BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 2: Top 10 OWASP part 2

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Võ Sỹ Minh	21521146	21521146@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%
4	Bài tập 4	100%
5	Bài tập 5	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

Bài tập 1. A06:2021 – Vulnerable and Outdated Components

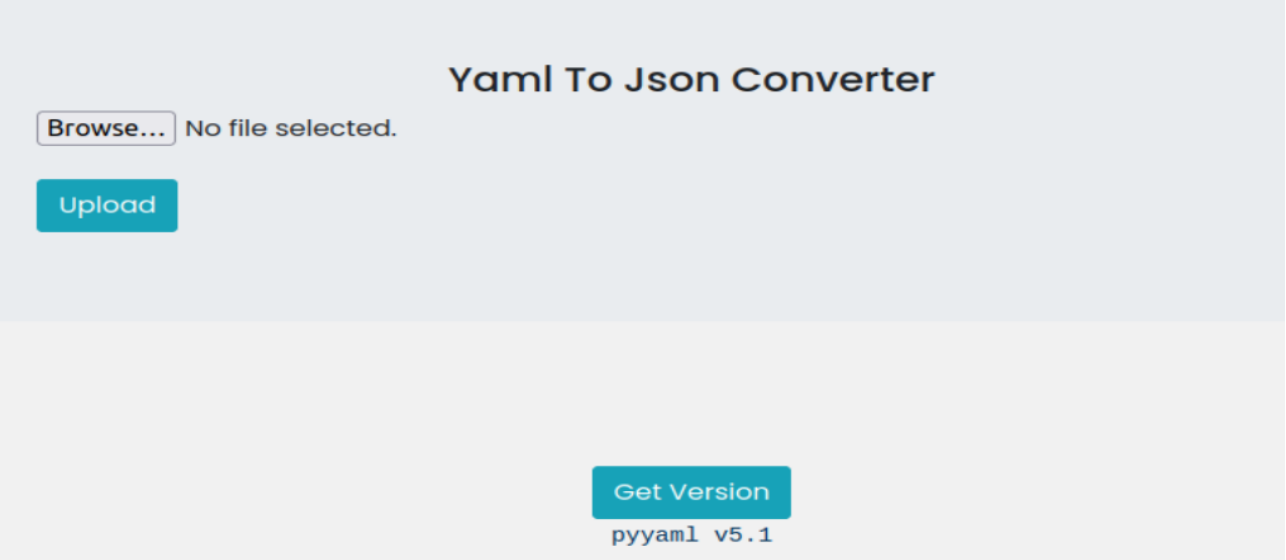
Tiêu đề: Vulnerable and Outdated Components.

Tài sản bị ảnh hưởng: dữ liệu, thông tin

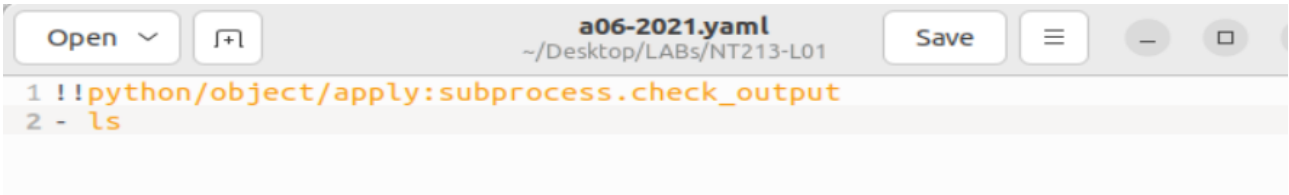
Mô tả lỗ hổng: "Vulnerable and Outdated Components" trong ứng dụng web là một vấn đề phổ biến khi ứng dụng sử dụng các thành phần (components) cũ và có lỗ hổng bảo mật, hoặc không được cập nhật đầy đủ.

Trong trường hợp này, việc sử dụng một công cụ chuyển đổi từ định dạng YAML sang JSON mà không kiểm tra dữ liệu đầu vào kỹ, cho phép tấn công việc thực thi mã từ tệp YAML.

