Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 02 (Session 01)

Tên chủ đề: Intro

GV: Nghi Hoàng Khoa

Ngày báo cáo: 15/03/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)
Lớp: NT213.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	5 Kịch bản	100%	

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

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Kịch bản 01

Tiêu đề: Vulnerable and Outdated Components – data, infomation
Mô tả lỗ hổng:
Tóm tắt: Web cho phép thực hiện chuyển đổi yaml sang json và ta cần thực hiện truyền file yaml có code thực thi

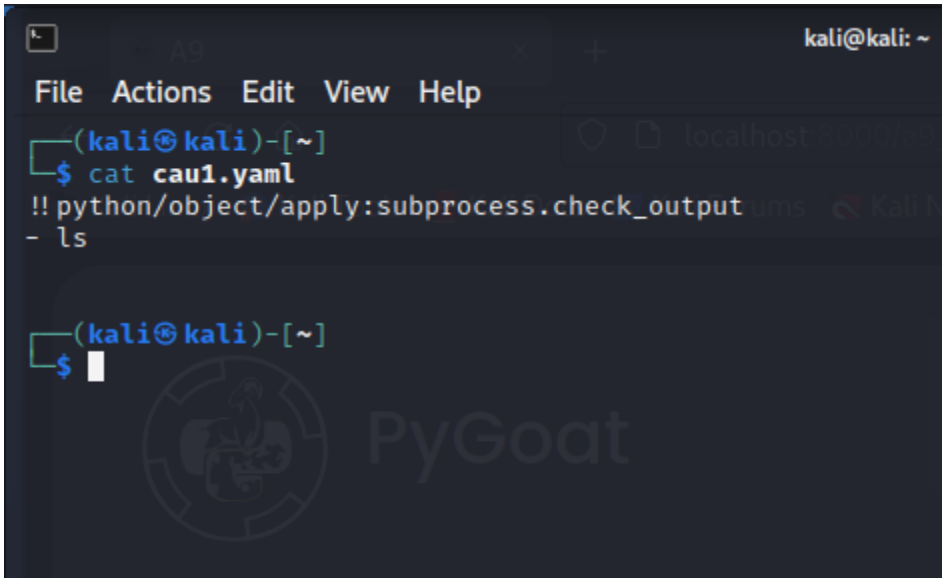
Các bước làm

Đầu tiên ta sẽ thực hiện vào trang web để xem trang web để xem thì ta thấy được chương trình có khả năng chuyển đổi từ yaml sang json

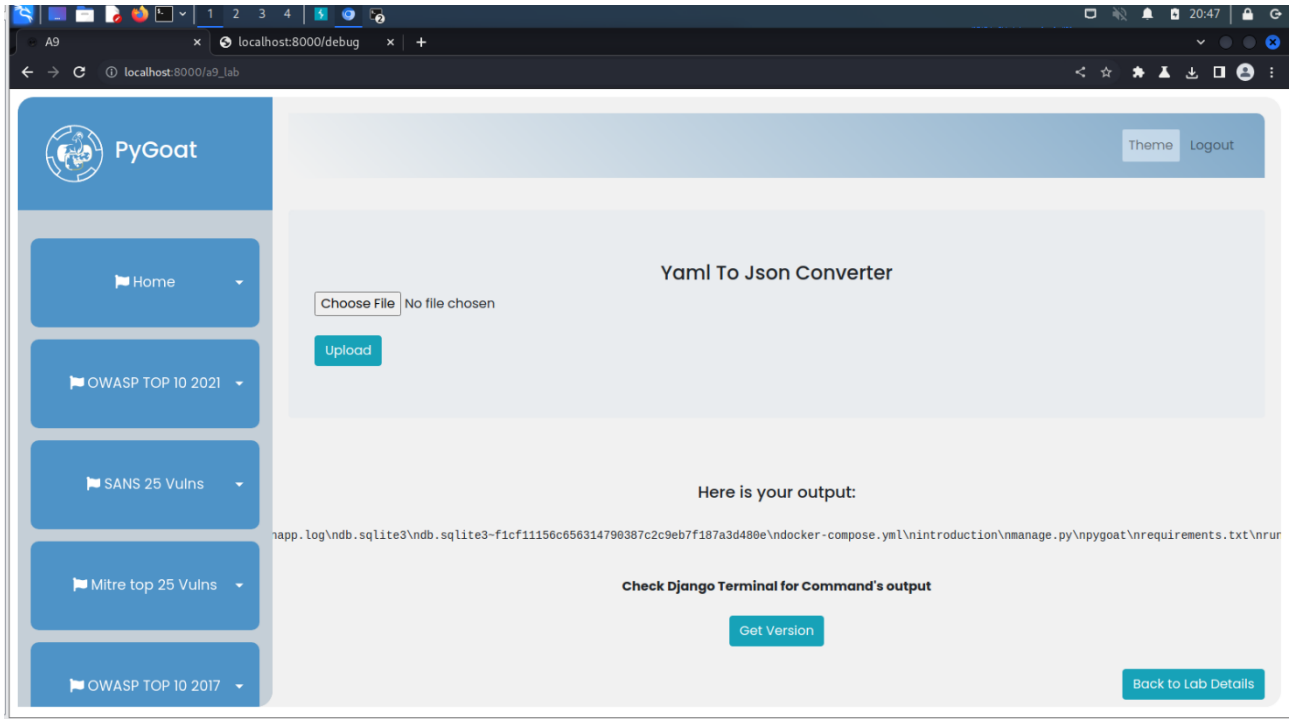
Vậy ta sẽ thử thực hiện khai thác bằng gửi một file yaml lên mà có thể thực hiện chạy code. Đầu tiên ta cần tạo ra 1 file yaml có code chạy:

