Esercitazione W13D1 - Pratica 1

Exploit File Upload

Fabio Benevento - 30/01/2024

Traccia

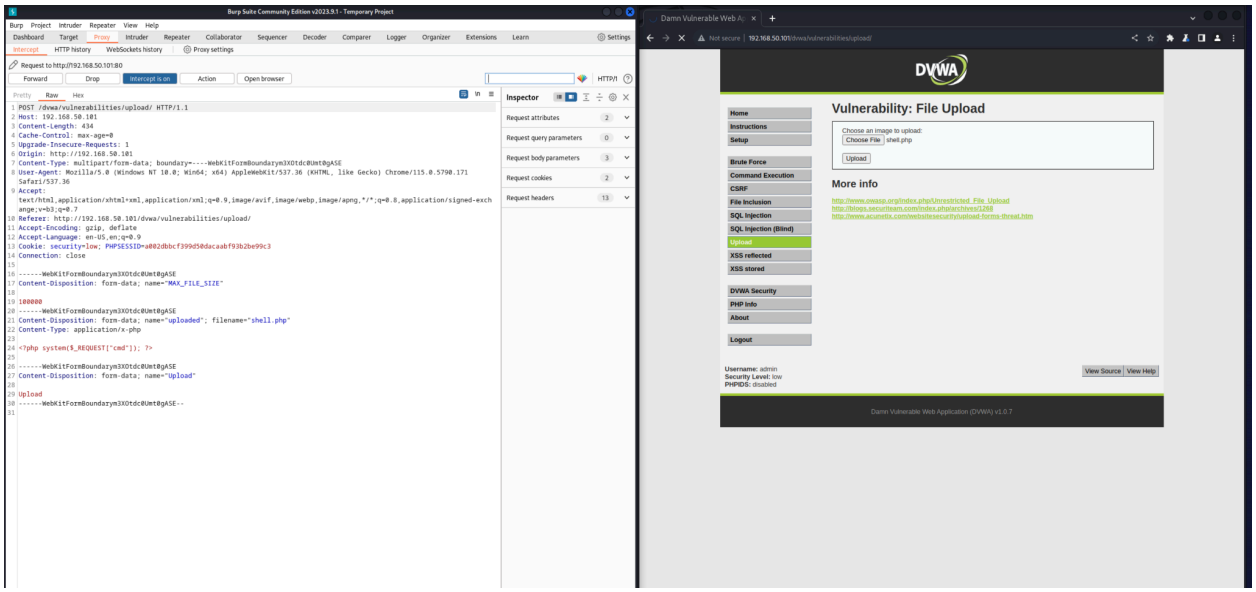
Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, è richiesto di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.
Consegnare:
1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