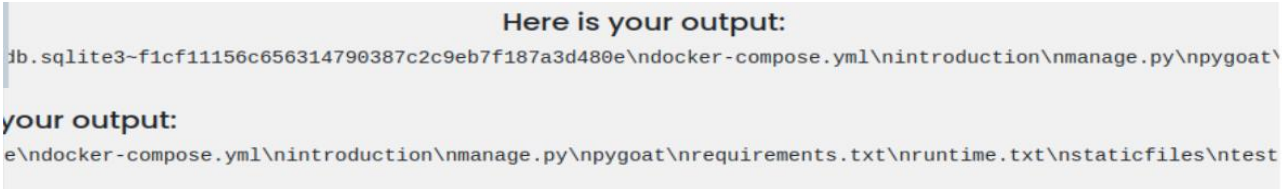
Phiên bản công cụ đã cũ



Khai thác lỗ hổng này bằng file yaml như sau:



Lệnh được tiêm thông qua file yaml được thực thi



Mức độ ảnh hưởng của lỗ hổng: high

Tác động bảo mật nào mà kẻ tấn công có thể đạt được: Kẻ tấn công có thể thực thi code độc hại để tìm kiếm thông tin bảo mật được lưu trữ trên server.
Khuyến cáo khắc phục:
- Cập nhật components: Đảm bảo rằng tất cả các omponent của ứng dụng, bao gồm cả thư viện và framework, đều được cập nhật lên phiên bản mới nhất.
- Kiểm tra mã đầu vào: Thực hiện kiểm tra nghiêm ngặt dữ liệu đầu vào từ người dùng, đặc biệt là các dữ liệu có thể được chuyển đổi hoặc xử lý bởi các thành phần cũ hay có lỗ hổng.
- Giới hạn quyền truy cập
- Sử dụng thư viện chuyển đổi an toàn

Bài tập 2. A07:2021 – Identification and Authentication Failures

Tiêu đề: Identification and Authentication Failures.
Tài sản bị ảnh hưởng: quyền truy cập tài khoản
Mô tả lỗ hổng: "Identification and Authentication Failures" trong ứng dụng web xảy ra khi hệ thống không thực hiện đủ biện pháp xác thực và nhận dạng người dùng một cách an toàn.

Trong trường hợp này, trang web cung cấp tài khoản admin và mật khẩu được lưu dưới dạng hash. Tuy không đăng nhập nhưng attacker vẫn có thể thực hiện các cuộc tấn công phá hoại để chặn tài khoản admin truy cập trong một khoảng thời gian nhất định.

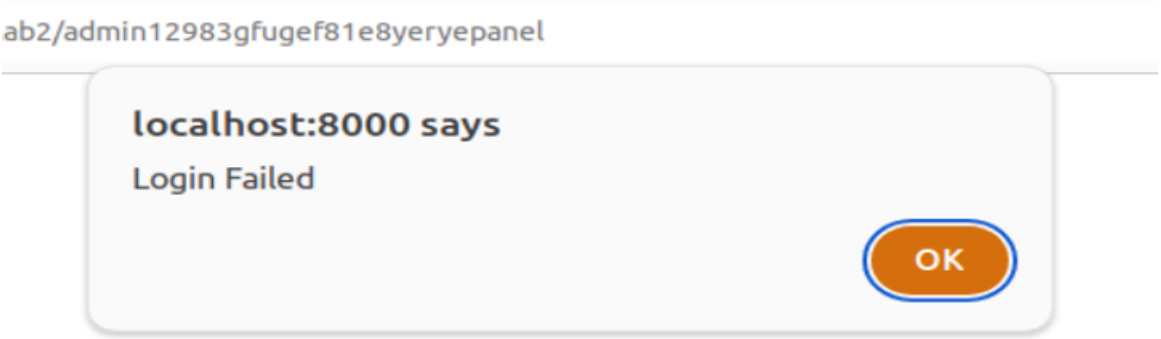
Các bước thực hiện:

Ở trang đăng nhập, có thể xem code:
Nếu đăng nhập thất bại đủ 5 lần sẽ block user 1440 phút. Với username recon được thì có thể chặn đăng nhập của admin bằng cách đăng nhập thất bại 5 lần.