!!python/object/apply:subprocess.check_output

- ls



Tiếp theo ta sẽ tải file lên và submit thì ta thấy được là kết quả trả về là lệnh ls, ta đã thực hiện tấn công thành công



Mức độ ảnh hưởng: high

Khuyến cáo: Thực hiện lọc đầu vào các file truyền vào, chặn các thao tác execute trên file được truyền vào

2. Kịch bản 02

#Tiêu đề: *Identification and Authentication Failures – quyền truy cập tài khoản*
#Mô tả lỗ hổng:

Tóm tắt: Web cung cấp tài khoản admin và password ở dạng hash, ta không cần đăng nhập mà chỉ cần thực hiện phá hoại để chặn tài khoản truy cập trong 1 ngày

Các bước làm:

Đầu tiên ta sẽ thực hiện việc login vào tài khoản thì ta không biết password là gì, ta chỉ biết được username là admin_pygoat@pygoat.com

Ta sẽ thực hiện đăng nhập lại với những password thông dụng như

123456

123

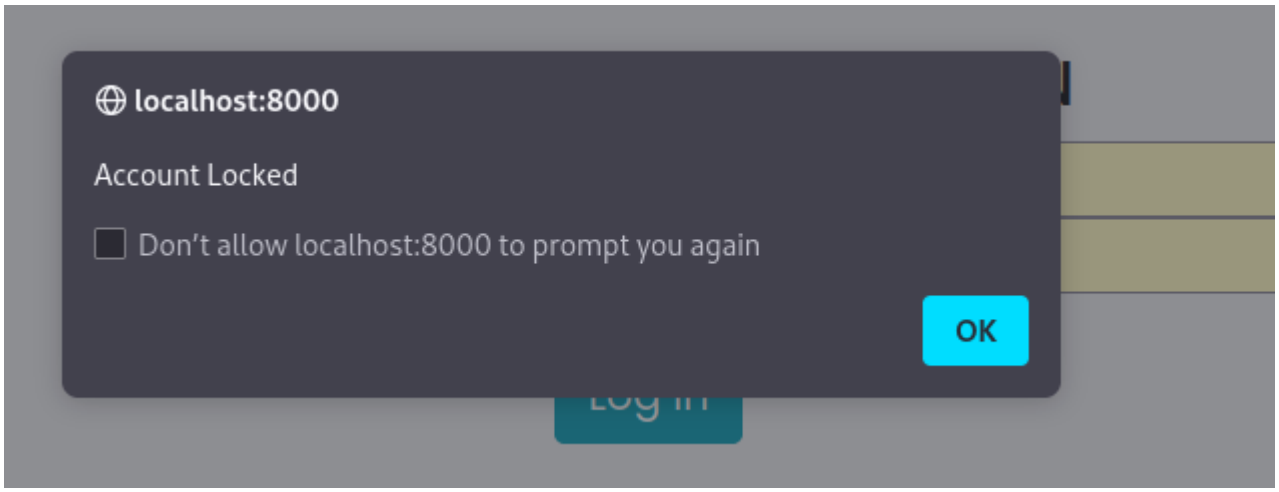
1234

Admin

Pass

Password

Nhưng khi đăng nhập quá 5 lần và bị sai thì tài khoản của ta sẽ bị xoá



Khi này một trường thông tin khác sẽ hiện lên rằng là việc đăng nhập 5 lần này có vấn đề thì sẽ lock tài khoản 1440 phút tức 24h, như vậy với quyền tài khoản khi ta nhập quá số lần thì sẽ bị khoá. Như vậy ta đã thực hiện khoá thành công tài khoản admin

```
    try:
      ph = PasswordHasher()
      ph.verify(user.password, password)
      if user.is_locked == True and user.lockout_cooldown < datetime.date.today():
        user.is_locked = False
        user.last_login = datetime.datetime.now()
        user.failattempt = 0
        user.save()
      return render(request,"Lab_2021/A7_auth_failure/lab2.html", {"user":user, "success":True,"failure":False})
    except:
      fail_attempt = user.failattempt + 1
      if fail_attempt == 5:
        user.is_active = False
        user.failattempt = 0
        user.is_locked = True
        user.lockout_cooldown = datetime.datetime.now() + datetime.timedelta(minutes=1440)
        user.save()
        return render(request,"Lab_2021/A7_auth_failure/lab2.html", {"user":user, "success":False,"failure":True, "is_locked":True})
      user.failattempt = fail_attempt
      user.save()
      return render(request,"Lab_2021/A7_auth_failure/lab2.html",{"success":False, "failure":True})
  except Exception as e:
    print(e)
    return render(request,"Lab_2021/A7_auth_failure/lab2.html",{"success":False, "failure":True})
```