Implementazione

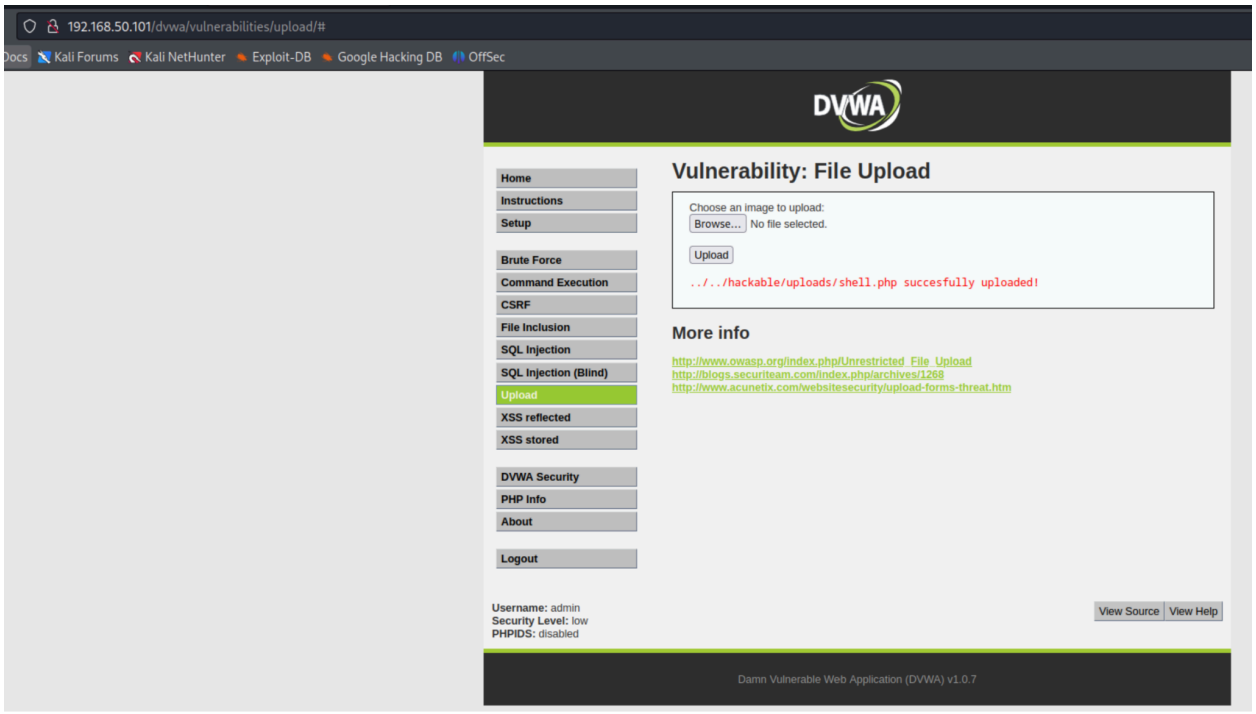
La shell utilizzata per questa esercitazione è molto basilare e consente di eseguire il comando passato come parametro nella richiesta GET.
Di seguito il codice sorgente PHP della shell:

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

Per il caricamento della shell tramite DVWA è possibile utilizzare l'apposito form nella sezione upload.
Intercettando la richiesta mediante Burpsuite è possibile analizzare la richiesta POST con il contenuto del file PHP che costituisce la shell caricata.



Facendo click su Forward la richiesta viene completata ed la risposta viene inviata al client che mostra la pagina di seguito.