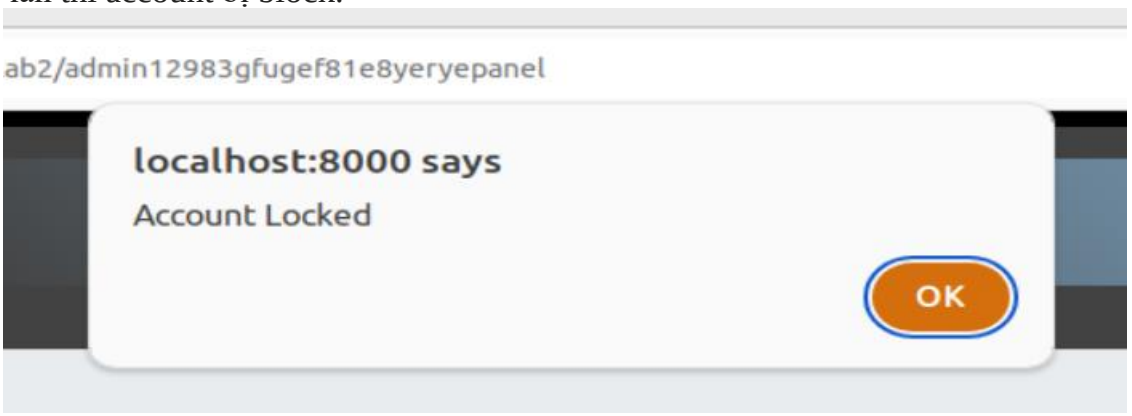
```
        fail_attempt = user.failattempt + 1
        if fail_attempt == 5:
          user.is_active = False
          user.failattempt = 0
          user.is_locked = True
          user.lockout_cooldown = datetime.datetime.now() + datetime.timedelta(minutes=1440)
          user.save()
          return render(request,"Lab_2021/A7_auth_failure/lab2.html", {"user":user,
"success":False,"failure":True, "is_locked":True})
```

Ghi mật khẩu ngẫu nhiên để đăng nhập thất bại

Login Failed



Sau 5 lần thì account bị block.



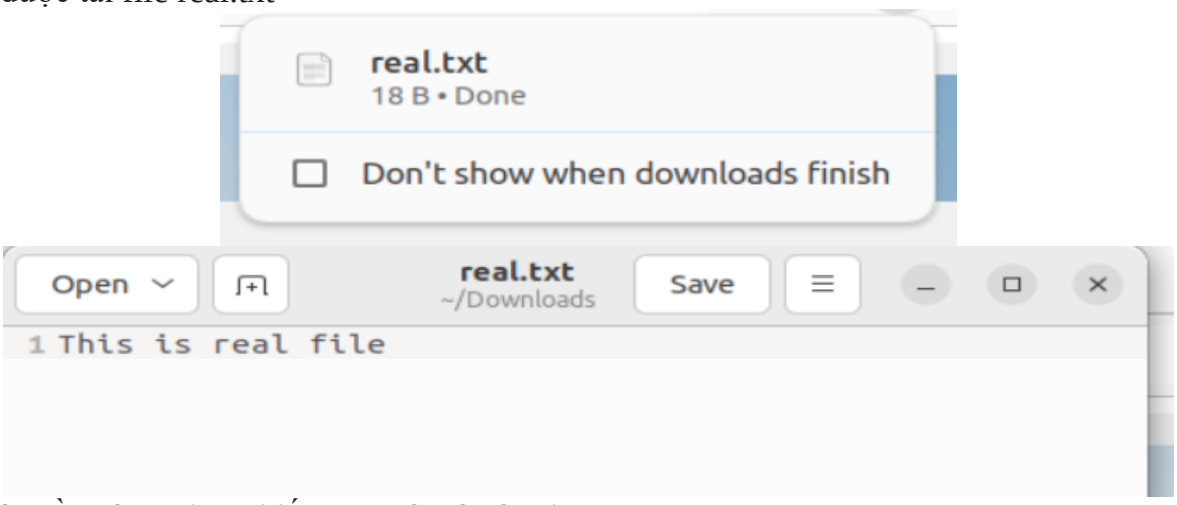
Mức độ ảnh hưởng: high
Tác động bảo mật mà kẻ tấn công có thể đạt được: Kẻ tấn công có thể tiến hành tấn công DOS vào trang web và chặn quyền truy cập của các user bình thường.
Khuyến cáo khắc phục:
- Sử dụng các phương pháp xác thực mạnh mẽ như hai yếu tố xác thực (2FA) hoặc mã thông báo xác thực một lần (OTP).
- Thực hiện quản lý tài khoản bằng cách theo dõi, kiểm soát và quản lý quyền truy cập của tài khoản admin. Đảm bảo rằng các tài khoản không sử dụng hoặc có nguy cơ bị chiếm đoạt được vô hiệu hóa hoặc xóa bỏ

Bài tập 3: A08:2021 – Software and Data Integrity Failures
Tiêu đề: Software and Data Integrity Failures.
Tài sản bị ảnh hưởng: dữ liệu, tính toàn vẹn
Mô tả lỗ hổng: "Software and Data Integrity Failures" xảy ra khi người tấn công tận dụng các lỗ hổng trong phần mềm hoặc quy trình để can thiệp vào tính toàn vẹn của dữ liệu. Trong trường hợp này, khi người dùng truy cập vào trang web và tải xuống một tệp dữ liệu, kẻ tấn công sẽ thực hiện việc chỉnh sửa nội dung của tệp này, sau đó tải lên một tệp mới đã được chỉnh sửa để can thiệp vào tính toàn vẹn dữ liệu.

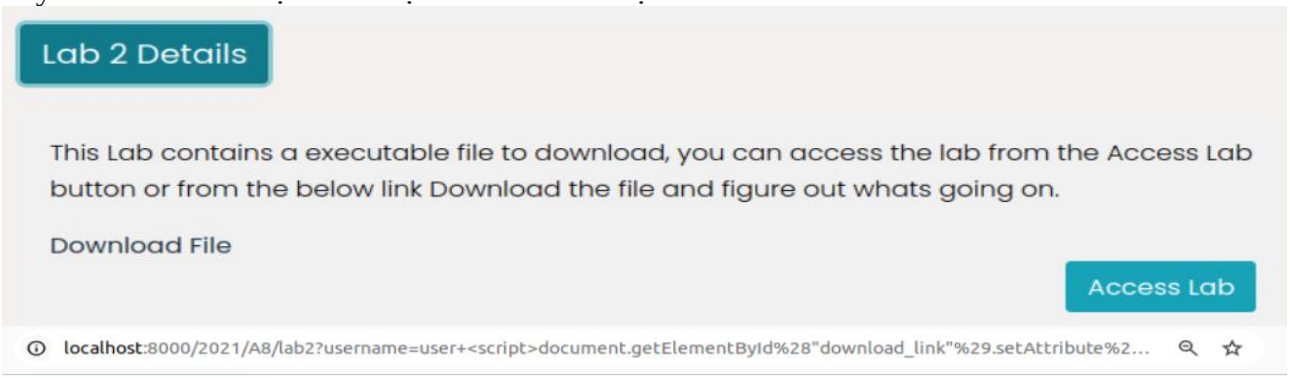
Các bước thực hiện:

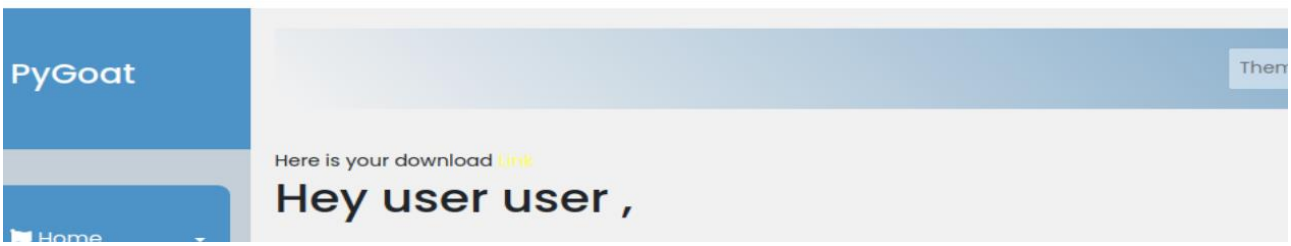
Sử dụng username bình thường

Tải được tải file real.txt

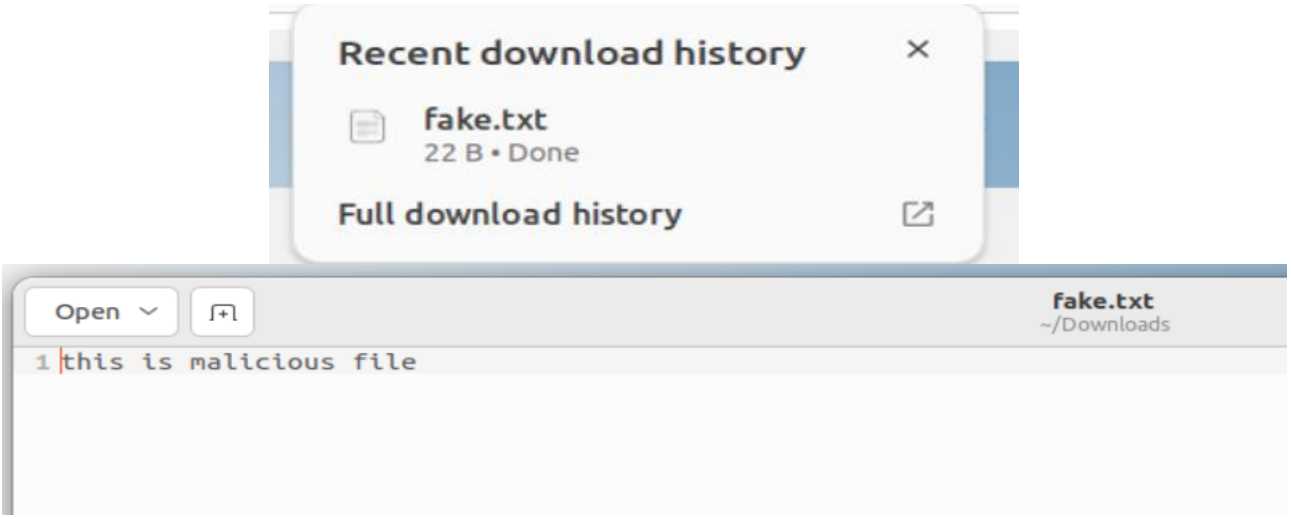


Ở yêu cầu bài ta được biết mục tiêu là vào được link sau:





Và tải được file fake.txt



Phân tích url mục tiêu:
http://localhost:8000/2021/A8/lab2?username=user+%3Cscript%3Edocument.getElementById%28%22download_link%22%29.setAttribute%28%22href%22%2C%22%2Fstatic%2Ffake.txt%22%29%3B%3C%2Fscript%3E

Thấy rằng username bằng với một đoạn script sau khi decode như sau thì ta có thể mở được trang chứa đường dẫn download như yêu cầu.

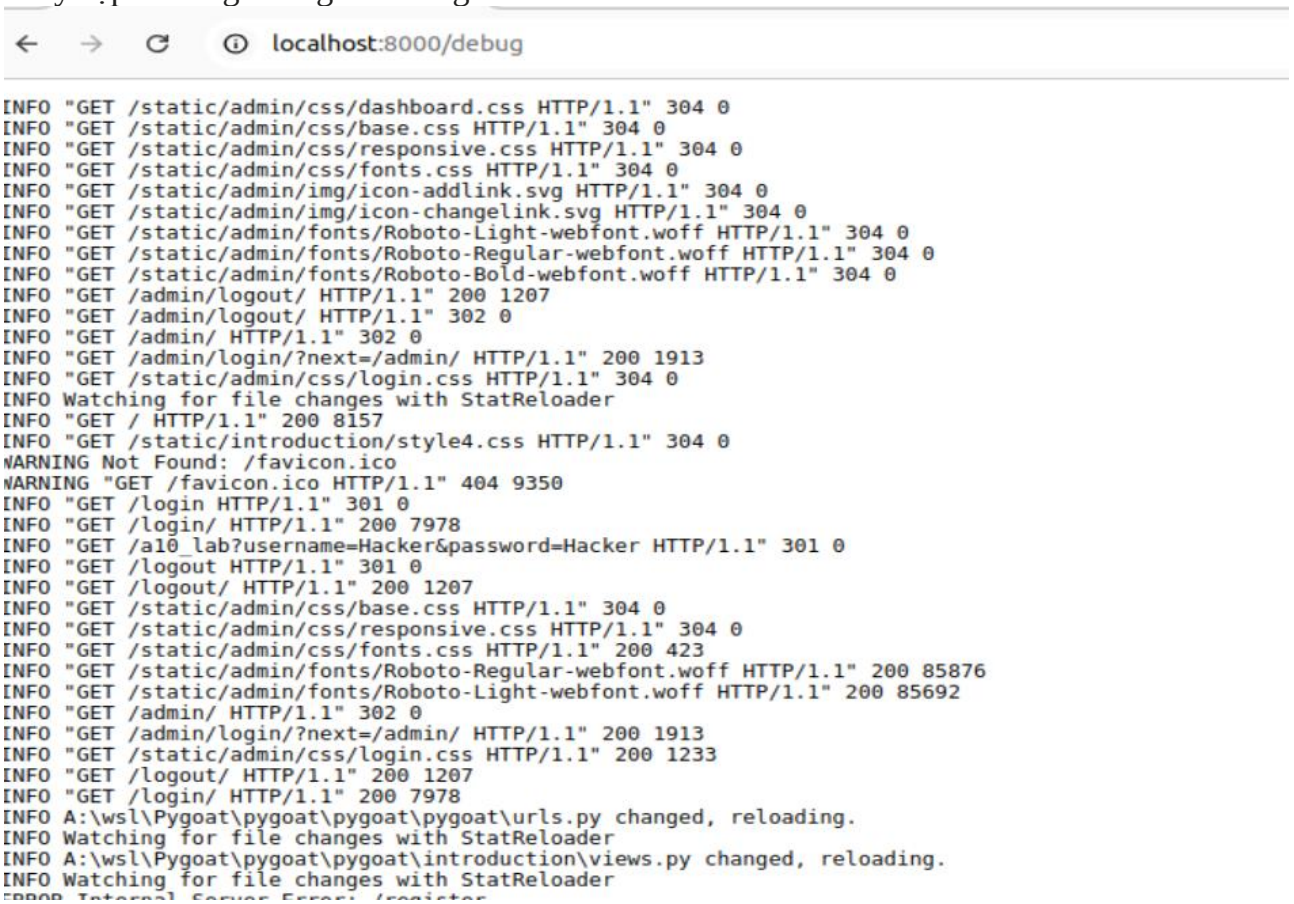
<script>document.getElementById("download_link")?.setAttribute("href", "/static/fake.txt");</script>

Mức độ ảnh hưởng: high
Tác động bảo mật: Kẻ tấn công có thể lợi dụng lỗ hổng này để thực hiện các cuộc tấn công như thay đổi dữ liệu, triển khai mã độc hại hoặc gây ra sự cố cho hệ thống bằng cách sửa đổi mã nguồn hoặc dữ liệu quan trọng.
Khuyến cáo khắc phục:
- Thực hiện các biện pháp kiểm tra tính toàn vẹn của dữ liệu sau khi nó đã được tải lên hệ thống. Sử dụng chữ ký số hoặc các cơ chế tương tự để xác minh phần mềm hoặc dữ liệu đến từ nguồn dự kiến và không bị thay đổi.
- Kiểm tra và xác thực mọi dữ liệu trước khi chấp nhận và xử lý, đảm bảo rằng chỉ dữ liệu hợp lệ mới được chấp nhận.

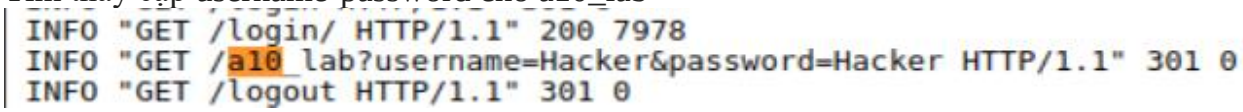
Bài tập 4: A09:2021 – Security Logging and Monitoring Failures
Tiêu đề: Security Logging and Monitoring Failures.
Tài sản bị ảnh hưởng: thông tin, dữ liệu ghi trong log
Mô tả lỗ hổng: "Security Logging and Monitoring Failures" xảy ra khi hệ thống không thực hiện việc ghi log và giám sát hoạt động của người dùng một cách đầy đủ hoặc hiệu quả. Trong trường hợp này, kẻ tấn công có thể thực hiện các hành động tấn công trên các trang chỉ có quyền truy cập của admin mà không để lại dấu vết trong các hệ thống ghi log hoặc không bị phát hiện thông qua giám sát hoạt động.

