

BÁO CÁO THỰC HÀNH

Môn học: BẢO MẬT WEB VÀ ỨNG DỤNG

Tên chủ đề: Tổng quan các lỗ hổng bảo mật web
thường gặp (phần 2)

GVHD: Ngô Đức Hoàng Sơn

Nhóm: 08

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P12.ANTT

STT	Họ và tên	MSSV	Email
1	Hồ Vĩnh Khánh	22520633	22520633@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng
1	Yêu cầu 1	100%
2	Yêu cầu 2	90%
3	Yêu cầu 3	100%
4	Yêu cầu 4	90%
5	Yêu cầu 5	90%
Điểm tự đánh giá		9.5/10

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

A. A06:2021 – Vulnerable and Outdated Components

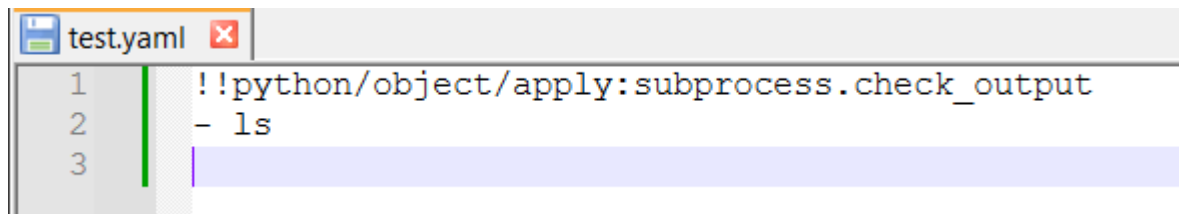
Tiêu đề: Vulnerable and Outdated Components. Tài sản bị ảnh hưởng bởi lỗ hổng này có thể là dữ liệu công ty, ứng dụng và dịch vụ mà công ty đó đang cung cấp, hệ thống mạng, độ tin cậy của công ty đối với người dùng ứng dụng hoặc dịch vụ đó.

Mô tả lỗ hổng:

- Sau một thời gian sử dụng sản phẩm (application, web, ...) nó có thể trở nên lỗi thời và cần phải cập nhật thường xuyên, trong quá trình đó có thể sẽ xuất hiện lỗ hổng này.
- Lỗ hổng xuất hiện khi phần mềm sử dụng các thư viện, frameworks, hoặc các thành phần phụ thuộc khác không được cập nhật lên phiên bản mới nhất hoặc chứa các lỗi bảo mật đã được phát hiện hoặc lỗi giữa các thành phần cập nhật với nhau.

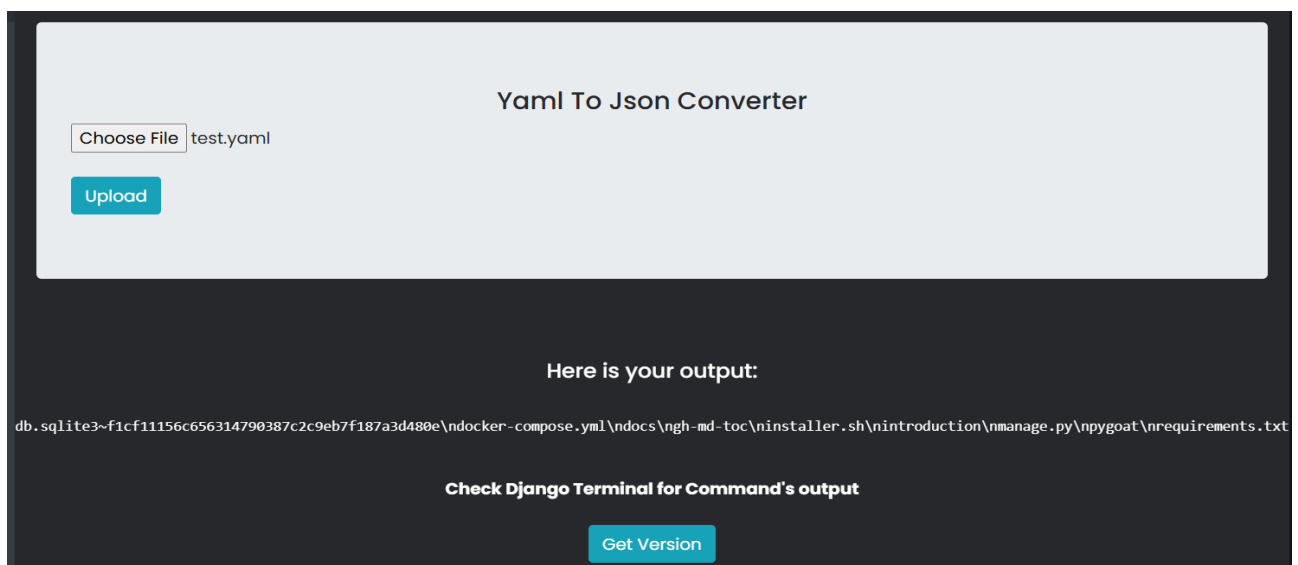
Tóm tắt: Bài lab được cung cấp với tính năng chuyển đổi tập tin yaml thành định dạng json.