View Code Back to Lab Details

Mức độ: high

Khuyến cáo: Thực hiện việc thông báo đăng nhập qua các bên như mail hoặc các thiết bị khác đã đăng nhập trước đó, thông báo đăng nhập thiết bị, thực hiện can thiệp truy vấn ip thiết bị để kiểm tra

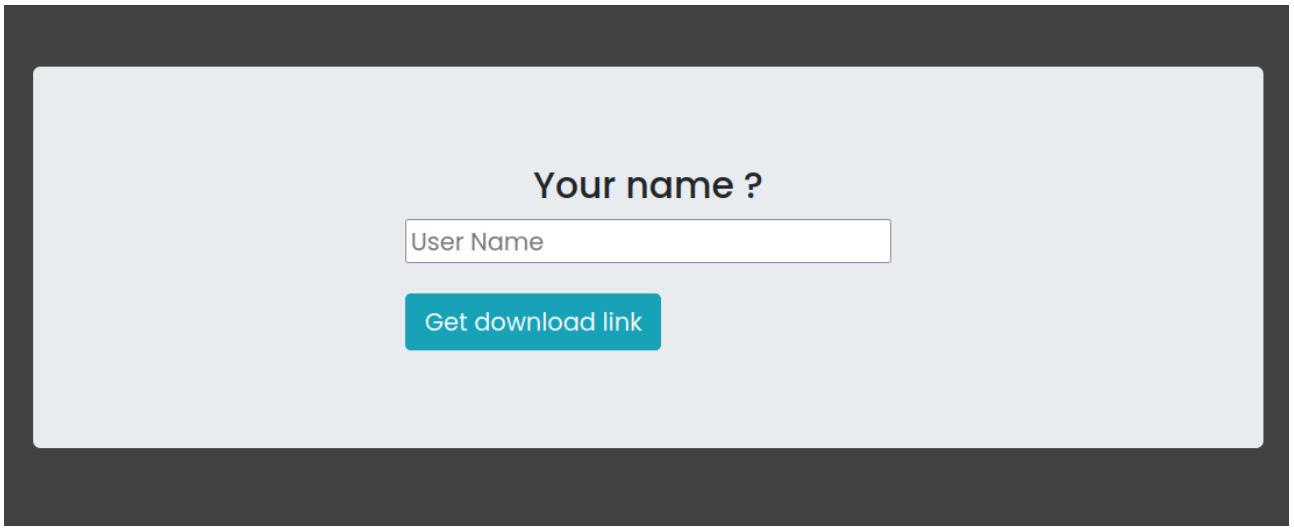
3. Kịch bản 03

#Tiêu đề: *Software and Data Integrity Failures - data*
#Mô tả lỗ hổng:

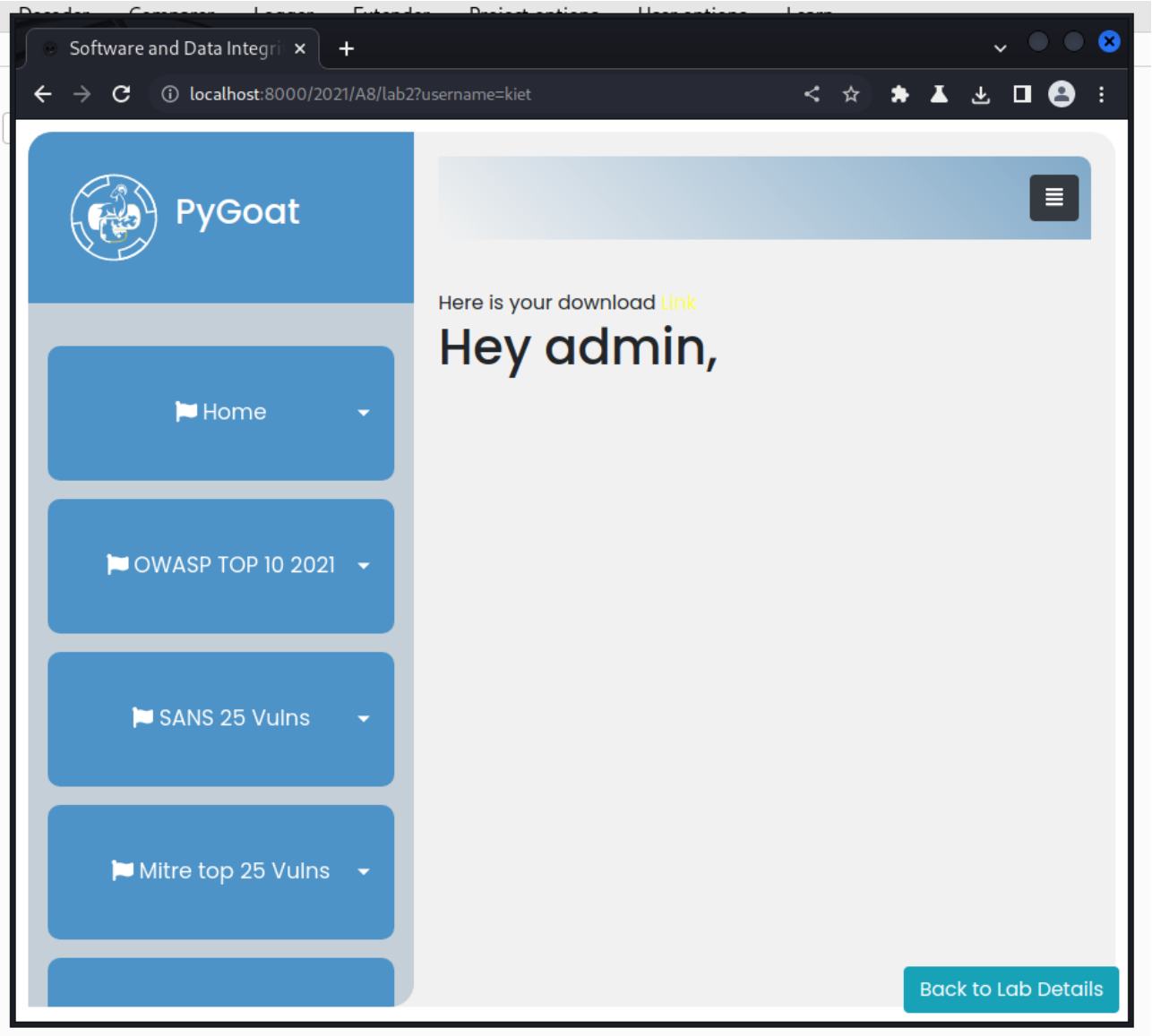
Tóm tắt: khi truy cập trang chúng ta sẽ tải file về nhưng chúng ta thực hiện việc chỉnh sửa và tải file khác về để can thiệp vào tính toàn vẹn dữ liệu

