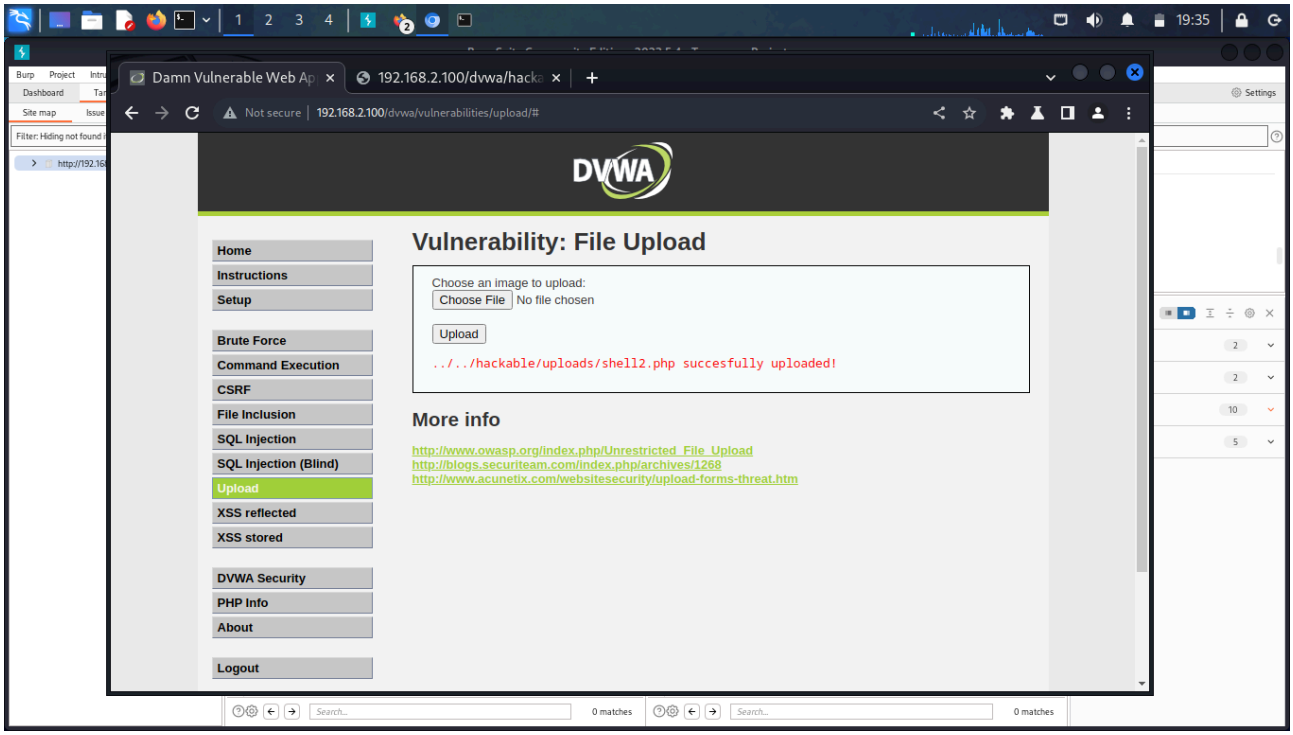
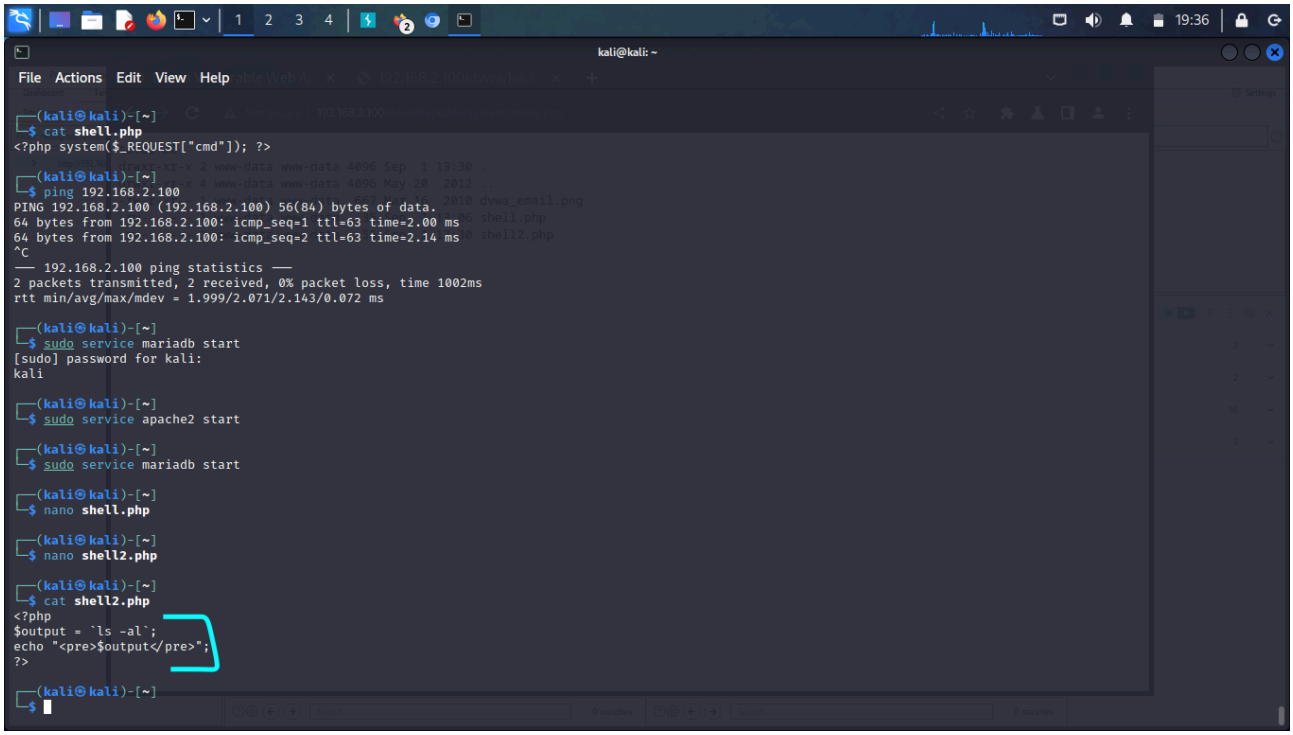
Anselmo Buonamici M4 - D1

File upload exploit

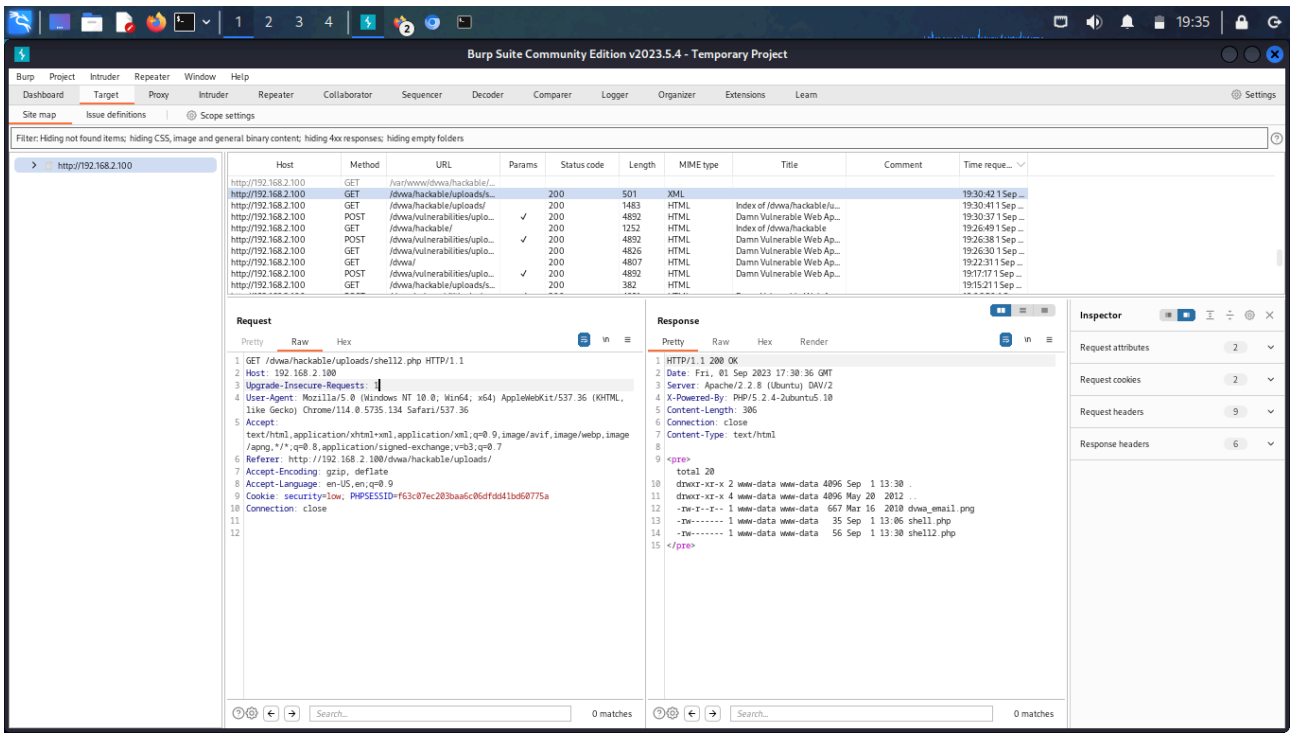
Questo esercizio prevede di sfruttare la vulnerabilità sull'upload di un file in form senza nessun controllo da parte della web app.



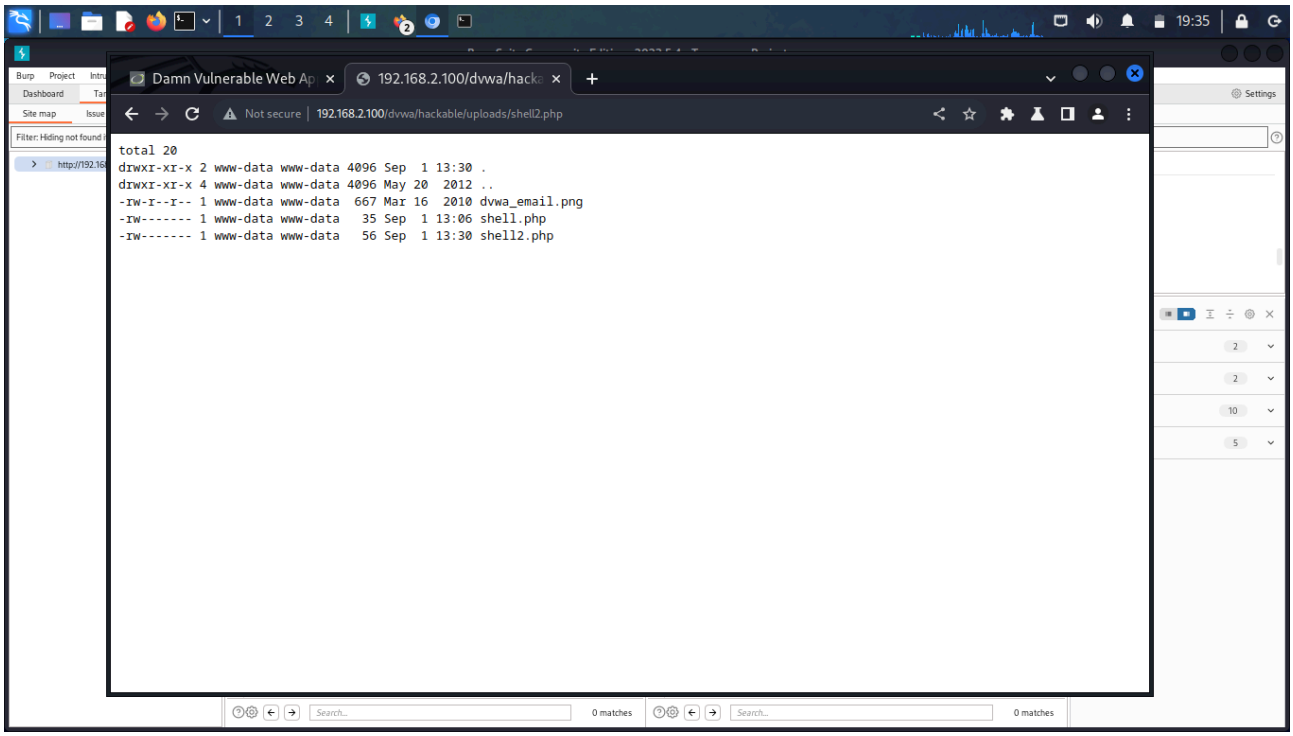
Codice php semplice usato per il primo test:



Richiesta GET dopo il caricamento tramite Burpsuite:



Sfruttamento della vulnerabilità ed esecuzione della shell sul server web:



Anselmo Buonamici M4 - D1

Sul web ho trovato tantissimi script in php più complessi e per l'esercizio ne ho scelto uno in grado di manipolare i permessi dei file dentro la web app.