- Bước 1: Ta tạo file test.yaml

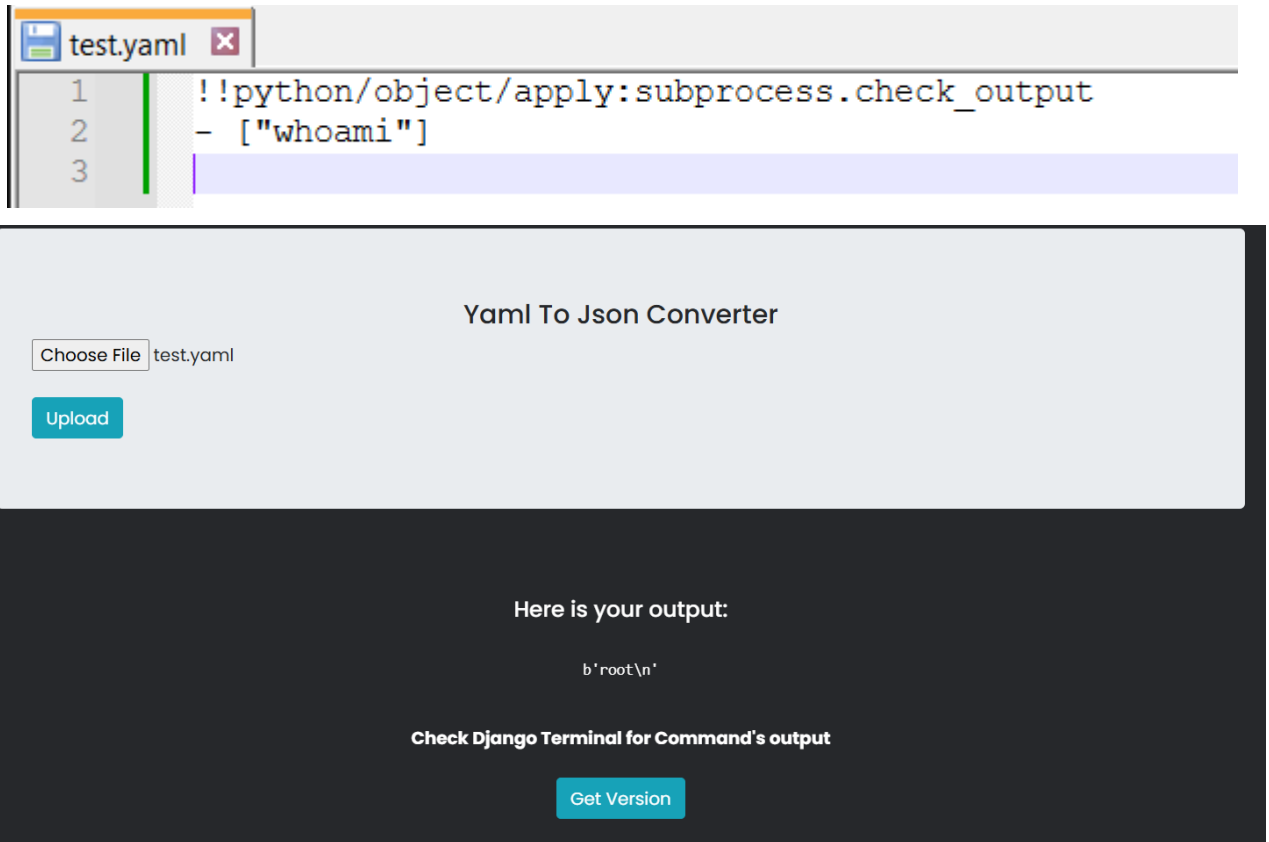


```
1  !!python/object/apply:subprocess.check_output
2  - ls
3
```

- Bước 2: Tiến hành upload file test.yaml lên trang web để chuyển thành file *.json



- Bước 3: Ta thử với lệnh whoami trong file code test.yaml và cho ra kết quả như trên hình



Mức độ ảnh hưởng của lỗ hổng: Khá cao

- Có thể tạo lỗ hổng cho kẻ tấn công và gây ra hậu quả nghiêm trọng như việc đánh cắp thông tin quan trọng và triển khai ransomware.
- Các kẻ tấn công có thể chiếm quyền kiểm soát phần mềm, thêm xóa sửa dữ liệu nhạy cảm trên hệ thống.
- Việc không bảo trì phần mềm có thể vi phạm các quy định về bảo vệ dữ liệu và gây tổn thất nghiêm trọng cho danh tiếng của tổ chức

Khuyến cáo khắc phục:

- Sử dụng phần mềm và các framework bên thứ ba đáng tin cậy
- Thường xuyên cập nhật các ứng dụng hệ thống để kịp thời phát hiện ngăn chặn các lỗ hổng đã bị phát hiện.
- Loại bỏ các phụ thuộc không sử dụng, tính năng, thành phần, tệp tin và tài liệu không cần thiết.
- Chỉ nên lấy các thành phần từ các nguồn chính thống qua các liên kết an toàn.
- Thực hiện các cuộc kiểm tra bảo mật định kỳ để phát hiện sớm các lỗ hổng và giảm thiểu rủi ro

B. A07:2021 – Identification and Authentication Failures

Tiêu đề: Identification and Authentication Failures. Tài sản bị ảnh hưởng có thể là dữ liệu nhạy cảm và thông tin cá nhân, tài khoản người dùng, quyền truy cập, hệ thống hạ tầng mạng và ứng dụng.