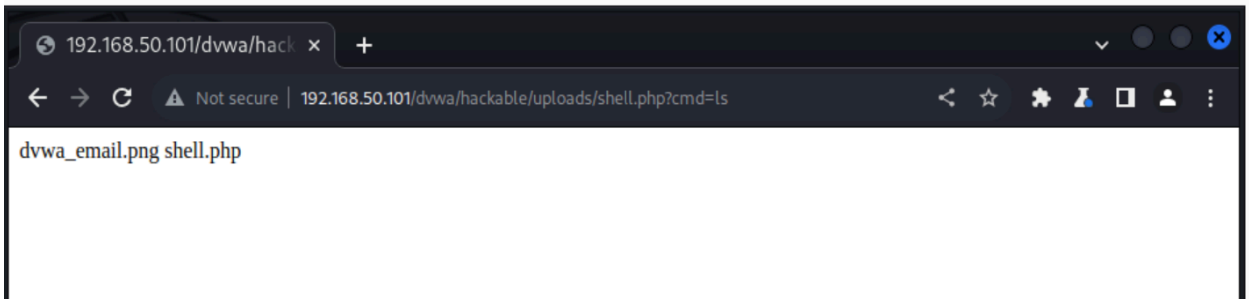


Richieste Shell

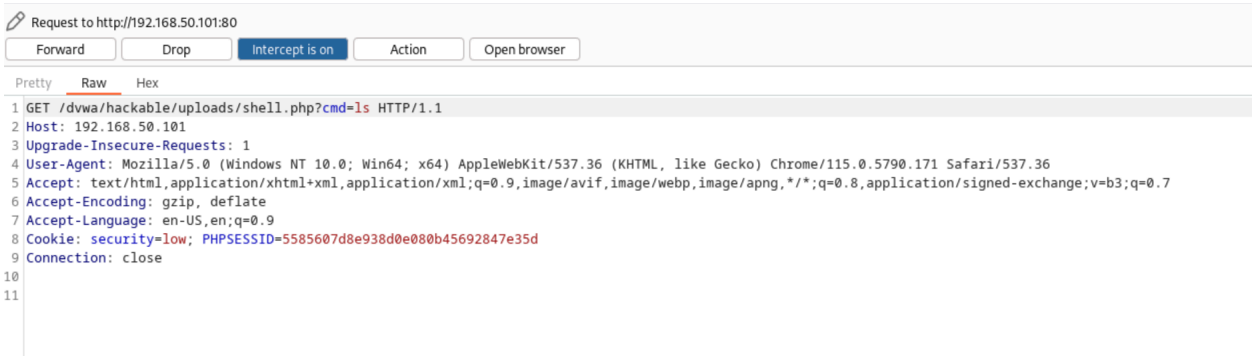
Nelle seguente sezione è mostrato il risultato di alcuni comandi inviati alla shell appena caricata tramite il browser.

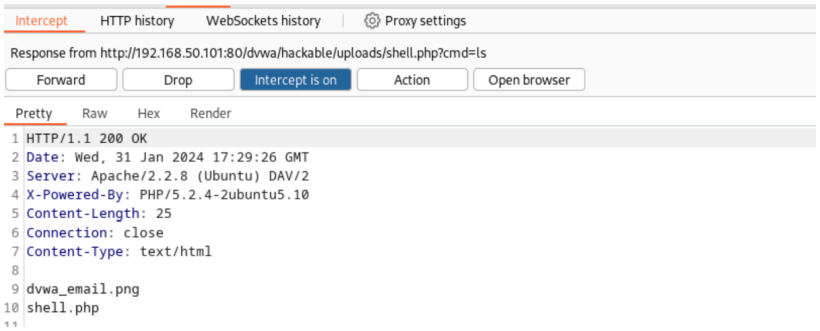
- **LS**

Il comando ls mostra l'elenco dei file nella directory corrente, in questo caso la root dell server web



Di seguito è mostrata la richiesta GET effettuata e la relativa risposta da parte del server intercettate mediante BurpSuite. Nella risposta è possibile notare il risultato con l'elenco dei file che saranno poi visualizzati sul browser



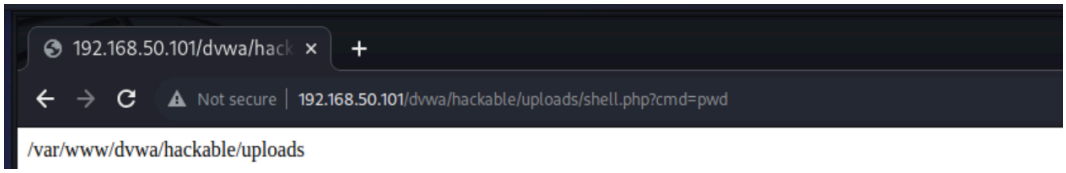


- **LS -AL**

Il comando è simile al precedente ma mostra i file nascosti (opzione -A) e un maggior dettaglio di informazioni sui file (-L)

