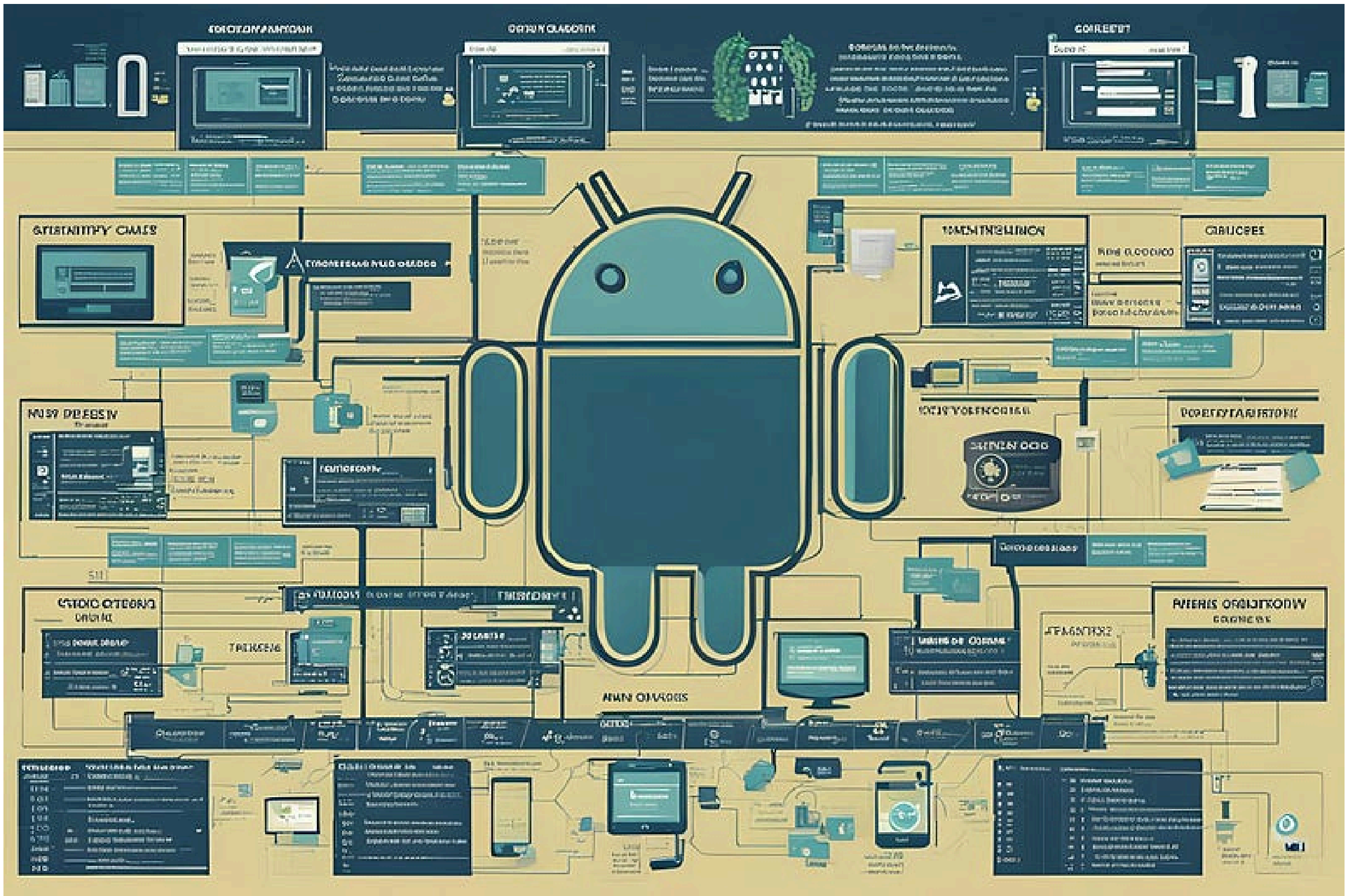
Information Disclosure + XSS on Android APP



I believe the security is a complex and very important process. Due to the lack of permission, the name of the application is not mentioned, and I call it an Android application.

About 2 month ago i had a PenTest contract with Programming Company for one Android Application, Android Applications have different challenges than Web Applications, for example you must to know **Android emulator** and some Android programming knowledge and etc.

Let’s go to tell you about this Android Application Vulnerability, usually like always i follow my Android Security Check-List for that and fortunately found some good vulnerability in first day but to this write-up want tell about one of the interesting vulnerability i found.

At the first time like a normal user work with Android Application and try to know application work flow and note each EndPoint i found, in this part you must try to find EndPoint and **Logical** Vulnerability and must note try to find technically vulnerability always, in some part of application like search bar and user profile i try to inject some payloads like **SQL** injection and **XSS**(Cross Site Scripting) but none of them work…

I decided to check my BurpSuite HTTP History and find some nice EndPoint, One of them was in a POST request that was sent to update the user's profile information and it was "**User_Id**" which was equal to the phone number of each user, and it did not have any special validation and as you thought about it, I also used **IDOR** I thought.

IDOR

I can simply change "**User_Id**" parameter and change other user's profile, it was work for all of user's because application use phone number for identification and don't have any validation, i can implementation some attack like Brute-Force for user phone number discovery and Next change user's profile information or in another scenario if i know any application user's phone number i can change that user profile information.

Information Disclosure + XSS

In second day when i review HTTP History in Burp-Suite suddenly one GET request catch my attention and it contain all of user information in response without any validation, the GET URL like this:

```
https://target.com/api/user_v3_6/profile/09396******
```

I can found IDOR again but with higher impact and it disclosure user information with have just one user phone number, user's information contain first-name,last-name,wallet-info,address,cart-info and etc.

Where is XSS?

If you remember, I injected some payload in some part of the application like the search bar and my user profile, and none of them worked, but in this IDOR and in this part, when the user information was loaded, my payload was also executed and it works here.

Maybe you don't believe but i was used this simple payload for exploit:

```
<script>alert`XSS`</script>
```

> The point you should pay attention to is that first of all, don't be disappointed and check the same section and route several times and try to test it with different methods and tricks every time and every EndPoint you find can help you. It helps in discovering a vulnerability,

> so pay attention to things like HTTP History and try to review it carefully and several times and examine the cycle and performance path of each part in order to be more successful in discovering logical and technical vulnerabilities.

Like always my friend **mk990** help me in this project.