Mô tả lỗ hổng: Lỗ hổng này xảy ra khi các hệ thống không đảm bảo hoặc thiếu sót trong việc kiểm soát việc truy cập vào hệ thống, ứng dụng, hoặc dữ liệu. Các vấn đề này có thể dẫn đến việc không xác định hoặc không xác thực đúng người dùng, cho phép kẻ tấn công giả mạo, nâng quyền, hoặc truy cập trái phép vào hệ thống.

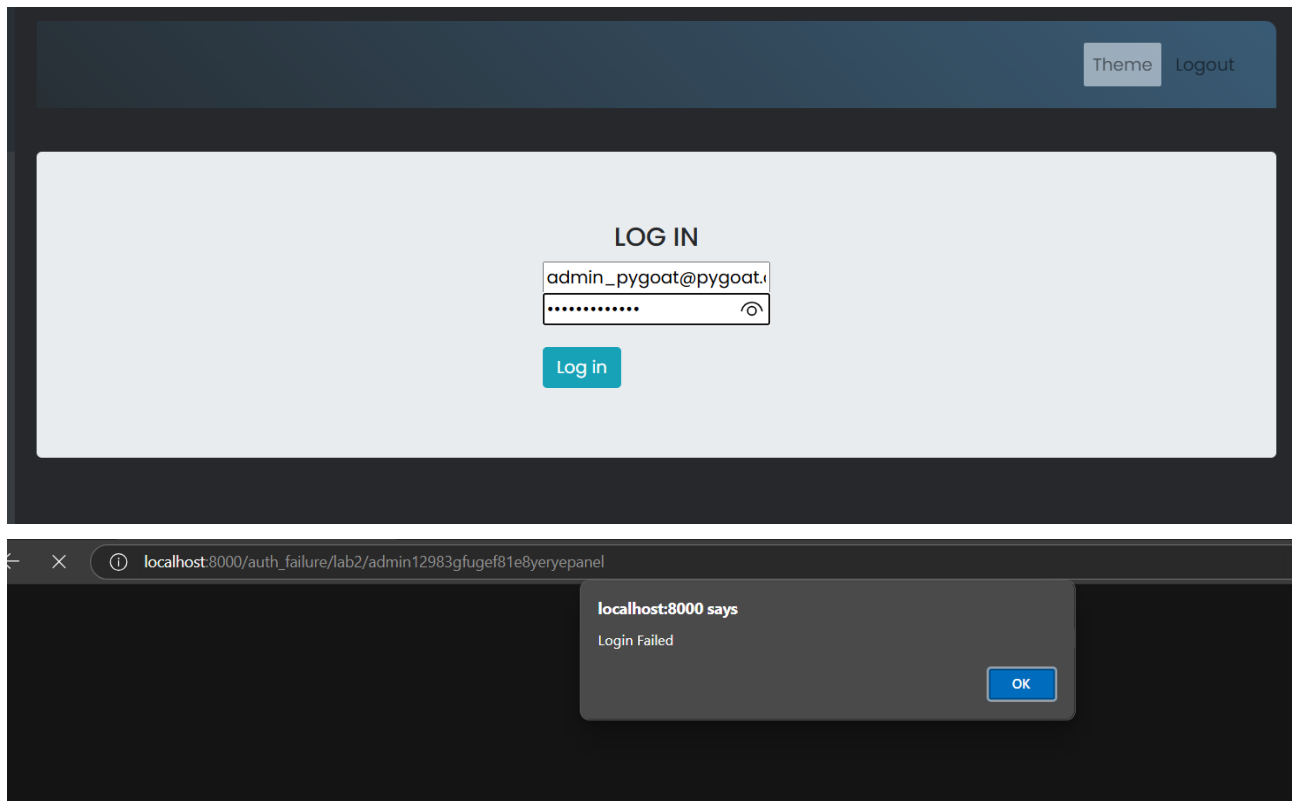
Tóm tắt: Lab cung cấp username cho tài khoản admin cùng với password được hash. Rất khó để đoán hay brute force được từ đoạn hash này. Vậy nên ta sẽ tìm cách để tài khoản admin này bị khoá.

- Bước 1: Kiểm tra code ta thấy nếu ta đăng nhập sai tài khoản admin 5 lần thì tài khoản sẽ bị khoá

```
user = AF_admin.objects.get(username=username)
print(type(user.lockout_cooldown))
if user.is_locked == True and user.lockout_cooldown > datetime.date.today():
    return render(request,"Lab_2021/A7_auth_failure/lab2.html", {"is_locked":True})

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})
```

- Bước 2: Ta thực hiện đăng nhập với username admin_pygoat@pygoat.com mà lab cung cấp. Random mật khẩu để thực hiện đăng nhập 5 lần sai liên tiếp



- Bước 3: Sau khi sai 5 lần tài khoản admin đã bị khoá 24h. Theo code là vậy nhưng thử hoài không blocked =))

Mức độ ảnh hưởng lỗ hổng: Rất cao

- Hệ thống dễ bị tấn công BruteForce
- Gây ảnh hưởng nghiêm trọng đến quyền kiểm soát hệ thống
- Có thể bị đánh cắp các dữ liệu nhạy cảm ảnh hưởng đến uy tín của các công ty, tổ chức

Khuyến cáo khắc phục

- Khuyến cáo thiết lập mật khẩu mạnh và xác thực nhiều yếu tố đối với tài khoản cá nhân. Và đặc biệt bắt buộc đối với các tài khoản nhạy cảm ví dụ như admin
- Ghi log lại các lần thực hiện đăng nhập và cảnh báo cho quản trị viên khi thấy các trường hợp đăng nhập sai nhiều lần
- Không sử dụng bất kỳ thông tin đăng nhập mặc định nào. Đặc biệt là quyền quản trị
- Hạn chế tối thiểu các quyền cho tài khoản
- Giới hạn các lần đăng nhập thất bại.