Các bước làm

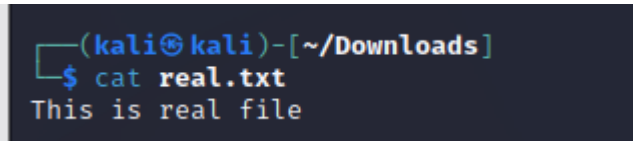
Đầu tiên chúng ta sẽ thực hiện truy cập vào trang thì sẽ hiện thông tin để ta nhập tên và tải file



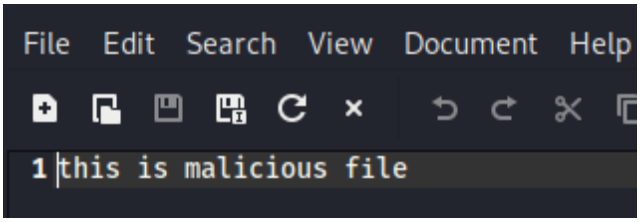
Sau khi nhập xong thì ta có 1 cái link download, ta sẽ thực hiện việc download



Sau khi tải về ta có được file real.txt



Ngoài ra gợi ý đề bài cho ta được thêm file fake.txt



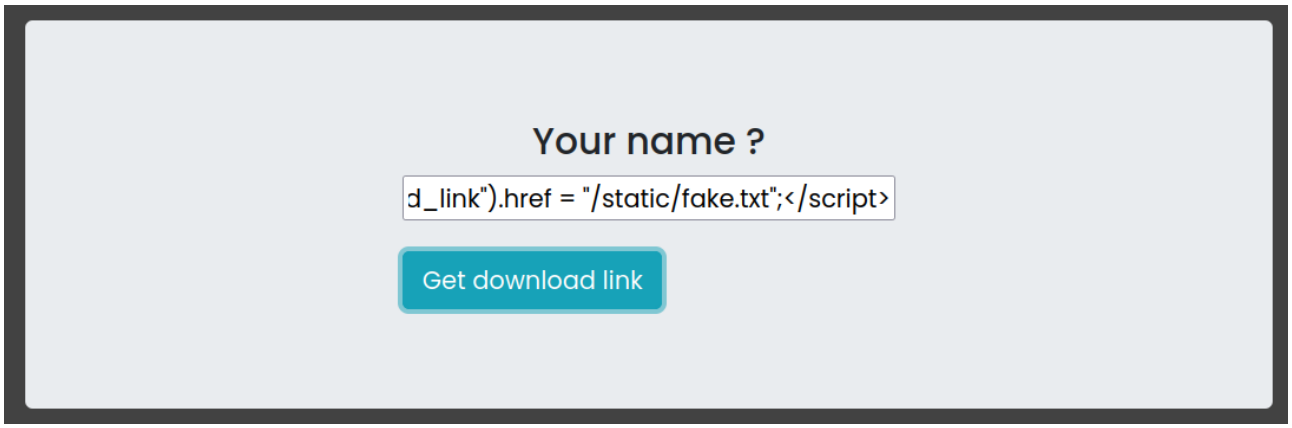
Kiểm tra thử tính toàn vẹn bằng sha256 thì ta thấy đây là 2 mà chúng ta sẽ thực hiện khai thác bằng cách là khi nhấn vào link thay vì tải file real thì ta sẽ tải file fake về

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sha256sum fake.txt
7f91a6bf2ebd692b02b442f1eb447bafca17b3f8d37331cd7cfcc68e3d2f23f7  fake.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ sha256sum real.txt
773ff9dfab2f6568bcce2b8f3a8db4e5c6f6962b187e65e5b0896c7cf2cfa777  real.txt