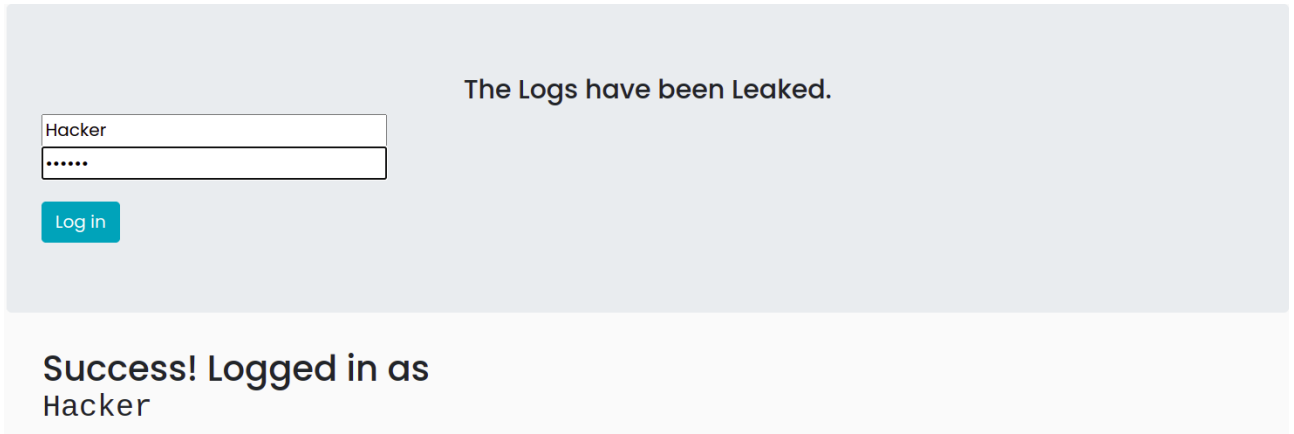
Các bước thực hiện:

Truy cập vào log bebug của trang web



Tìm thấy cặp username-password cho a10_lab





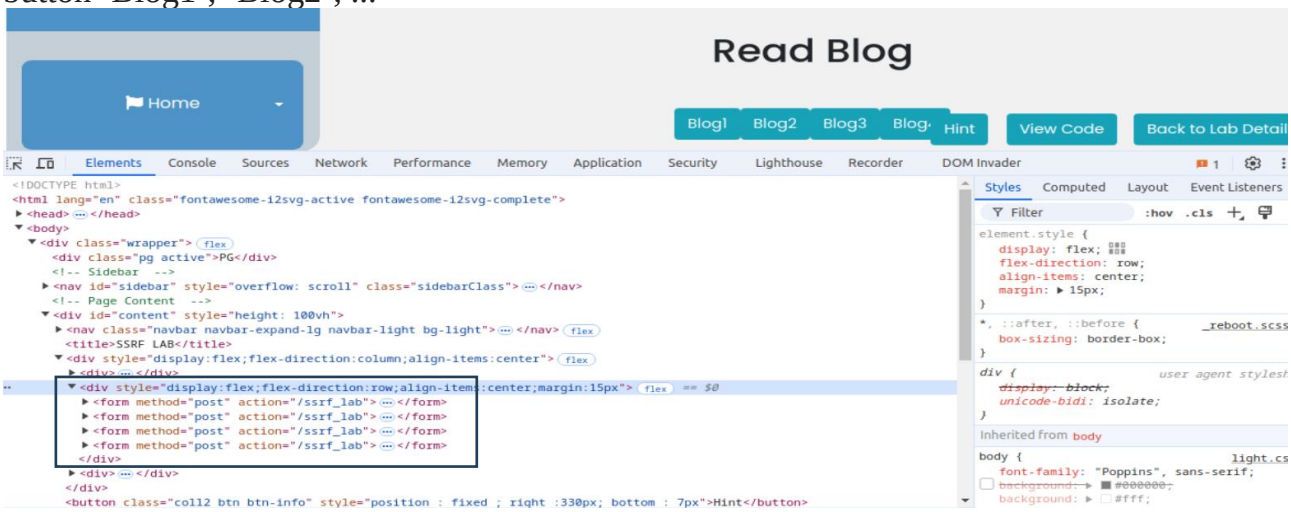
Mức độ ảnh hưởng: high

Tác động bảo mật: Kẻ tấn công có thể tận dụng lỗ hổng này để thực hiện các cuộc tấn công mà không bị phát hiện hoặc bị truy kích. Họ có thể thực hiện các hành động độc hại như khai thác lỗ hổng bảo mật, đánh cắp dữ liệu nhạy cảm, ...