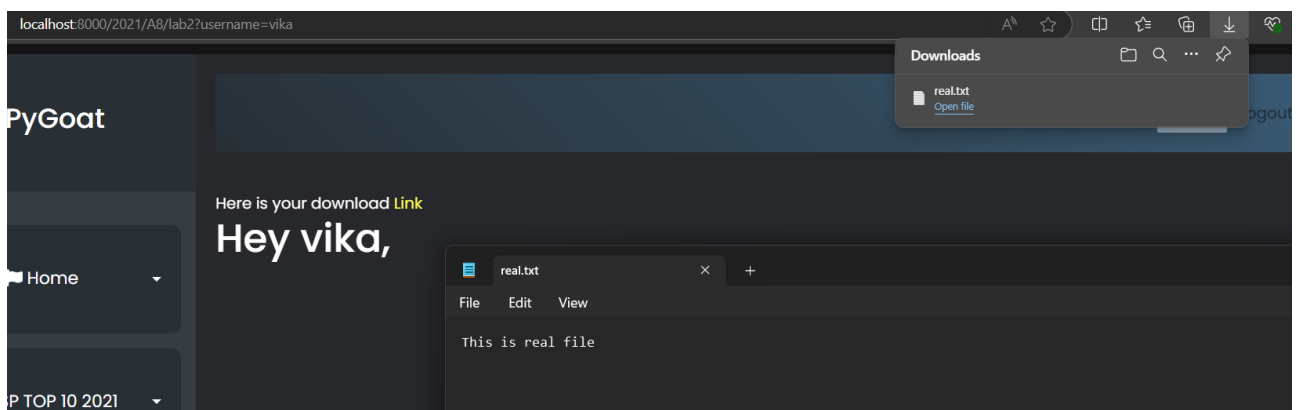
C. A08:2021 – Software and Data Integrity Failures

Tiêu đề: Software and Data Integrity Failures. Tài sản bị ảnh hưởng có thể là dữ liệu hệ thống, thông tin cá nhân, tài khoản người dùng, quyền truy cập, cơ sở hạ tầng mạng của hệ thống.

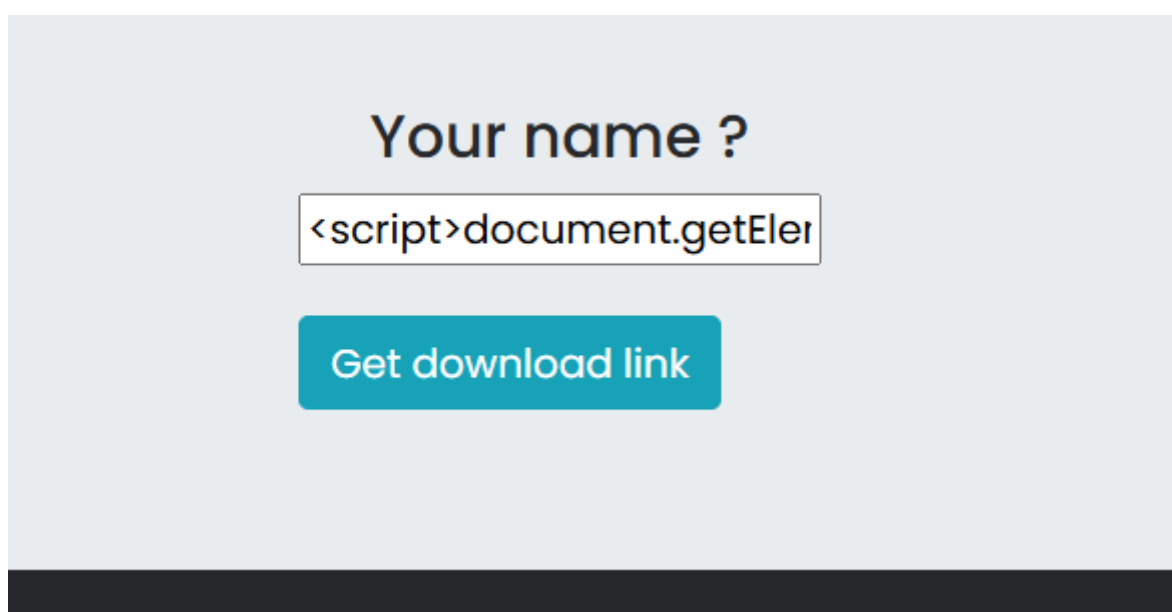
Mô tả lỗ hổng: Lỗ hổng này xảy ra khi phần mềm thiết kế và bảo vệ dữ liệu hệ thống không an toàn, không đảm bảo tính toàn vẹn. Điều này có nghĩa là hacker có thể thay đổi hoặc kiểm soát các thành phần phần mềm và dữ liệu, dẫn đến việc làm sai lệch hoặc lạm dụng hệ thống.