┌──(kali㉿kali)-[~/Downloads]
└─$
```

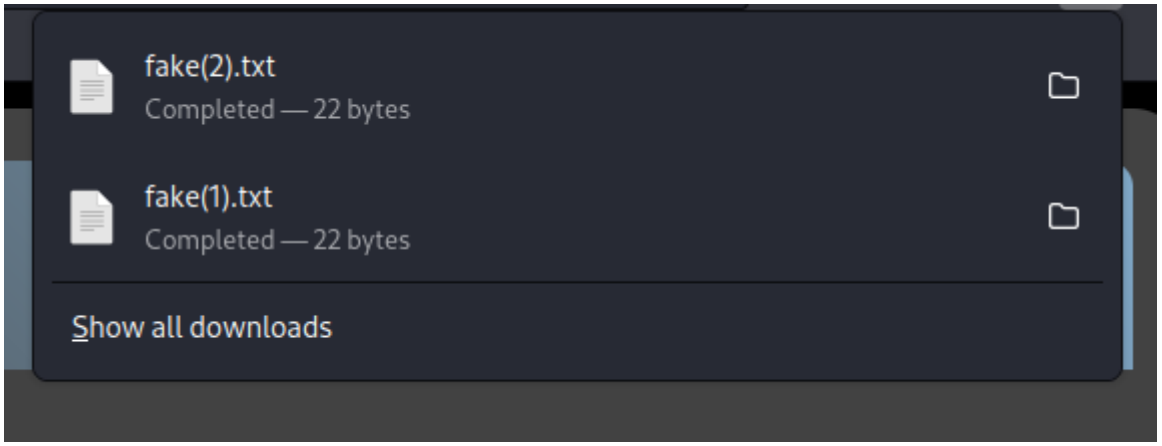
Bằng ý tưởng đó ta sẽ thực hiện code js bằng cách thêm đoạn code bên dưới:

<script>document.getElementById("download_link").href = "/static/fake.txt";</script>

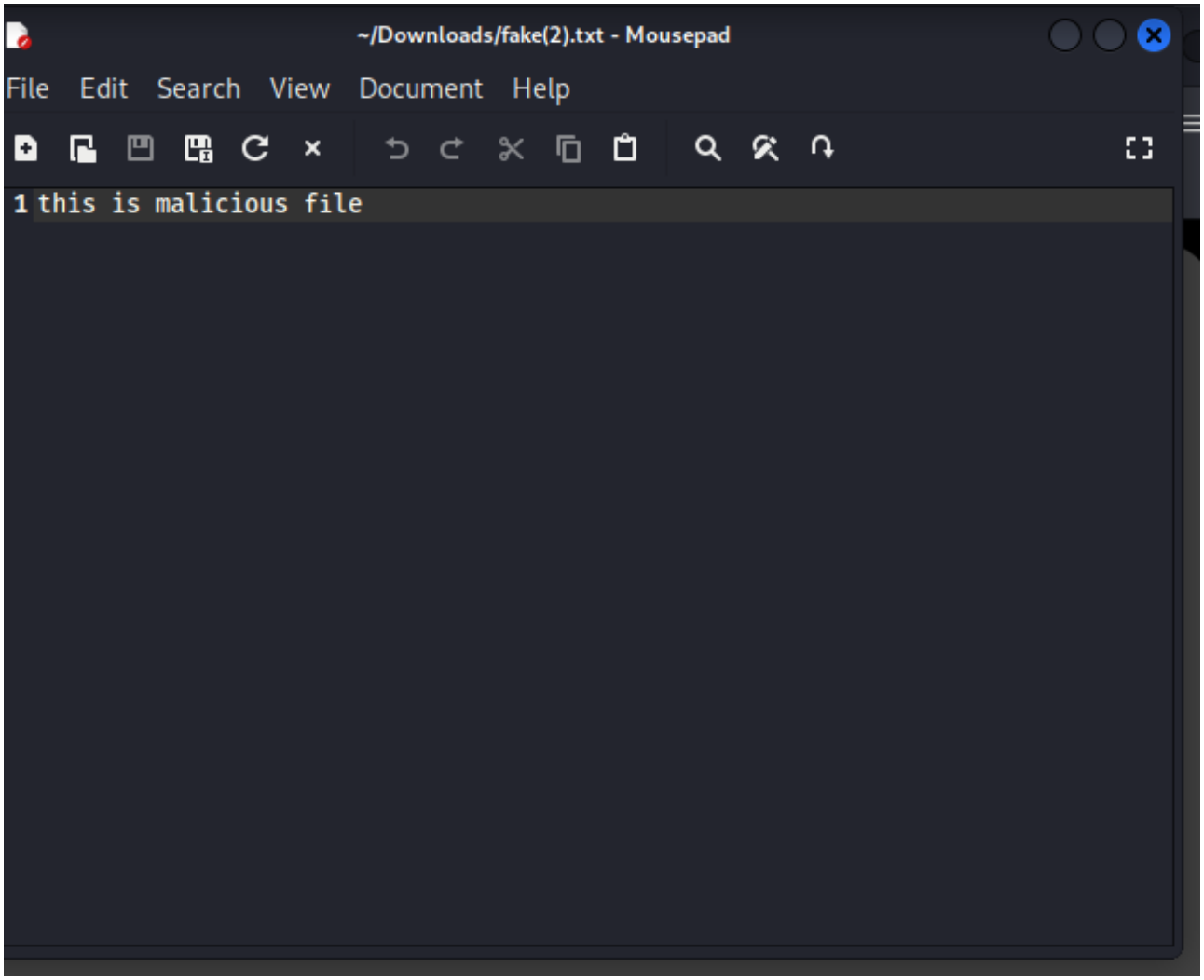
Ta sẽ thực hiện thay thế tên bằng đoạn code vừa rồi



Khi đó web sẽ tải về một file fake



Kiểm tra thì ta thấy được là thông tin đã bị thay đổi



Mức độ: high

Khuyến cáo: Thực hiện filter đầu vào của phần input nhằm chặn các script được truyền vào để tránh bị chèn các lệnh thực thi vào chương trình.

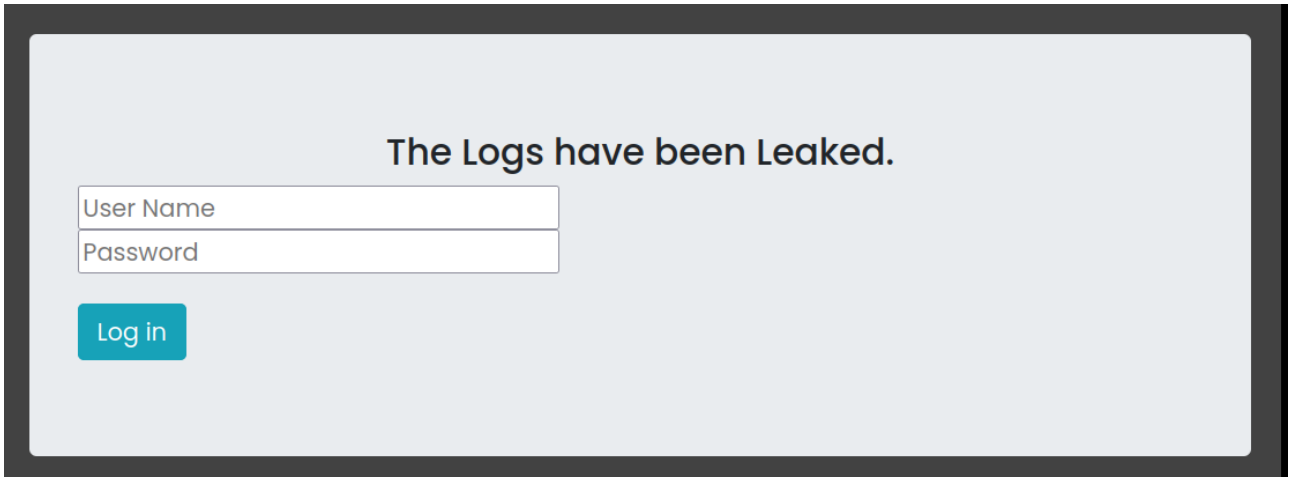
4. Kịch bản 04

