BÁO CÁO BÀI TẬP

**Môn học: Bảo mật Web và Ứng dụng**

**Kỳ báo cáo: Cuối kỳ**

*GV: Nghi Hoàng Khoa*

*Ngày báo cáo: 04/06/2023*

1. **THÔNG TIN CHUNG:**

Lớp: NT213.N21.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Vũ Hoàng Thạch Thiết | 20521957 | 20521957@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Warm up |  |
| 2 | Cr@ck m3 |  |
| 3 | RacMe |  |
| 4 | MimeMe |  |
| 5 | Flappy Bird |  |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

## Warm up

* Phần này ta chỉ cần vào link discord được cung cấp là có được flag

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

* Flag : flag{tk4\_d3\_qj0t\_m0\_h0j\_r0j\_tr3n\_tr4nq\_s4ck\_c0n\_h0n\_qj0t\_nu0c\_m4t\_r0j\_tr3n\_d3\_tkj}

## Cr@ck m3

Ảnh có chứa văn bản, Phông chữ, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

* Sử dụng jadx để decompile file apk được cung cấp thành file java cho dễ xem
* Trong đường dẫn sources/com/example/secret/ ta đọc file MainActivity.java

Ảnh có chứa ảnh chụp màn hình, Phần mềm đa phương tiện, phần mềm

Mô tả được tạo tự động

* Trong hàm toggle:

+ Biến sb được khai báo để nhận input từ người dùng và lưu trữ

+ Biến string sử dụng hàm getstring để lấy giá trị gì đó tên là something.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

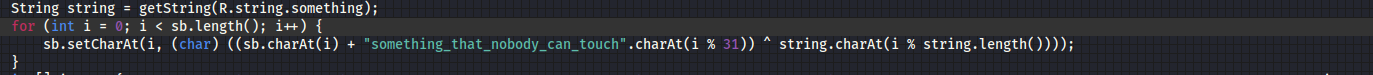
Mô tả được tạo tự động

* Trong R.java ta thấy nó có khai báo biến tên là something thì có thể giá trị nó ta có thể xem được trong string.xml

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Nó được khai báo là “no\_one\_can\_escape\_from\_me”
* String = “no\_one\_can\_escape\_from\_me”



+ Trong vòng for có vai trò mã hóa các ký tự trong sb ta nhập bằng cách :

* Với mỗi ký tự trong sb

+ Lấy ký tự tương ứng trong chuỗi khóa bí mật "something\_that\_nobody\_can\_touch" bằng cách sử dụng toán tử % để tính toán chỉ số trong chuỗi khóa dựa trên chỉ số của ký tự hiện tại trong chuỗi sb

+ Thực hiện XOR giữa ký tự hiện tại trong sb và ký tự trong chuỗi khóa bí mật tương ứng

+ Sử dụng phương thức setCharAt() của đối tượng StringBuilder để thay thế ký tự hiện tại trong chuỗi sb bằng kết quả XOR được

Ảnh có chứa ảnh chụp màn hình, Phần mềm đa phương tiện, hàng, phần mềm

Mô tả được tạo tự động

* Trong vòng for này thì sẽ kiểm tra độ dài của chuỗi sb có bằng 41 không. Nếu đúng thì tiếp tục kiểm tra xem từng ký tự của sb với từng ký tự trong kết quả của biểu thức XOR giữa giá trị ngẫu nhiên nhiên được tạo bởi generator.nextInt() & 255 và giá trị tương ứng trong mảng iArr
* So sánh kết quả của phép XOR với ký tự tương ứng trong chuỗi sb
* Vậy ý tưởng sẽ là tìm chuỗi sb bằng cách làm ngược lại quá trình mã hóa

Ảnh có chứa ảnh chụp màn hình, Phần mềm đa phương tiện, phần mềm, Phần mềm đồ họa

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Flag : flag{4ndr0id\_r3v\_5ucks55555555\_@$#&#$^#$}

## RacMe

Ảnh có chứa ảnh chụp màn hình, hàng

Mô tả được tạo tự động

* Đọc mã nguồn thì thấy có lỗ hổng LFI
* Nó sẽ kết hợp đường dẫn hiện tại với biến “note” được truyền bởi user để có thể tạo đường dẫn đầy đủ tới thư mục được yêu cầu
* Từ đó có ý tưởng ta sẽ truy cập các thư mục trong server thông qua biến note

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

* Ta truyền các tham số từ từ vào để xem bao nhiêu thì nó sẽ đưa ta đến được /etc/passwd