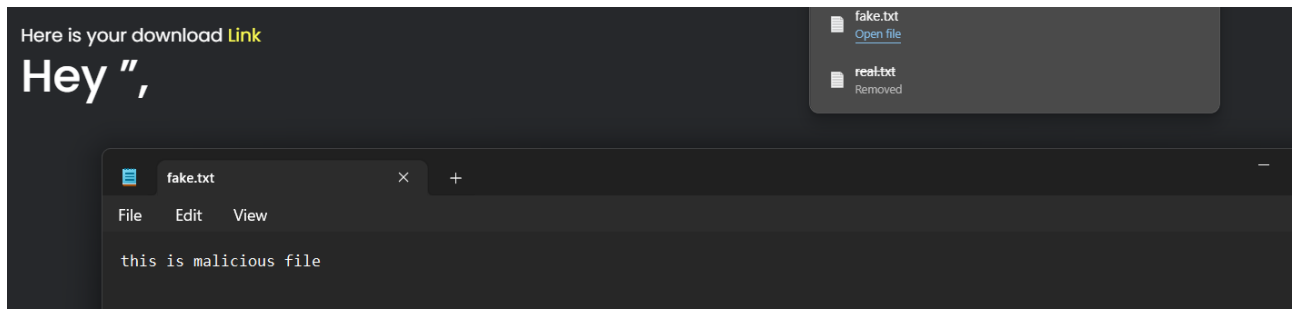
Tóm tắt: Khi truy cập trang, nhập tên xong sẽ có link tải file về. Khi đó ta thực hiện chỉnh sửa, tải file khác về để can thiệp tính toàn vẹn của dữ liệu.

- Bước 1: Truy cập vào trang, nhập tên vào form để tải file và kiểm tra file đã tải về.



- Bước 2: Ta nhập lại vào form bằng 1 đoạn script
“<script>document.getElementById("download_link").href =
"/static/fake.txt";</script>”





⇒ Kiểm tra lại nội dung file ta thấy đường link download ban đầu đã thay đổi. Tải về là 1 file fake có nội dung khác hoàn toàn so với file real. Tức là tính toàn vẹn của file đã bị can thiệp

Mức độ ảnh hưởng của lỗ hổng: Cao

- Dữ liệu không toàn vẹn khiến ứng dụng có thể truy cập đến các file thực thi mã độc, xâm nhập hệ thống
- Tự động cập nhật các bản cập nhật mà không xác minh tính toàn vẹn đầy đủ

Khuyến cáo khắc phục:

- Sử dụng input chặn script, các kí tự lạ
- Áp dụng chữ ký số vào trong việc xác minh phần mềm
- Mã hoá dữ liệu
- Theo dõi các log truy cập đến dữ liệu

D. A09:2021 – Security Logging and Monitoring Failures

Tiêu đề: Security Logging and Monitoring Failures. Tài sản bị ảnh hưởng có thể là các thiết bị IoT, máy chủ, các thiết bị mạng và cơ sở dữ liệu cá nhân của người dùng.

Mô tả lỗ hổng: Lỗi này xảy ra khi thiếu hoặc không có các hoạt động theo dõi, giám sát và ghi nhật ký hoạt động của hệ thống. Điều này dẫn đến khó khăn trong việc phát hiện, điều tra và ngăn chặn các hành vi tấn công mạng, khai thác lỗ hổng của các hacker, có thể gây ra hậu quả nghiêm trọng.

Tóm tắt: Gợi ý cho biết log có thể xem được ở /debug

- Bước 1: Truy cập vào localhost:8000/debug

```
localhost:8000/debug x +
localhost:8000/debug
INFO "GET /static/admin/css/dashboard.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/base.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/responsive.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/fonts.css HTTP/1.1" 304 0
INFO "GET /static/admin/img/icon-addlink.svg HTTP/1.1" 304 0
INFO "GET /static/admin/img/icon-changelink.svg HTTP/1.1" 304 0
INFO "GET /static/admin/fonts/Roboto-Light-webfont.woff HTTP/1.1" 304 0
INFO "GET /static/admin/fonts/Roboto-Regular-webfont.woff HTTP/1.1" 304 0
INFO "GET /static/admin/fonts/Roboto-Bold-webfont.woff HTTP/1.1" 304 0
INFO "GET /admin/logout/ HTTP/1.1" 200 1207
INFO "GET /admin/logout/ HTTP/1.1" 302 0
INFO "GET /admin/ HTTP/1.1" 302 0
INFO "GET /admin/login/?next=/admin/ HTTP/1.1" 200 1913
INFO "GET /static/admin/css/login.css HTTP/1.1" 304 0
INFO Watching for file changes with StatReloader
INFO "GET / HTTP/1.1" 200 8157
INFO "GET /static/introduction/style4.css HTTP/1.1" 304 0
WARNING Not Found: /favicon.ico
WARNING "GET /favicon.ico HTTP/1.1" 404 9350
INFO "GET /login HTTP/1.1" 301 0
INFO "GET /login/ HTTP/1.1" 200 7978
INFO "GET /a10_lab?username=Hacker&password=Hacker HTTP/1.1" 301 0
INFO "GET /logout HTTP/1.1" 301 0
INFO "GET /logout/ HTTP/1.1" 200 1207
INFO "GET /static/admin/css/base.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/responsive.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/fonts.css HTTP/1.1" 200 423
INFO "GET /static/admin/fonts/Roboto-Regular-webfont.woff HTTP/1.1" 200 85876
INFO "GET /static/admin/fonts/Roboto-Light-webfont.woff HTTP/1.1" 200 85692
INFO "GET /admin/ HTTP/1.1" 302 0
INFO "GET /admin/login/?next=/admin/ HTTP/1.1" 200 1913
INFO "GET /static/admin/css/login.css HTTP/1.1" 200 1233
INFO "GET /logout/ HTTP/1.1" 200 1207
INFO "GET /login/ HTTP/1.1" 200 7978
INFO A:\wsl\Pygoat\pygoat\pygoat\urls.py changed, reloading.
INFO Watching for file changes with StatReloader
INFO A:\wsl\Pygoat\pygoat\pygoat\introduction\views.py changed, reloading.
INFO Watching for file changes with StatReloader
ERROR Internal Server Error: /register
Traceback (most recent call last):
  File "A:\wsl\Pygoat\venv\lib\site-packages\django\core\handlers\exception.py", line 34, in inner
    response = get_response(request)
  File "A:\wsl\Pygoat\venv\lib\site-packages\django\core\handlers\base.py", line 124, in _get_response
    raise ValueError(
ValueError: The view introduction.views.register didn't return an HttpResponse object. It returned None instead.
ERROR "GET /register HTTP/1.1" 500 63038
INFO A:\wsl\Pygoat\pygoat\pygoat\introduction\views.py changed, reloading.
INFO Watching for file changes with StatReloader
INFO "GET /register HTTP/1.1" 200 18
INFO A:\wsl\Pygoat\pygoat\pygoat\introduction\views.py changed, reloading.
INFO Watching for file changes with StatReloader
```