#Tiêu đề: Security Logging and Monitoring Failures – information
#Mô tả lỗ hổng:

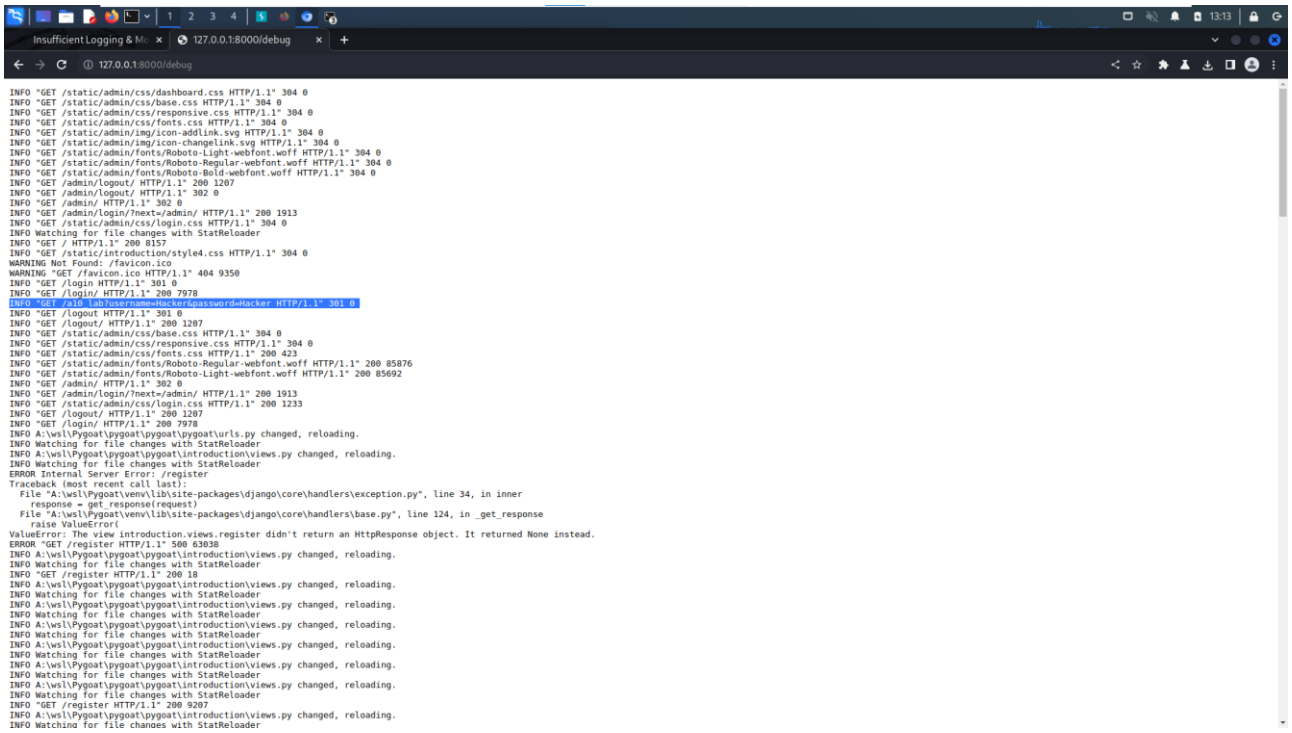
Tóm tắt: thực hiện vào các trang chỉ có admin mới có quyền và khai thác thông tin

Các bước làm

Đầu tiên ta vào trang web để xem



Với gợi ý của câu này thì ta sẽ vào route debug để kiểm tra thông tin thì ta thấy được username và password



Với thông tin này thì ta có thể thực hiện đăng nhập vào trang nhưng do gợi ý của thầy thì bên dưới không có database để login nên ta chỉ có thể khai thác tới đây.

Username=Hacker

Password=Hacker

Mức độ: high

Khuyến cáo: Thực hiện việc phân quyền hữu hạn cho các tài khoản được truy cập vào trang web, ngăn chặn các tài khoản thường truy cập vào những trang chỉ dành cho admin

