the adress list and Enable your Intercepter. You will see this url for address verification or getting address data:

Licensed under CC BY-SA 4.0

> *"https://accounts.tokopedia.com/ajax/profile/address/get-address (https://accounts.tokopedia.com/ajax/profile/address/get-address) token=24923e36078ef2a103e4759ccdfde875&address_id=38379551"*

address_id with example incremented id

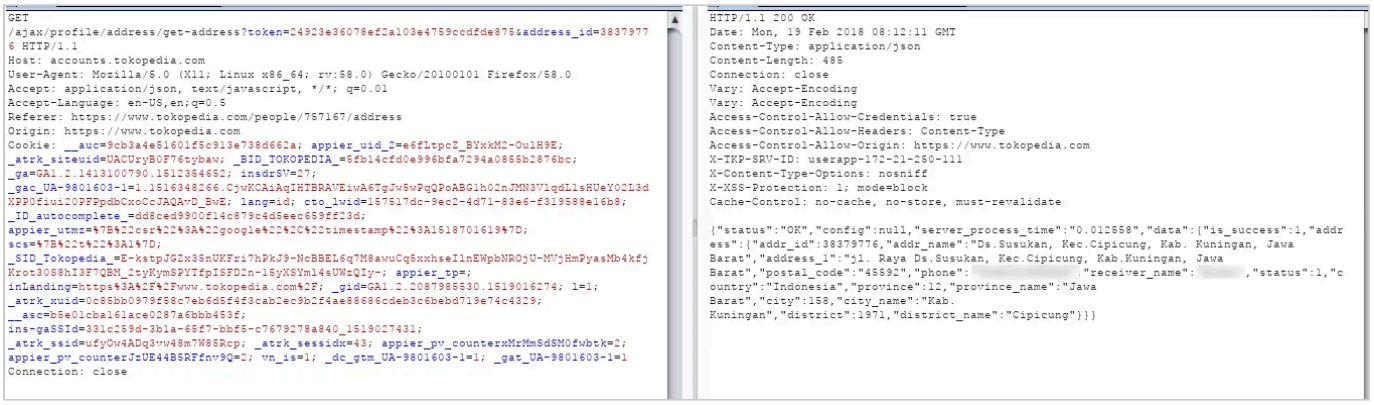
Exploitability

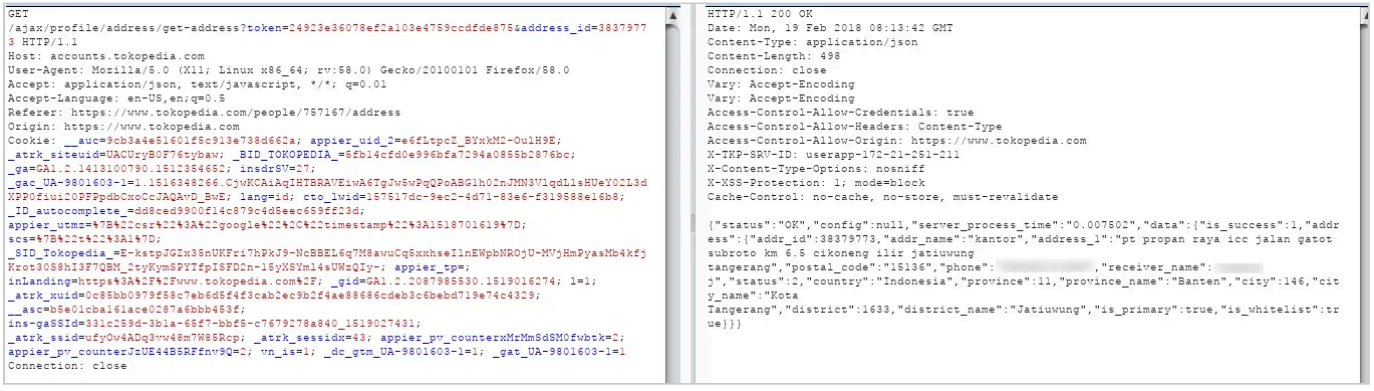
Since address_id is unique(incremented) id, you can incremented one by one with valid token you have for your account. Furthermore, this could be used to perform data grabbing and leaking sensitive information about user data.

Impact

An Authenticated user can perform data grabbing and leak other user sensitive information like address, phone number, shipping name and other information detail.

PoC





TIMELINE

19/02/2018 – Sending Initial Report

19/02/2018 – Verifying and confirm the Report as valid

20/02/2018 – Tokopedia fixed the bug and retest

20/02/2018 – Tokopedia asking my data, and assign this issue as MEDIUM

21/02/2018 – Tokopedia re-assign severity to Signifficant because of PII exposed

22/02/2018 – Sending data to Tokopedia

21/03/2018 – Tokopedia sent reward

Bug Bounty # IDOR # Security # Writeup # Tutorial

Licensed under CC BY-SA 4.0