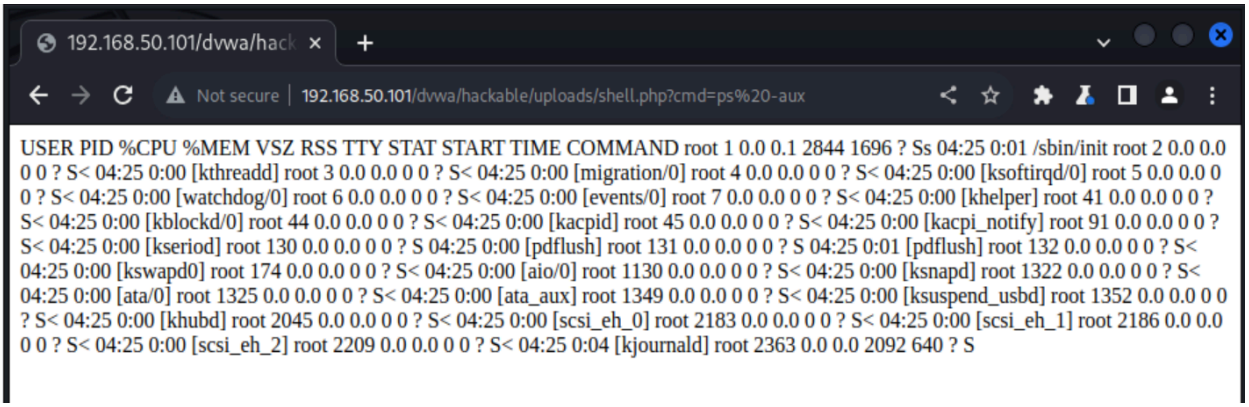
- **PWD**

Tramite il comando PWD viene mostrata la directory di lavoro corrente



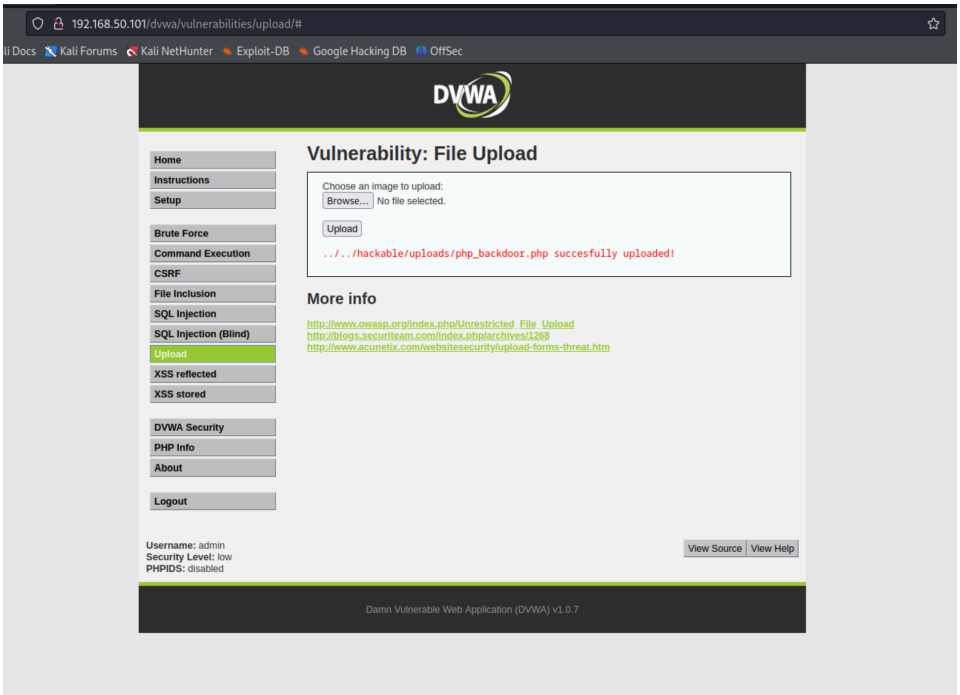
- **PS -AUX**

Mediante il comando ps -aux è possibile reperire l'elenco dettagliato di tutti i processi attivi per tutti gli utenti

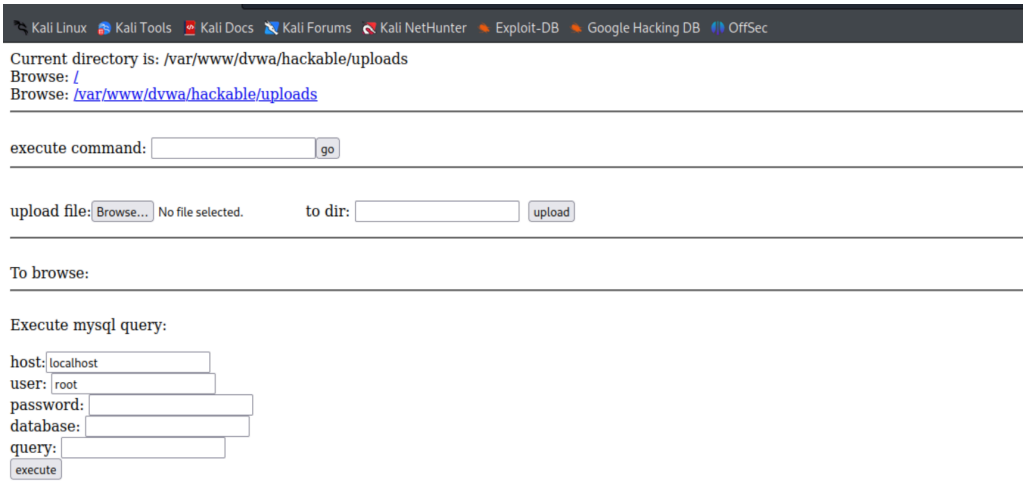


Bonus: shell sofisiticata

Kali Linux mette a disposizione anche web-shell più complesse come ad esempio la shell php_backdoor.php, di cui di seguito è mostraato il caricamento tramite la sezione Upload della DVWA.



La shell è dotata di interfaccia grafica come mostrato nella seguente immagine.

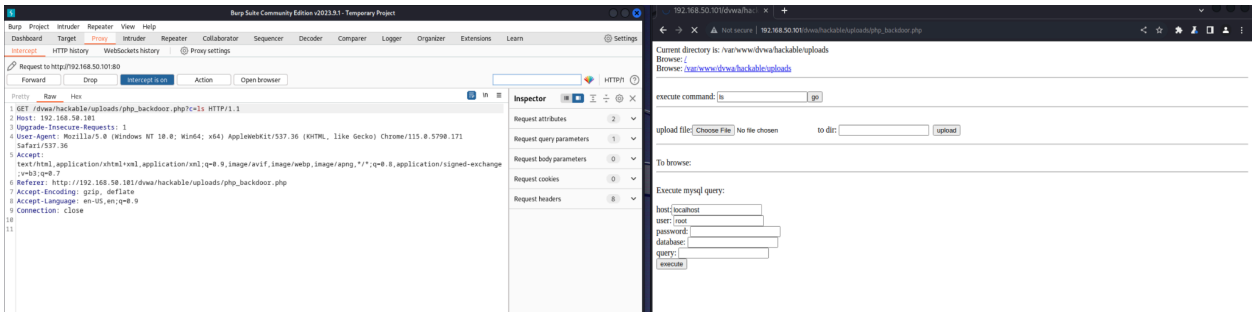


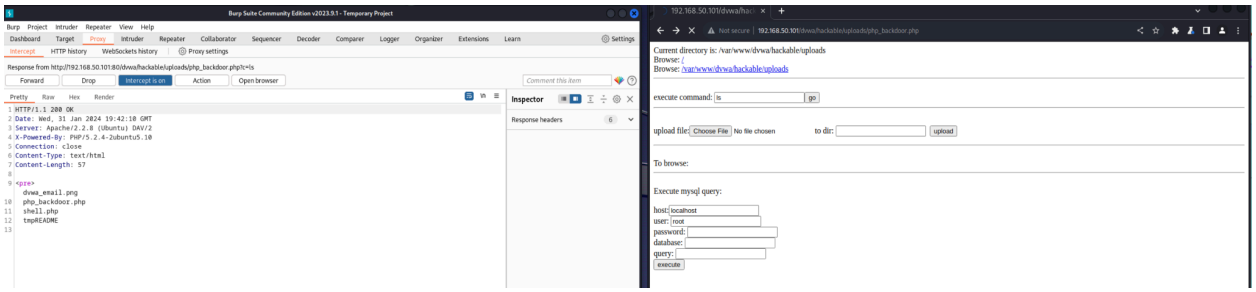
Tramite la shell è possibile effettuare le seguenti operazioni:

- eseguire comandi di sistema (come per la precedente shell)
- effettuare l'upload di un file
- eseguire query verso un database mysql

