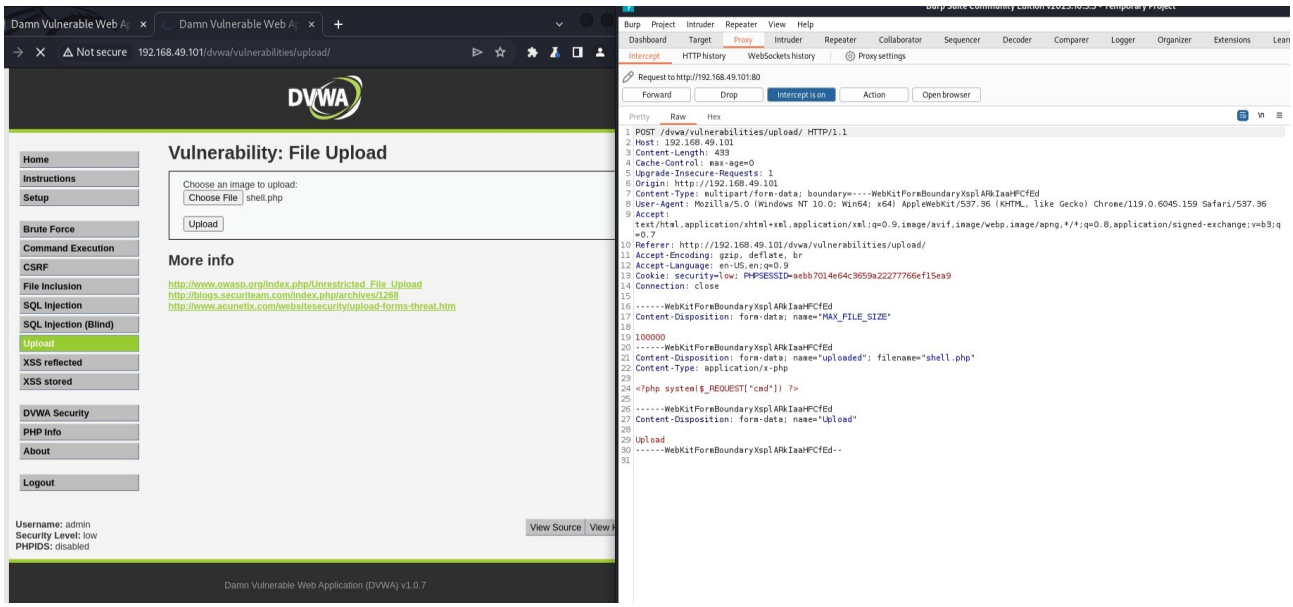
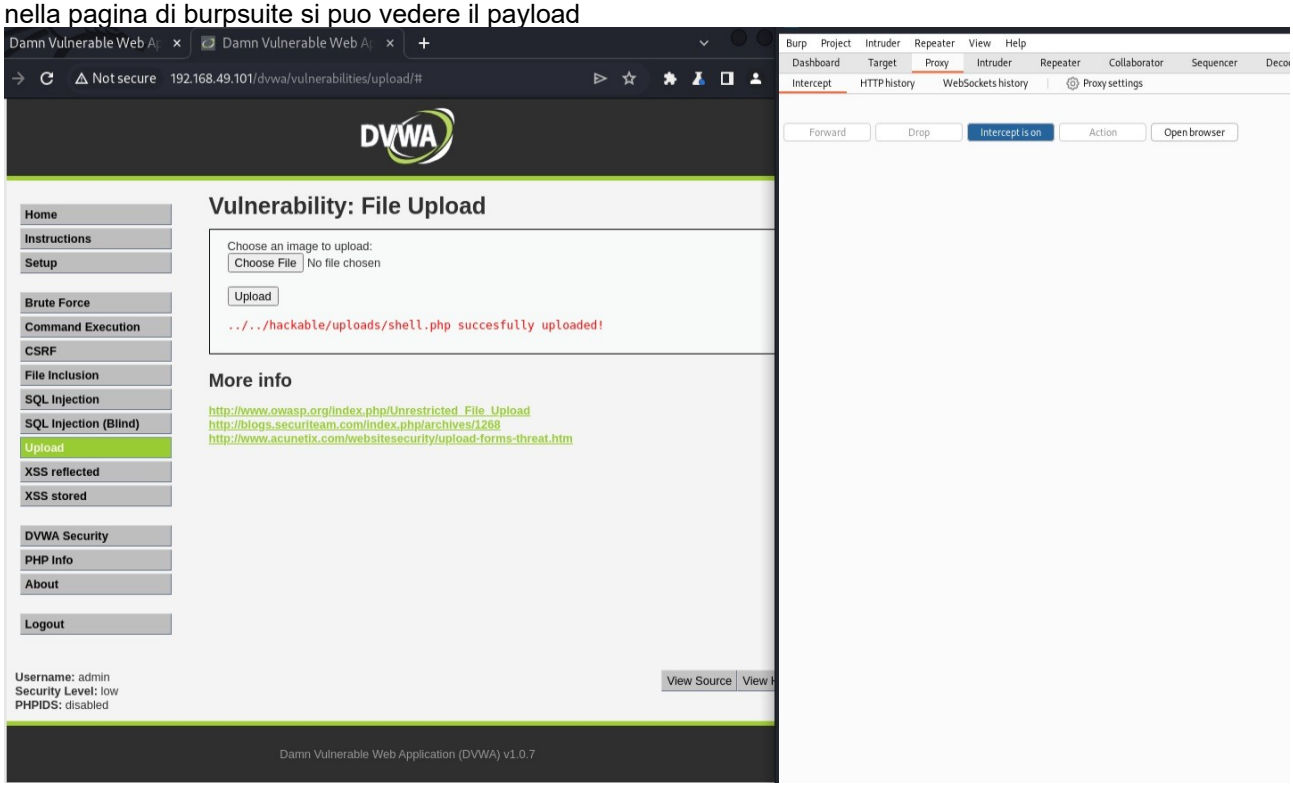
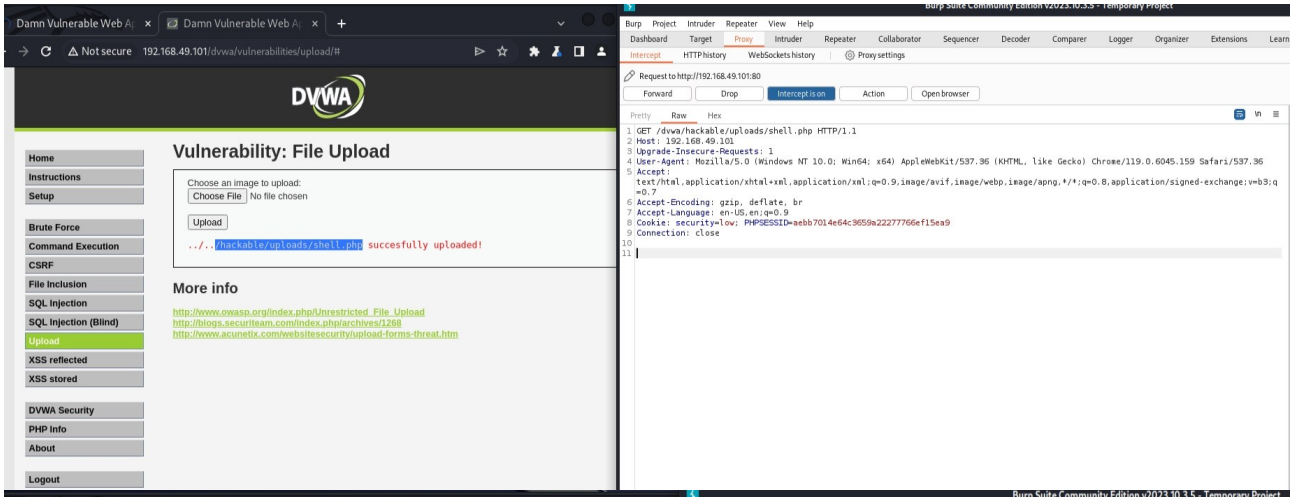
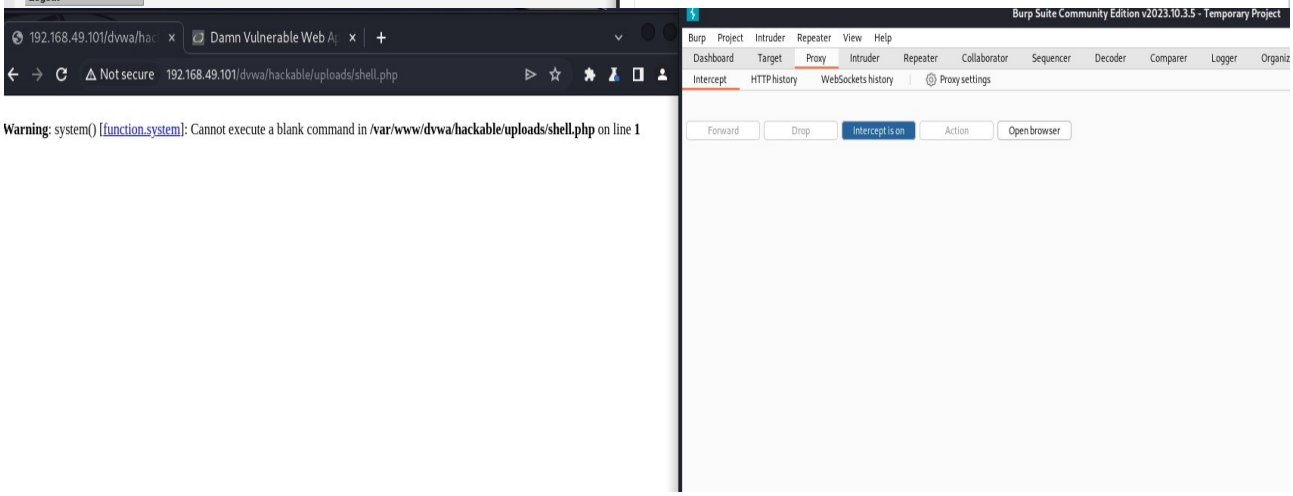


Tramite la pagina di upload di DVWA carico il codice in php.
