BÀI TẬP CTF

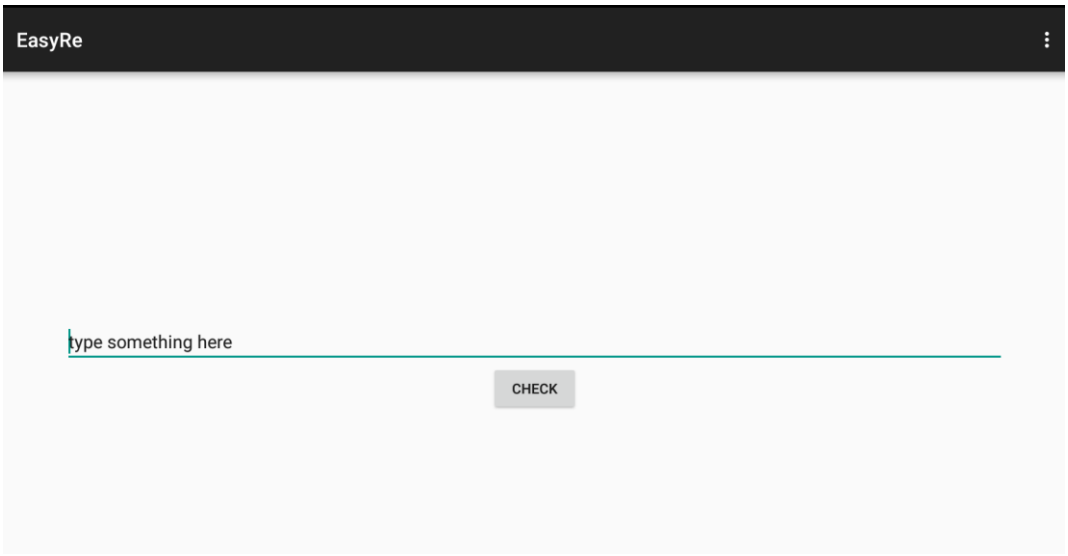
Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

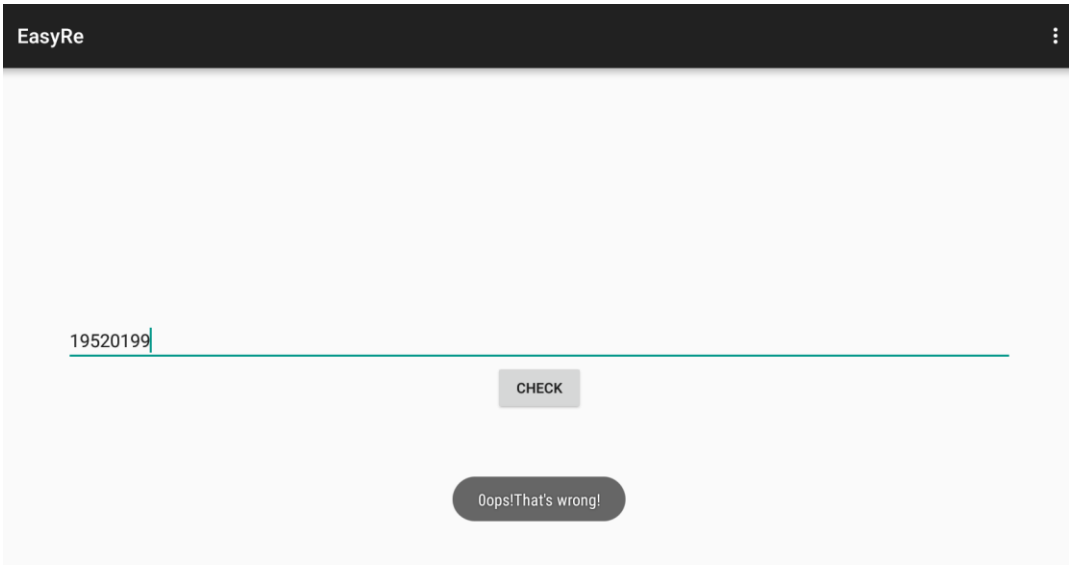
Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

Challenge 1: EasyRe

- Cài đặt ứng dụng, ở đây em sử dụng LDPlayer để chạy ứng dụng
- Ta thấy ứng dụng đơn giản gồm một input nhập vào và một nút kiểm tra



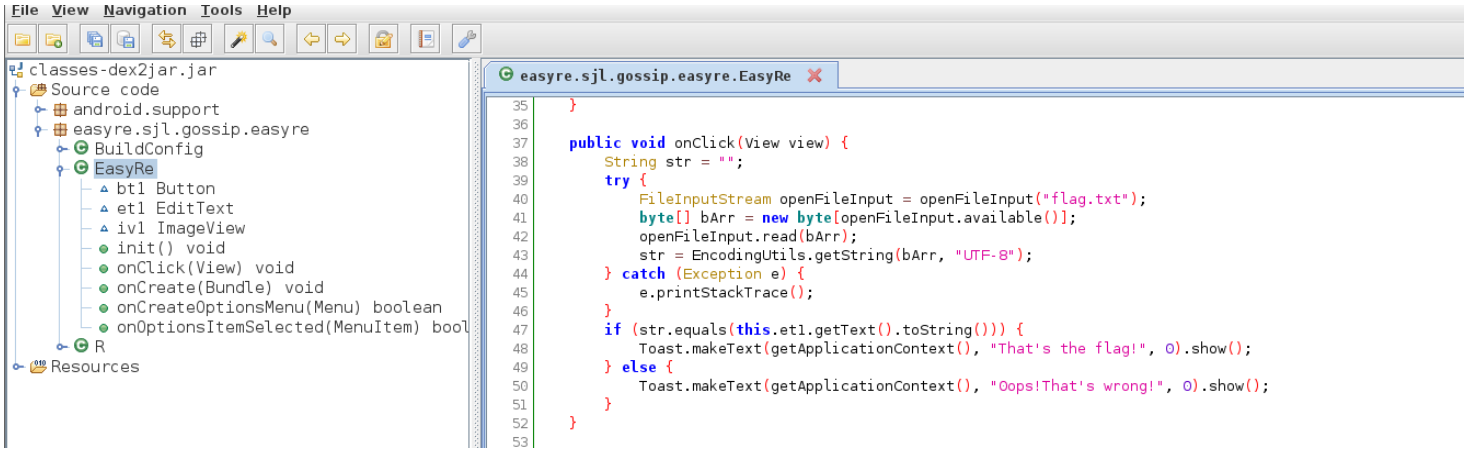
- Thử nhập nội dung là 19520199 và nhấn check thì xuất hiện thông báo **Oops! That's wrong!**



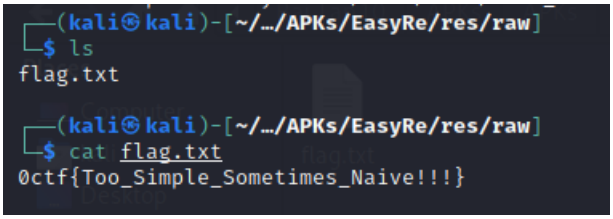
- Giải nén file EasyRe.apk, sau đó sử dụng dex2jax để chuyển file class.dex thành file jar
- Sử dụng jadx-gui để dịch ngược ứng dụng và xem các logic cơ bản của nó

```
┌──(kali㉿kali)-[~/…/Bai Tap 10/APKs/APKs/EasyRe]
└─$ jadx-gui classes-dex2jar.jar
```

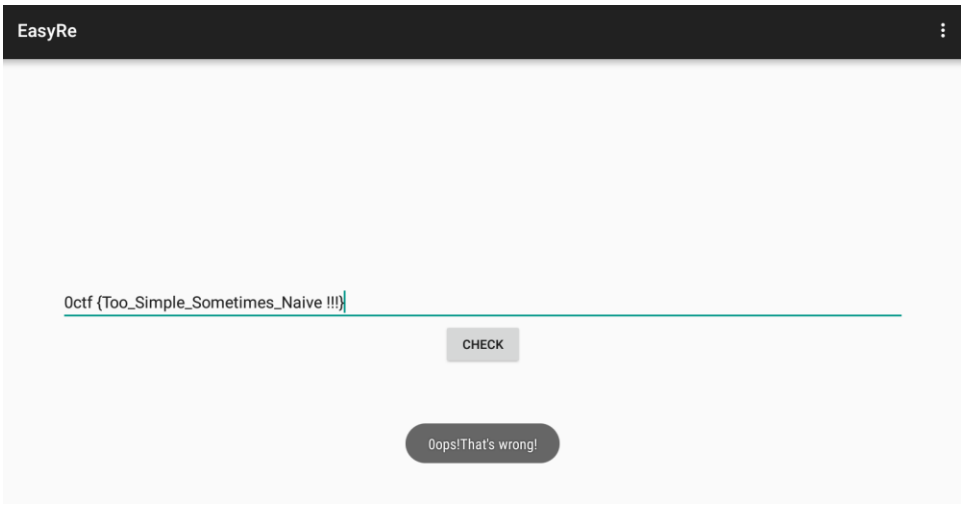
- Ở activity EasyRE ta thấy biến str lưu chuỗi được được từ file flag.txt và sau đó so sánh với chuỗi nhập vào của chúng ta. Nếu đúng in ra thông báo That’s the flag ngược lại in ra Oops” That’s wrong.



- Do đó flag của ta nằm trong file flag.txt. File flag.txt nằm tại res/raw
- Đọc file này và ta thu được flag thành công



- Thử nhập chuỗi vừa tìm được và nhấn nút check. Ta thành công in ra thống báo Oops! That's wrong!



FLAG: 0ctf{Too_Simple_Sometimes_Naive!!!}