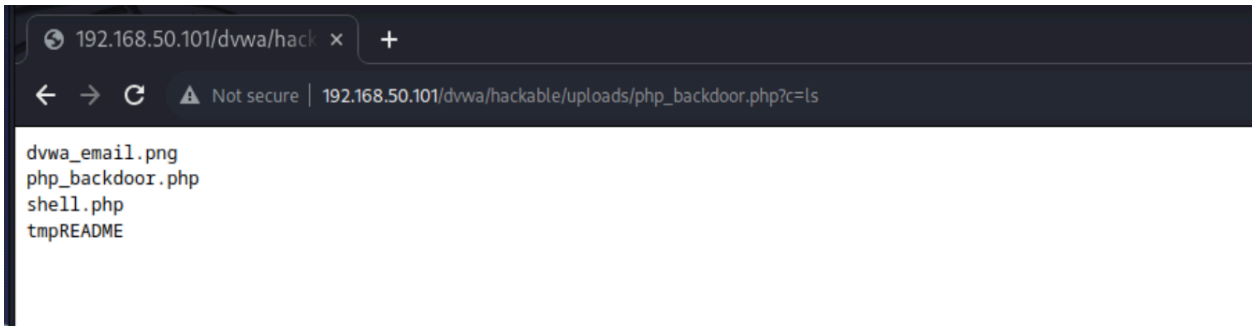
Esecuzione comandi

La shell permetti di eseguire comandi della shell di Linux. Di seguito è mostrata l'esecuzione del comando ls con la relativa richiesta/risposta intercettata mediante BurpSuite.