- Bước 2: Ta có thể tìm thấy được username là Hacker và password là Hacker

```
INFO "GET /login HTTP/1.1" 301 0
INFO "GET /login/ HTTP/1.1" 200 7978
INFO "GET /a10_lab?username=Hacker&password=Hacker HTTP/1.1" 301 0
INFO "GET /logout HTTP/1.1" 301 0
INFO "GET /logout/ HTTP/1.1" 200 1207
INFO "GET /static/admin/css/base.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/responsive.css HTTP/1.1" 304 0
```

- Bước 3: Trở lại đăng nhập bằng account Hacker:Hacker. Nhưng không có gì nữa cả :))

Mức độ ảnh hưởng: Cao

- Gây hậu quả nghiêm trọng cho hệ thống vì để lộ thông tin username và password. Nặng hơn nữa có thể mất cắp các tài liệu mật, nhạy cảm

- Các hacker có thể thực hiện tấn công mạng làm gián đoạn dịch vụ
- Rò rỉ thông tin cá nhân khách hàng gây thiệt hại về tài sản và cả uy tín, danh dự

Khuyến cáo khắc phục:

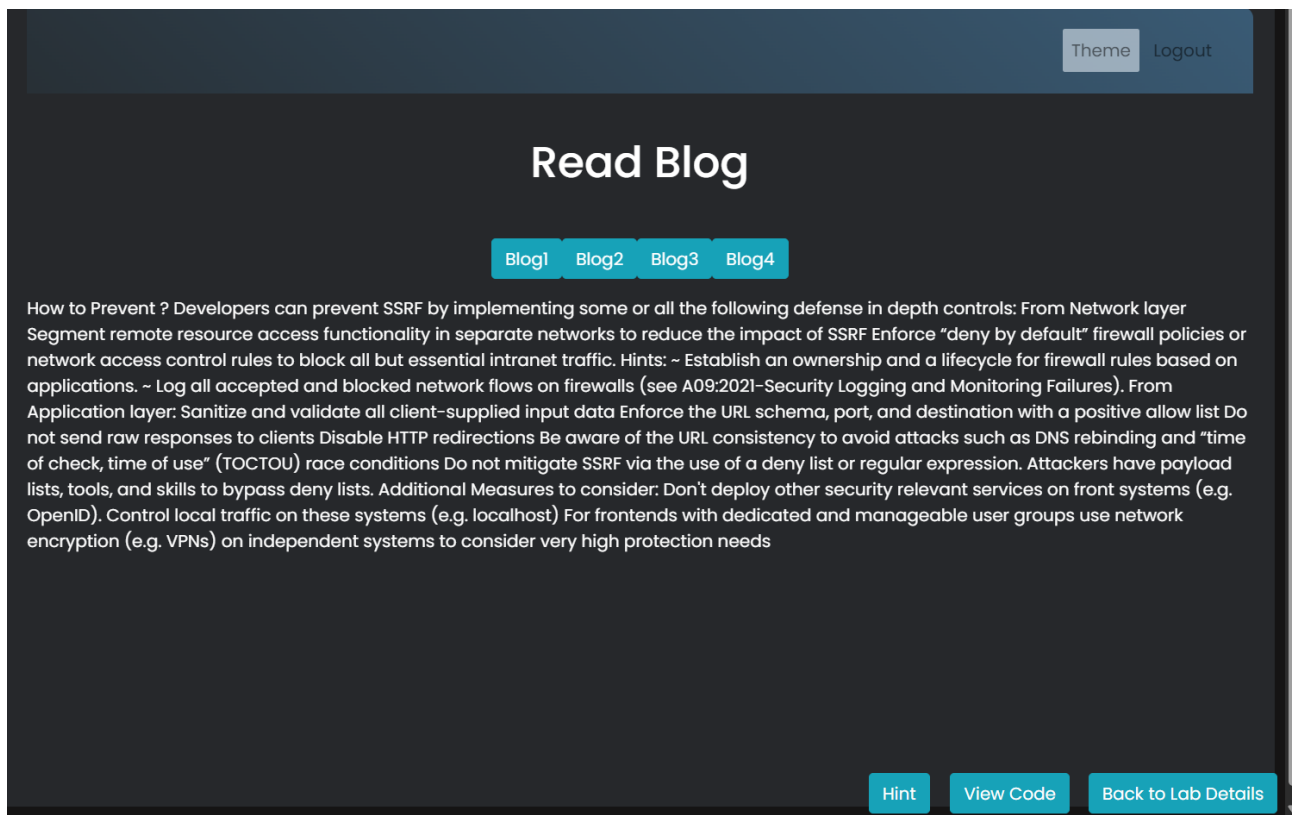
- Tăng cường giám sát, ghi lại và quản lý nhật ký hoạt động
- Triển khai các biện pháp bảo vệ, ngăn chặn việc truy cập vào các dữ liệu cá nhân, tài liệu nhạy cảm
- Đảm bảo nhật ký ghi hoạt động lạ toàn vẹn không bị giả mạo
- Kiểm soát truy cập, quản lý các dữ liệu đầu vào cần xác thực