5. Kịch bản 05

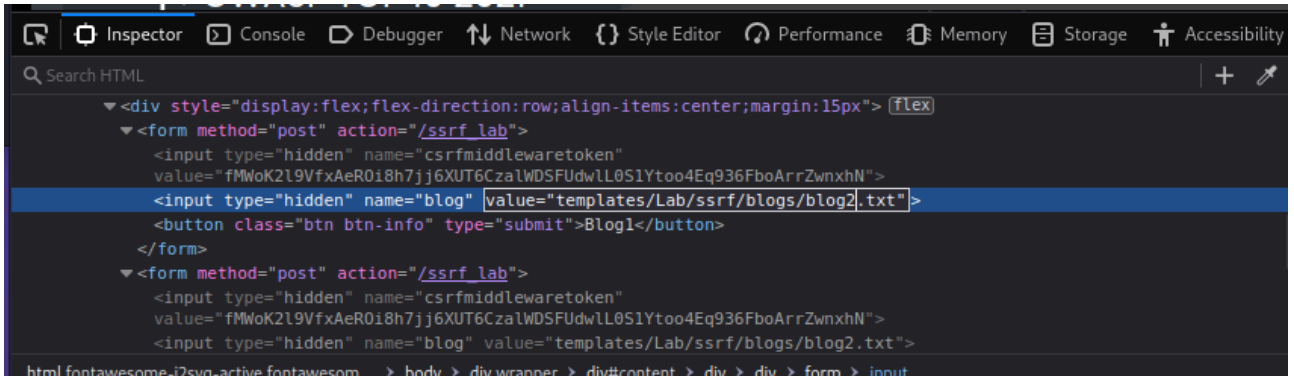
#Tiêu đề: Server-Side Request Forgery (SSRF)
#Mô tả lỗ hổng:

Tóm tắt: Thực hiện kiểm tra các button và thay đổi đường truy cập vào code

Các bước thực hiện

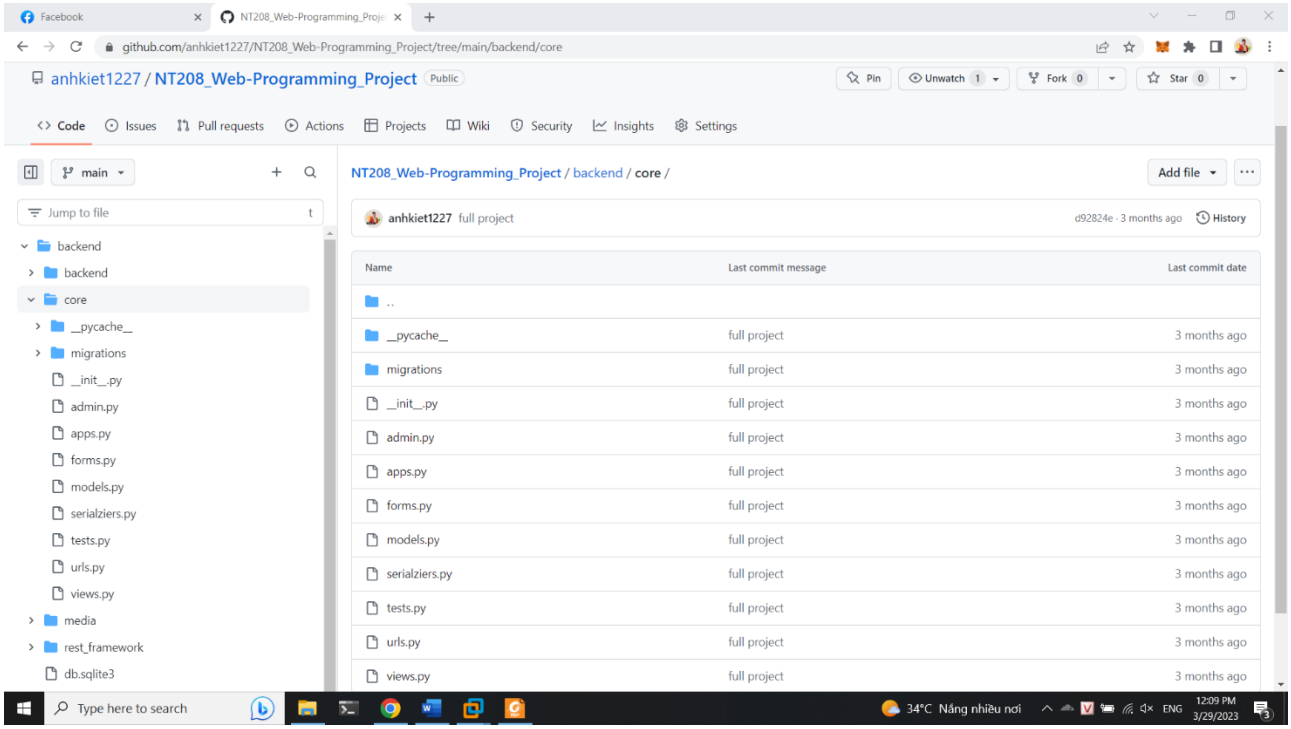
Đầu tiên ta sẽ vào trang để xem thì ta thấy được là khi ấn vào blog1 ta thấy thông tin của blog1

Đầu tiên ta sẽ thay đổi trường thông tin thành blog2 và xem



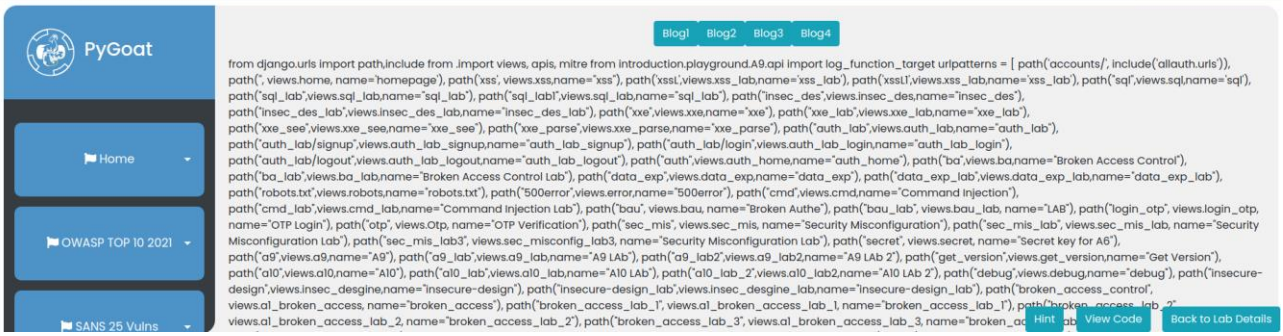
Thì sau khi ấn ta sẽ thấy thông tin trở thành blog2 được thể hiện bên dưới

Như vậy ta sẽ thử các tên của cái file python trong 1 django project