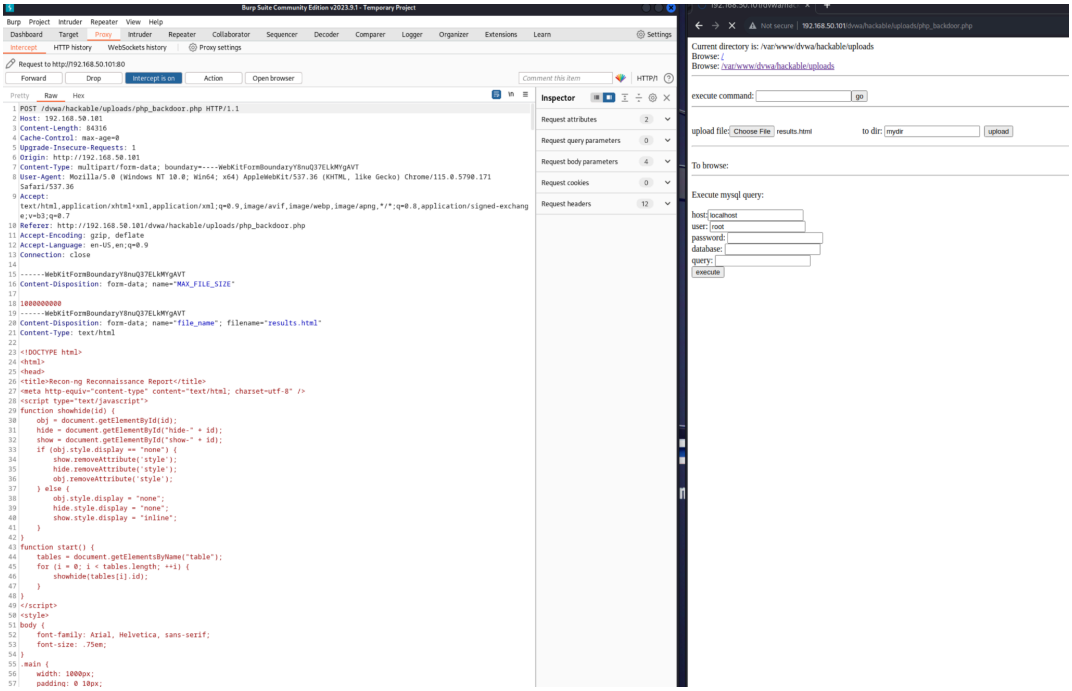


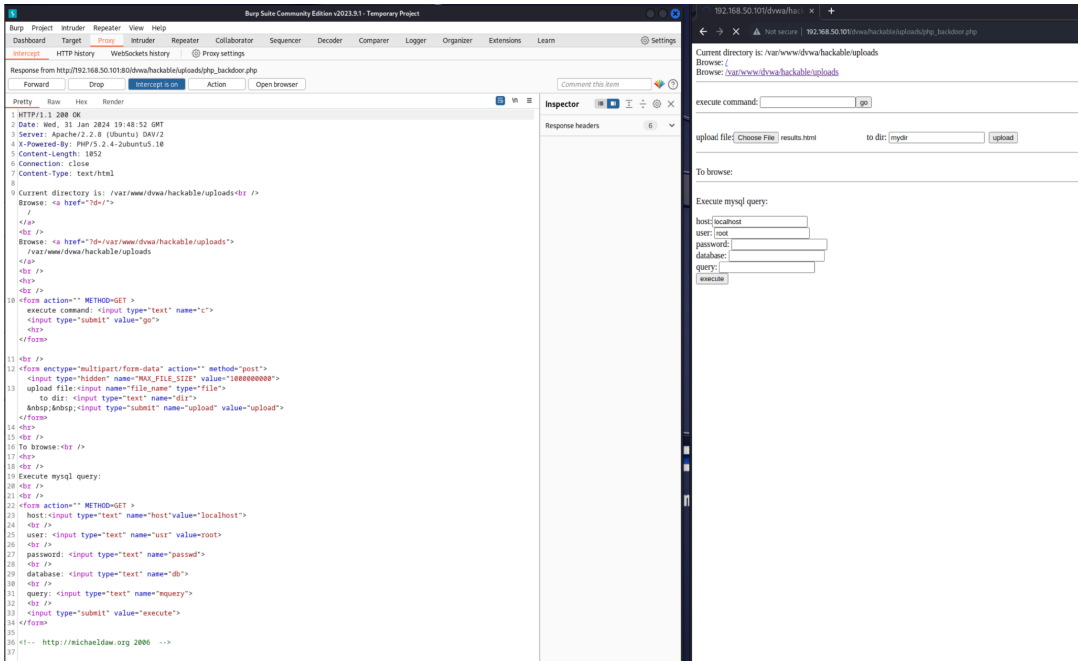
Il risultato viene mostrato dalla seguente pagina.



Upload file

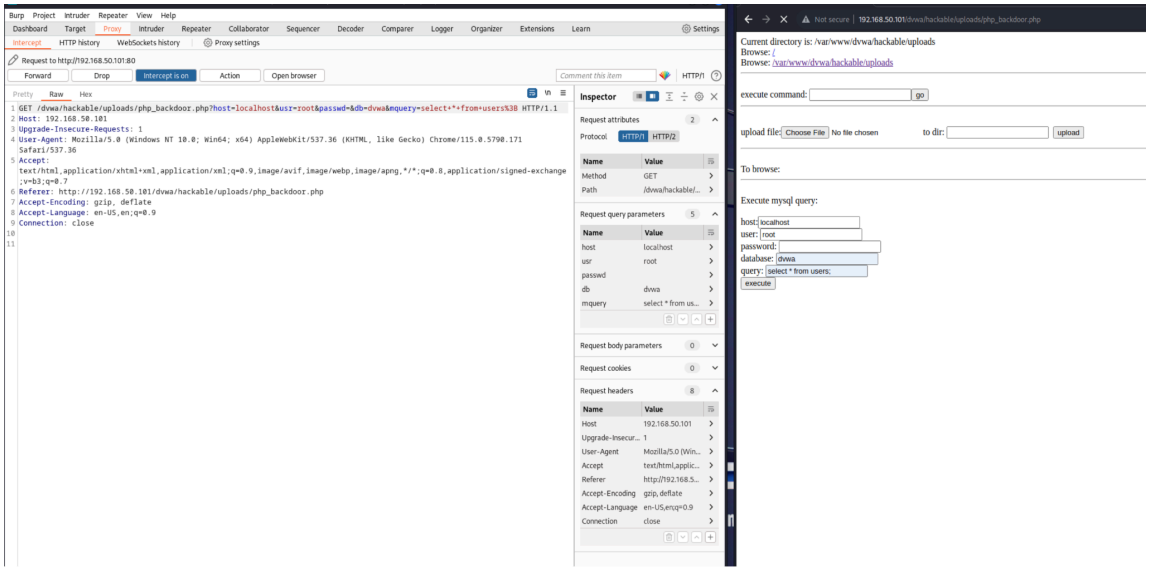
Tramite la sezione Upload File è possibile selezionare un file sulla propria macchina e caricarlo nella directory indicata dal campo “to dir:”. Nelle immagini seguenti sono mostrate la richiesta e la relativa risposta intercettata tramite BurpSuite

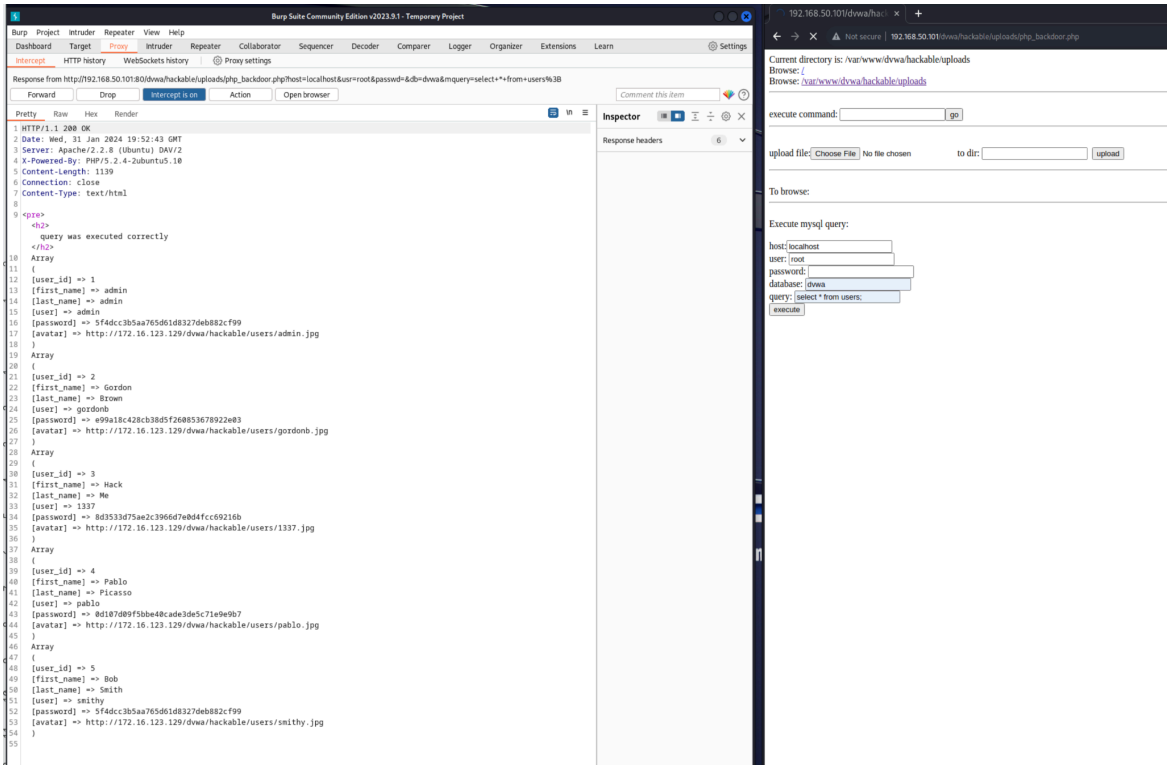




Richiesta al databse

L'ultima funzionalità della shell è quella di interrogazione di un database. Nelle immagini successive è mostrato il processo di richiesta/risposta della query SELECT * FROM users del database DVWA





Il risultato della query viene mostrato in una pagina sul browser come di seguito