E. A10:2021 – Server-Side Request Forgery (SSRF)

Tiêu đề: Server-Side Request Forgery (SSRF). Tài sản có thể bị ảnh hưởng là thông tin cá nhân của người dùng và cơ sở dữ liệu.

Mô tả lỗ hổng: Lỗ hổng này xảy ra khi các ứng dụng web không thực hiện đầy đủ các biện pháp xác thực URL do người dùng cung cấp để đảm bảo chỉ những người dùng được phép mới có thể truy cập vào tài nguyên và chức năng của hệ thống.

Tóm tắt: Có 4 button ứng với 4 blog, mỗi khi ấn vào thì trang sẽ load lại để lấy thông tin của blog tương ứng.



- Bước 1: F12 để xem thì thấy rằng thông tin sẽ được load lên từ 1 file txt tương ứng.

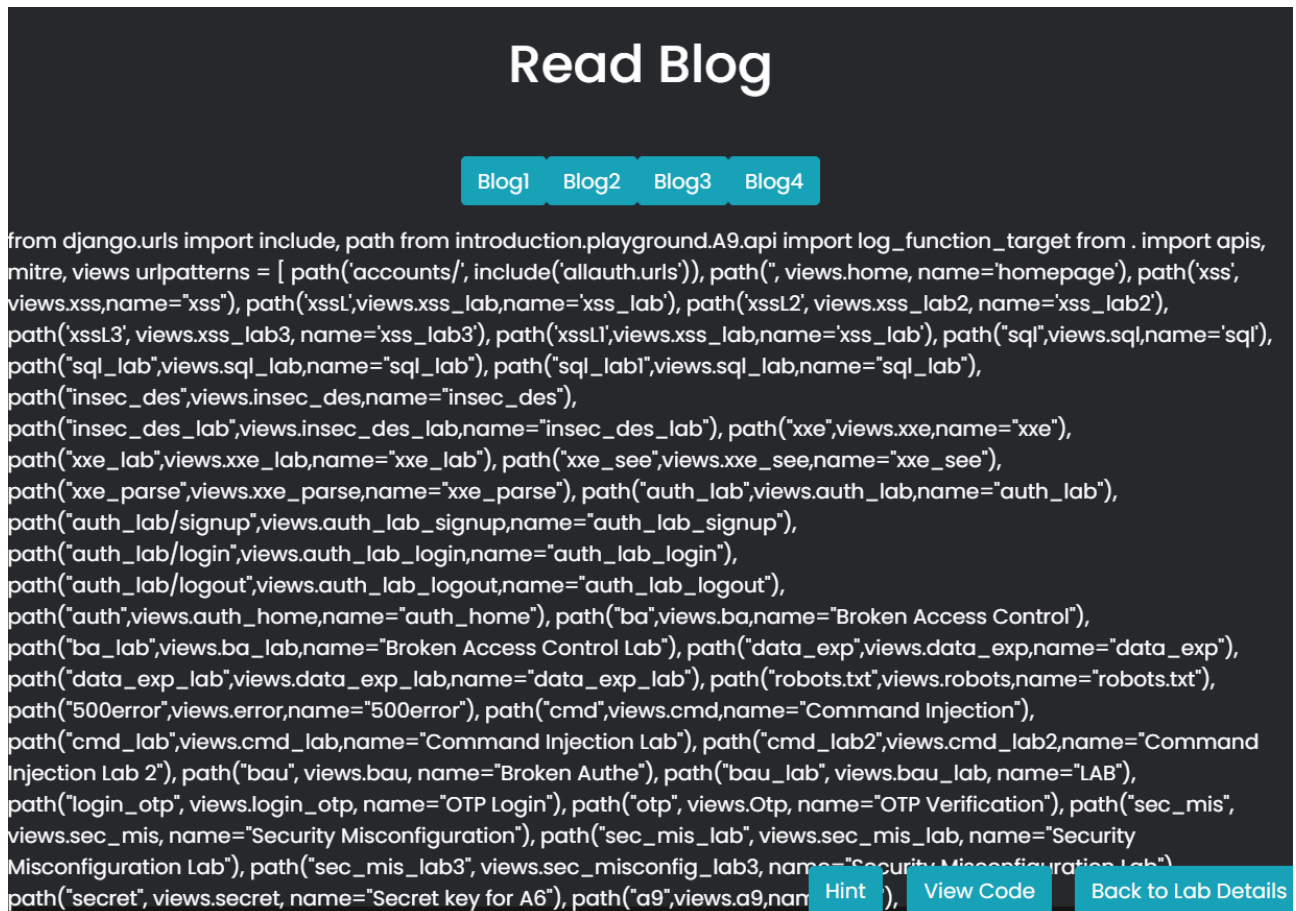
```
<div style="display:flex;flex-direction:column;align-items:center">
  <div>
    <h1> Read Blog </h1>
    <br>
  </div>
  <div style="display:flex;flex-direction:row;align-items:center;margin:15px">
    <form method="post" action="/ssrf_lab">
      <input type="hidden" name="csrfmiddlewaretoken" value="RMh0L5PHNwLs4aTdZkKe3akPKz7DJwgPIGsGlyBhpSAuYQOARBJ8rNYSqhSdNeWs">
      <input type="hidden" name="blog" value="templates/Lab/ssrf/blogs/blog1.txt">
      <button type="submit" class="btn btn-info"> Blog1 </button>
    </form>
    <form method="post" action="/ssrf_lab">
      <input type="hidden" name="csrfmiddlewaretoken" value="RMh0L5PHNwLs4aTdZkKe3akPKz7DJwgPIGsGlyBhpSAuYQOARBJ8rNYSqhSdNeWs">
      <input type="hidden" name="blog" value="templates/Lab/ssrf/blogs/blog2.txt">
      <button type="submit" class="btn btn-info"> Blog2 </button>
    </form>
    <form method="post" action="/ssrf_lab">
      <input type="hidden" name="csrfmiddlewaretoken" value="RMh0L5PHNwLs4aTdZkKe3akPKz7DJwgPIGsGlyBhpSAuYQOARBJ8rNYSqhSdNeWs">
      <input type="hidden" name="blog" value="templates/Lab/ssrf/blogs/blog3.txt">
      <button type="submit" class="btn btn-info"> Blog3 </button>
    </form>
    <form method="post" action="/ssrf_lab">
      <input type="hidden" name="csrfmiddlewaretoken" value="RMh0L5PHNwLs4aTdZkKe3akPKz7DJwgPIGsGlyBhpSAuYQOARBJ8rNYSqhSdNeWs">
      <input type="hidden" name="blog" value="templates/Lab/ssrf/blogs/blog4.txt">
      <button type="submit" class="btn btn-info"> Blog4 </button>
    </form>
  </div>
</div>
```