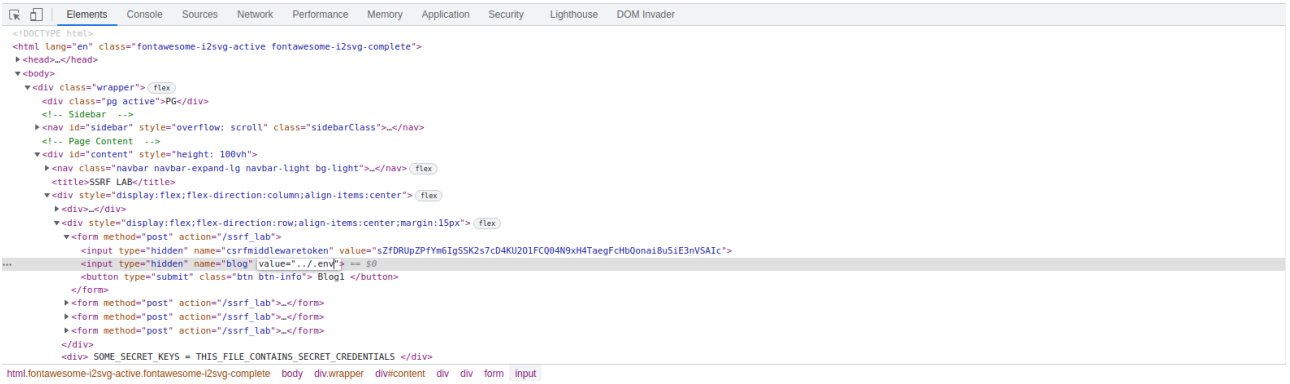


Như ta thấy được là có các file như là admin.py, forms.py, urls.py,... thì ta sẽ thử với urls.py

Ta thấy kết quả trả về như hình bên dưới



Và với gợi ý yêu cầu đề bài là tìm file .env, với quy trình clean code thì thông thường file .env sẽ ở phía trước các folder chứa code python vậy nên phần truyền vào sẽ là ../.env



Sau khi thực hiện click lại blog1 thì ta thấy được secret

Mức độ: high

Khuyến cáo: Thực hiện filter các button khi thực hiện code chương trình thay vì tự động thực hiện

---

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

– YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT