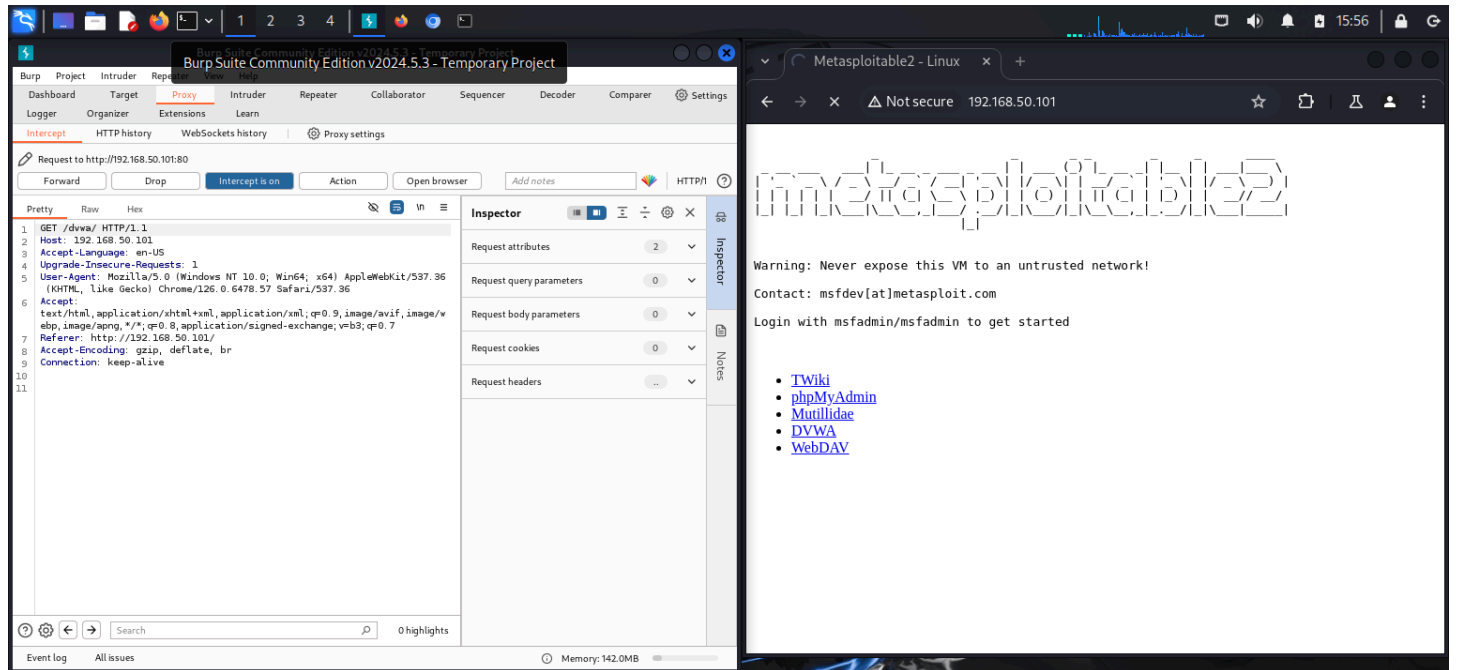
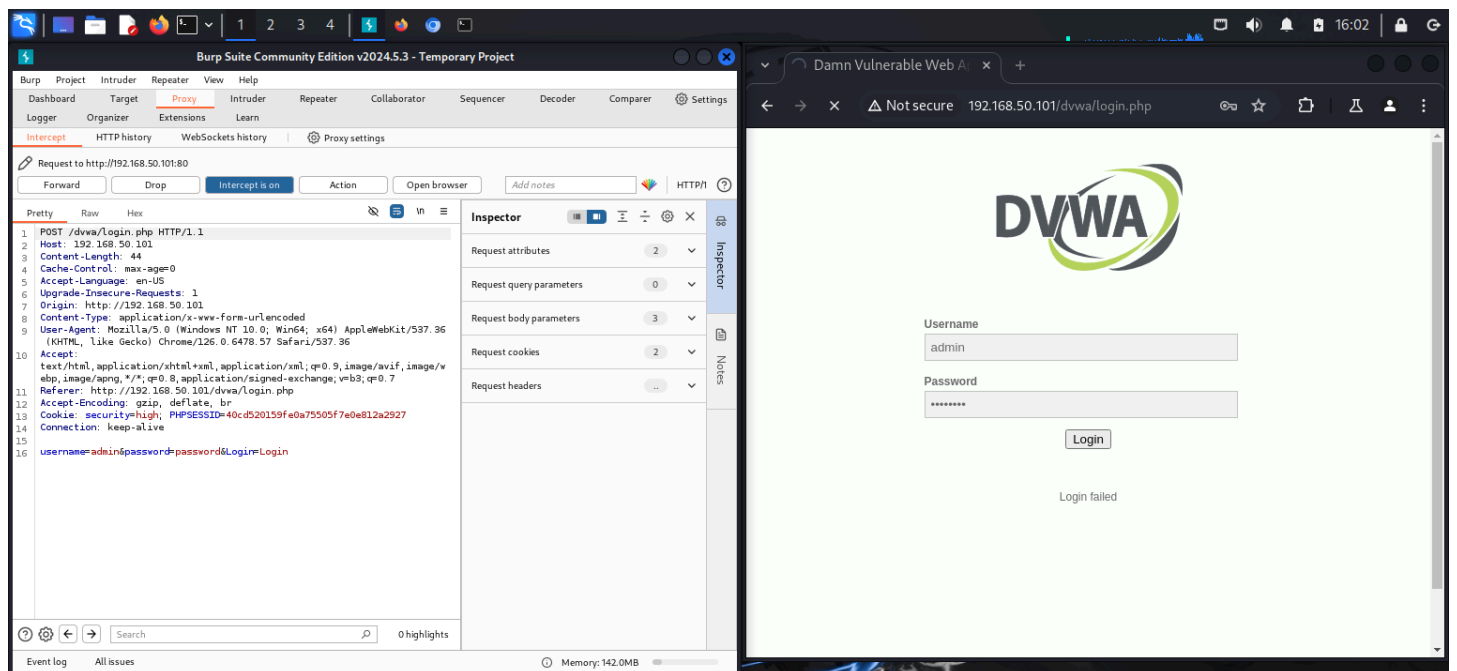