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

* Nhưng ở đây thì normal user mới có quyền xem được note
* Normal user sẽ được xác thực bằng biến cookie PHPSESSID
* Ta chỉ cần thay đổi biến này thành bất kỳ gì là không còn là normal user được đăng ký trong hệ thống nữa

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

* Ta thêm giá trị 1 vào cuối

Ảnh có chứa văn bản, Phông chữ, bức thư, ảnh chụp màn hình

Mô tả được tạo tự động

* Kết quả trả về cho ta các thông tin các tài khoản trong linux
* Nhưng ở đây ta muốn RCE
* Tìm kiếm thông tin thì ta biết là PHP SESION sẽ được lưu trữ ở /tmp/sess\_<PHPSESSID>

Ảnh có chứa văn bản, Phông chữ, hàng, ảnh chụp màn hình

Mô tả được tạo tự động

* Với PHPSESSID là ID cũ của ta trước khi sửa đổi

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, màu trắng

Mô tả được tạo tự động

* Kết quả trả về cho ta
* Nhưng vẫn chưa thể có được RCE
* Sau khi đọc blog: <https://ctf.zeyu2001.com/2021/metactf-cybergames/custom-blog?fbclid=IwAR1pGjSlyEuDTlnEPhRV6zYJVvFJOEsanvnUwJqSUfa7Cxs11kEONyAYeZM>
* Thì thấy là ta cần phải set 1 biến nào đó(trong blog là biến theme) bằng hàm system với giá trị là c để từ c qua đó ta có thể thực hiện các lệnh system
* Nhưng ở đây thì không thấy được ta có thể set được biến nào nên ta sẽ tạo tài khoản với username là “<?php system($\_GET['c']) ?>” từ đó có biến c để thao tác

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

* ở đây ta dùng biến “m” vì “c” đã có người tạo trước đó

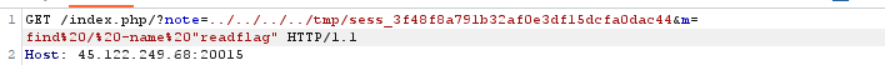


* Tạo thành công thì ta làm lại các bước như trên và muốn sử dụng biến “m” thì ta chỉ cần “&m=<lệnh>” là được

Ảnh có chứa văn bản, biên lai, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

* Kết quả trả về lệnh ls của ta



* Tìm các file có flag

Ảnh có chứa văn bản, Phông chữ, hàng, ảnh chụp màn hình

Mô tả được tạo tự động

* Ta thấy có 1 thư mục là /readflag



* Ta cd đến và thực thi

Ảnh có chứa văn bản, biên lai, Phông chữ, hàng

Mô tả được tạo tự động

* Flag: “flag{racing\_racing\_and\_you\_pwned\_me}”

## MIMEME

* Nothing ... The source code is enough

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

* Khi vào trang web, một form login hiện ra. Điểm đặc biệt là không thấy nút đăng ký

Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự động

* Dựa vào nội dung file docker cung cấp đi kèm, ta thấy các điểm đáng chú ý sau:

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

* Code được cung cấp
* Việc truy cập và các chức năng của web thông qua một router (cơ chế của ExpressJS), và đường dẫn các router có thể thấy trong file agent.js
* Thấy được việc đăng ký hay các chức năng như upload và details phải có thông tin xác thực qua identifier và token

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

* Thực hiện đăng ký một user để lấy các thông tin cần

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, Phông chữ

Mô tả được tạo tự động

* Ta đăng ký 1 user
* Thực hiện kiểm tra check với thông tin vừa có

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, Phông chữ

Mô tả được tạo tự động

* Sau khi đăng ký ta dùng /agents/check để kiểm tra
* Kế đến phần thông tin của user vừa đăng ký qua detail có dạng request POST với data body là các JSON đi kèm

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, Phông chữ

Mô tả được tạo tự động

* Tại đây để kiểm tra rõ hơn, thực hiện trên môi trường docker được cung cấp

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

* Có thể thấy nội dung của admin là sẽ nhận các thông tin được upload lên của user
* Mà các thông tin này không hề có một cơ chế lọc hay cơ chế fillter các html
* Thực hiện truyền vào các tag html

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Trang web, phần mềm

Mô tả được tạo tự động

- Ta đưa thử các thông tin mà không được lọc vào 1 dạng json Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Vậy là có thể thực hiện tấn công XSS tại trang của admin
* Nếu thực hiện store XSS và lấy về nội dung tại trang của admin được không ?

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

* Ta truyền URL vào trực tiếp để attack thì không được
* Có vẻ cơ chế truyền file JSON trực tiếp không cho phép thực hiện
* Xem qua chức năng upload của web

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Các request sẽ đính kèm một file, và xét điều kiện của file và trả về

Tuy nhiên file sẽ yêu cầu phải là một dạng recordingẢnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Nó phải có Type là audio/wave
* Và file đó phải có đuôi dạng là “.wav”
* Kế đến phải có một buffer đính kèm có regex filter, nếu tra bảng ASCII ta có thể kết luận dạng buffer là: RIFF[a-z0-9]{8}WAVE
* Đi kèm đó là cơ chế gửi nhiều file cùng lúc, khi đó ta chỉnh sửa lại request

eẢnh có chứa văn bản, ảnh chụp màn hình, Hình chữ nhật, mẫu

Mô tả được tạo tự động

* Xem thử bảng ASCII

Ảnh có chứa văn bản, Phông chữ, số, ảnh chụp màn hình

Mô tả được tạo tự động

* Sau đó ta truyền payload vào trang web
* Khi đó trên admin đã thấy có 1 file wav được cập nhật lên và có tên file là một dạng mã hoá

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

* Ta truy cập vào file audio thì ta thấy sẽ kích hoạt việc gọi đến một URL đã truyền vào khi tạo file

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

* Đây là payload ta dùng để tấn công khi đã dùng ở local thì ta xác định được flag sẽ lưu ở h2
* Bằng cách đó ta thực hiện tấn công XSS bằng cách gọi lại tên file đã tạo và đợi việc truy cập vào file audio đã truyền lên

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, phần mềm

Mô tả được tạo tự động

* Khi kiểm tra thì thấy bị mất thông tin hostna,e

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Đây là request nhận được

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

* Sử dụng decode base64 là có được flag
* Vậy là ta có thể khai thác để lấy được flag từ phía admin mà không cần đăng nhập
* Thực hiện tương tự trên webserver ta có

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

* Ta đưa payload chuẩn bị lúc nãy vào

Ảnh có chứa văn bản, phần mềm, số, Trang web

Mô tả được tạo tự động

- Chỉnh sửa thông tin để có thể tấn công

- Ảnh có chứa văn bản, phần mềm, số, Trang web

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Flag: flag{mime\_sniffing\_is\_cool\_right???}

## Flappy Bird

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Mô tả được tạo tự động

* Khi truy cập app ta được giao diện như trên
* Kiểm tra một vòng source code của app, ta có các thông tin

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Mô tả được tạo tự động

* Đây là code xử lý điểm để gọi đến hàm championActivity
* Một hàm sẽ kích hoạt gọi đến chương trình ChampionActivity để lấy ra flag nếu hàm đếm điểm đến giá trị “999.999.999”

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Đây là hàm gọi tới hàm getflag()
* Tuy nhiên lại phát hiện ra có một chương trình log ra một giá trị gọi là Signature, giá trị này có vẻ để kiểm tra tính toàn vẹn của app

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

- Hàm xử lý log ra giá trị signature để bảo đảm tính toàn vẹn để không thể sửa đổiẢnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Tuy nhiên giá trị log này ta có thể lấy được bằng cách truy cập vào file lưu trữ của app
* Nhờ vào đó ta có thể thay đổi code smali để thực hiện thay đổi app theo hướng mình muốn
* Thay đổi việc kiểm tra giá trị signature của app bằng cách truyền thẳng giá trị cần kiểm tra vào kết quả trả về của hàm

Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn

Mô tả được tạo tự động

* Hình trên là xử lý signatire sẽ gene ra chuỗi

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

* Ta truyền thẳng giá trị signature vào giá trị trả về của hàm

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

* Hàm xử lý điểm so sánh với giá trị 999.999.999 để có thể gọi hàm champion

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Ta thay đổi giá trị thành 0 để có thể có được flag
* Thay đổi điều kiện đếm điểm để đạt được việc gọi ra hàm ChampionActivity để rồi lấy ra được flag

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Ta ký cho app
* Quá trình ký xác nhận app và tải app lên thiết bị kiểm thử

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Ký và tải app
* Kết quả trả về của flag hiển thị trên màn hình

Ảnh có chứa văn bản, ảnh chụp màn hình, máy tính, phần mềm

Mô tả được tạo tự động

Flag: flag{ck0n\_vj3c\_kh0\_d3\_d4n\_d4u}