- Bước 2: Sử dụng phần mềm Burp Suite để chặn gói tin. Hoặc có thể sửa ngay trên code trong inspect

```
<div>
  <form method="post" action="/ssrf_lab">
    <input type="hidden" name="csrfmiddlewaretoken" value="itiwd
teFUjymmHYDGzVYDYBNOM1zdLmrMntcNW0fwFnoglV0YQUS1BfQuuM9ht2
4">
    <input type="hidden" name="blog" value="urls.py">
    <button type="submit" class="btn btn-info"> Blog1 </button>
  </form>
  <form method="post" action="/ssrf_lab">...</form>
  <form method="post" action="/ssrf_lab">...</form>
  <form method="post" action="/ssrf_lab">...</form>
</div>
```

- Bước 3: Chuyển qua Reapter và thay đổi giá trị \$blog=urls.py để đọc file urls.py có trong cây thư mục của Django

The screenshot displays the Burp Suite interface. On the left, the 'Request' tab shows a POST request to `/ssrf_lab` with a `Content-Type: application/x-www-form-urlencoded`. The request body contains a `csrfmiddlewaretoken` and a `blog` parameter set to `urls.py`. The main pane shows the 'Response' tab, which is a 200 OK response from `localhost:8000`. The response body is an HTML page titled 'Read Blog' with a sidebar containing links to 'OWASP TOP 10 2021', 'SANS 25 Vulns', and 'Mitre top 25 Vulns'. The right pane shows the 'Inspector' tab, which displays the request body parameters, including the `csrfmiddlewaretoken` and the `blog` parameter set to `urls.py`.



- Bước 4: Để tìm file .env ta thử lần lượt .env, ../.env, ../../.env. Nhưng trong bài này ta không thấy file .env

Mức độ ảnh hưởng: Cao

- Dữ liệu nhạy cảm bị truy cập trái phép ví dụ như file .env trên
- Hacker có thể truy cập và đánh cắp dữ liệu nhạy cảm của người dùng, thông tin đăng nhập, dữ liệu cá nhân.
- Truy cập vào hệ thống và mạng nội bộ, thực hiện các hành vi tấn công như chiếm quyền điều khiển hệ thống, cài đặt phần mềm độc hại, hoặc phá hoại dữ liệu

Khuyến cáo khắc phục:

- Xác thực và lọc URL.
- Xác minh đa yếu tố khi đăng nhập
- Giới hạn lần đăng nhập sai và gửi cảnh báo về cho người quản trị
- Đặt mật khẩu mạnh với nhiều điều kiện như: Trên 8 ký tự, có chữ hoa và thường, có số và cả ký tự đặc biệt.
- Chỉ cấp quyền truy cập vào tài nguyên và chức năng của ứng dụng cho những người dùng cần thiết.

--HẾT--