S6L1 - Exploit File Upload

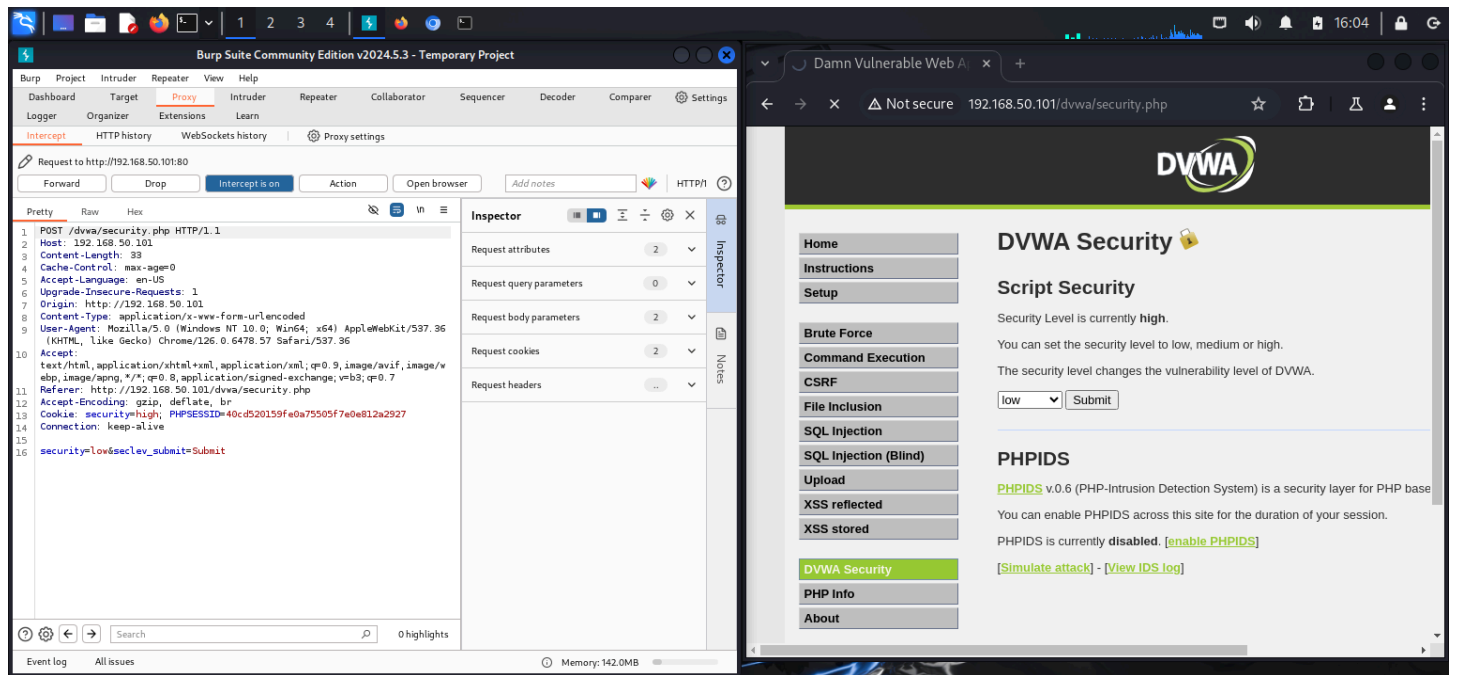
Forward dopo il collegamento al sito di Metasploitable



Forward dopo l'inserimento delle credenziali



Forward dopo il cambio del livello di sicurezza



The screenshot shows the Burp Suite Community Edition v2024.5.3 interface on the left and the DVWA Security page on the right. In Burp Suite, a POST request to `http://192.168.50.101:80/dvwa/security.php` is intercepted. The request body contains a `security=low&seclev_submit=Submit` parameter. The DVWA Security page shows the security level is currently high, with a dropdown menu set to low and a Submit button.

Burp Suite Request Details:

```
1 POST /dvwa/security.php HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 92
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.50.101
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
10 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
11 Referer: http://192.168.50.101/dvwa/security.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; PHPSESSID=40cd520159fe0a75505f7e0e812a2927
14 Connection: keep-alive
15
16 security=low&seclev_submit=Submit
```

DVWA Security Page:

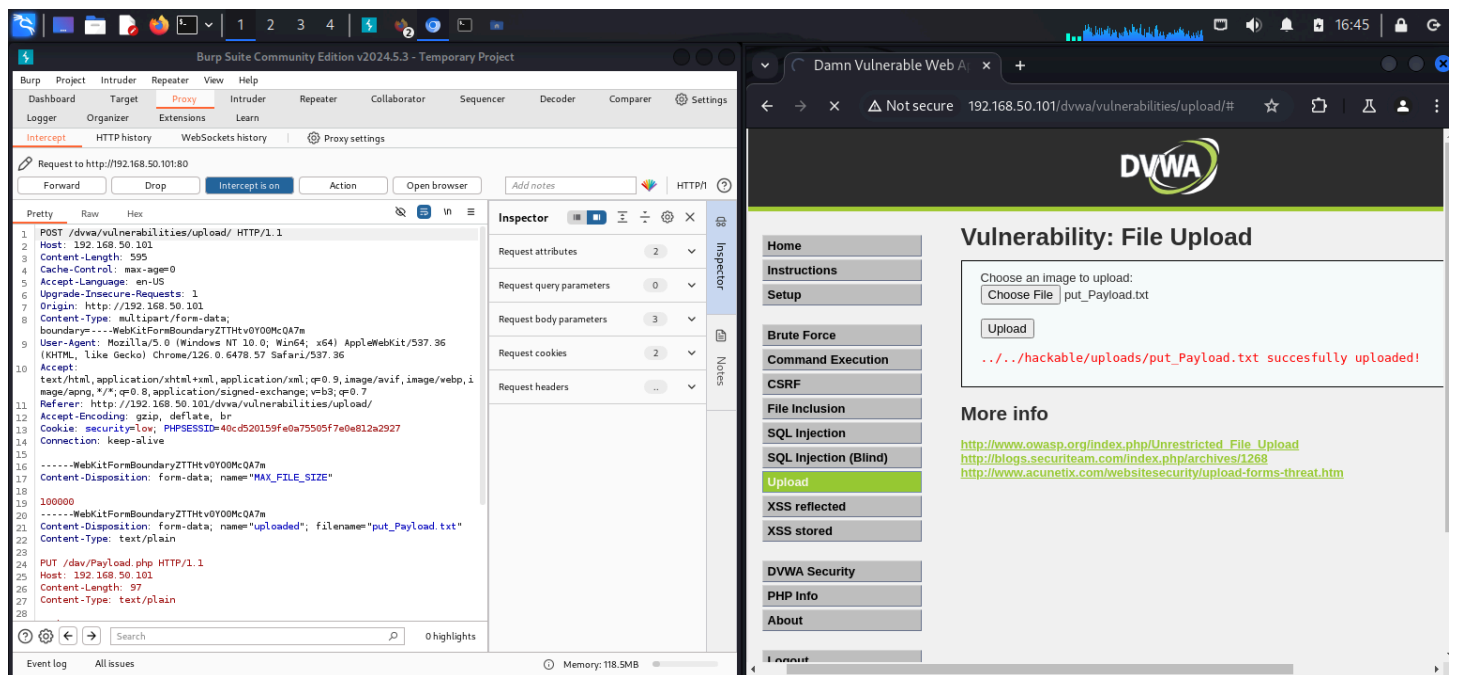
Security Level is currently high.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

Forward dopo il caricamento del file



The screenshot shows the Burp Suite Community Edition v2024.5.3 interface on the left and the DVWA File Upload page on the right. In Burp Suite, a POST request to `http://192.168.50.101:80/dvwa/vulnerabilities/upload/` is intercepted. The request body contains a `put_Payload.txt` file. The DVWA File Upload page shows the file `put_Payload.txt` successfully uploaded.

Burp Suite Request Details:

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 595
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.50.101
8 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZTTHtV0Y00McQA7m
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=40cd520159fe0a75505f7e0e812a2927
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryZTTHtV0Y00McQA7m
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryZTTHtV0Y00McQA7m
21 Content-Disposition: form-data; name="uploaded"; filename="put_Payload.txt"
22 Content-Type: text/plain
23
24
25 PUT /dav/Payload.php HTTP/1.1
26 Host: 192.168.50.101
27 Content-Length: 97
28 Content-Type: text/plain
```

DVWA File Upload Page:

Choose an image to upload:

Choose File put_Payload.txt

Upload

.../hackable/uploads/put_Payload.txt successfully uploaded!

Effettiva aggiunta e caricamento del file sul sito