Khuyến cáo khắc phục:
- Đảm bảo các log được mã hóa chính xác để ngăn chặn việc tiêm nhiễm hoặc tấn công vào hệ thống ghi log hoặc giám sát.
- Sử dụng các biện pháp xác thực hai yếu tố (2FA) và hạn chế quyền truy cập theo nguyên tắc "tối thiểu quyền hạn".

Bài tập 5: A10:2021 – Server-Side Request Forgery (SSRF)
Tiêu đề: Server-Side Request Forgery (SSRF).
Tài sản bị ảnh hưởng: các tập tin nội bộ của server.
Mô tả lỗ hổng: Lỗ hổng "Server-Side Request Forgery (SSRF)" xảy ra khi kẻ tấn công có thể tạo ra các yêu cầu từ máy chủ đến các địa chỉ mà họ kiểm soát, thậm chí có thể là các hệ thống nội bộ hoặc không công khai. Trong tình huống này, kẻ tấn công thường sử dụng các yêu cầu này để khai thác hoặc tấn công các hệ thống khác trong mạng nội bộ hoặc bên ngoài.
Các bước thực hiện:

Tìm kiếm các component thực hiện các phương thức post/ get để khai thác, ở đây là các button ‘Blog1’, ‘Blog2’, ...



Sau khi xem cấu trúc của button ‘Blog1’ thì thấy trường ‘value’ chứa đường dẫn đến file blog. Thông qua đây ta có thể xem thông tin của các file lưu trữ ở server.

Với gợi ý của bài là file ‘.env’ thì mục tiêu là đọc file ‘.env’ tuy nhiên file này không có trong thư mục này và thông thường là ở bên ngoài của thư mục project, cuối cùng thì file này nằm trước thư mục templates ‘../.env’.

Sau khi chỉnh, nhấn vào button 'Blog1', đọc file '.env' thành công

Mức độ ảnh hưởng: high
Tác động bảo mật:
- Đọc dữ liệu từ máy chủ nội bộ: Kẻ tấn công có thể sử dụng SSRF để đọc dữ liệu từ máy chủ nội bộ, bao gồm các tệp cục bộ, thông tin kết nối và cấu hình hệ thống nội bộ. Điều này có thể tiết lộ thông tin nhạy cảm hoặc cung cấp thông tin cần thiết cho các cuộc tấn công tiếp theo.
- Tấn công truy cập vào dịch vụ nội bộ: Kẻ tấn công có thể sử dụng SSRF để tạo ra các yêu cầu HTTP hoặc các loại yêu cầu khác đến các dịch vụ nội bộ, chẳng hạn như giao thức FTP, SSH, Redis, hoặc MongoDB, có thể dẫn đến việc tấn công trực tiếp lên các dịch vụ này.
- Phạm vi của cuộc tấn công từ xa: SSRF có thể được sử dụng như một điểm vào mạng nội bộ từ xa, cho phép kẻ tấn công khai thác các lỗ hổng khác trong mạng nội bộ hoặc tạo ra các cuộc tấn công từ xa khác.
Khuyến cáo khắc phục:
- Xác thực và kiểm tra đầu vào: Đảm bảo rằng tất cả các URL được chấp nhận từ người dùng đều được kiểm tra kỹ lưỡng và chỉ chấp nhận các URL hợp lệ.
- Hạn chế quyền truy cập: Hạn chế quyền truy cập của ứng dụng đến các tài nguyên nội bộ và chỉ cho phép truy cập vào các tài nguyên cần thiết.
- Sử dụng whitelist thay vì blacklist: Thay vì chỉ định các tài nguyên không được phép truy cập, nên sử dụng whitelist để chỉ định các tài nguyên được phép truy cập

---

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

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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 .DOCX và .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]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- 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 bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

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

HẾT