La pagina ha protocollo http e verbo POST quindi posso trasportare dati nel payload della pagina;
avendo impostato la sicurezza a LOW posso caricare file di tipo php (dinamici in quanto la loro trasposizione prevede una rielaborazione del dato inserito e non una trasposizione passiva come per un file jpeg) senza che vengano bloccati;
nella pagina di burpsuite si puo vedere il payload

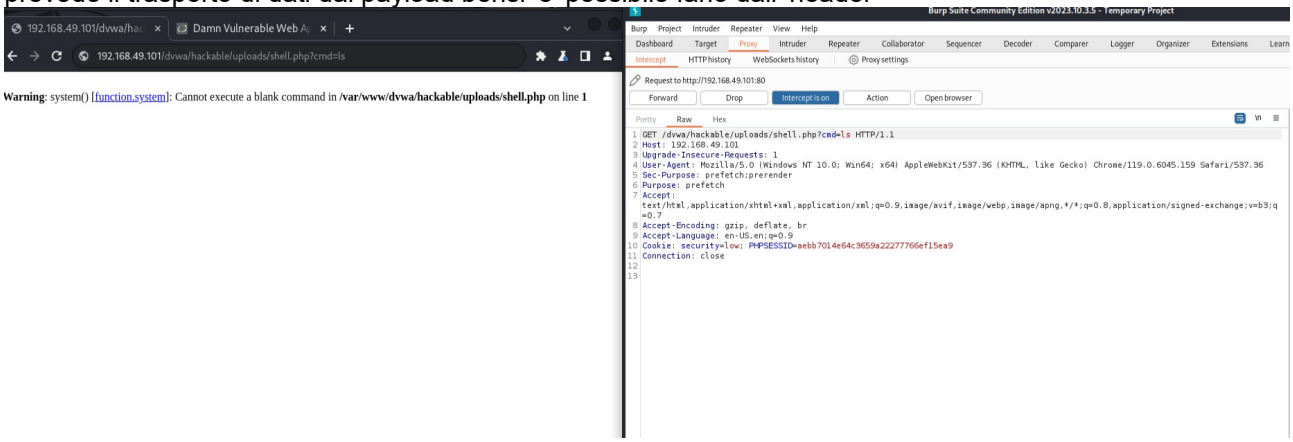


dopo aver caricato il file con successo, vado sulla pagina http dove e' presente il file

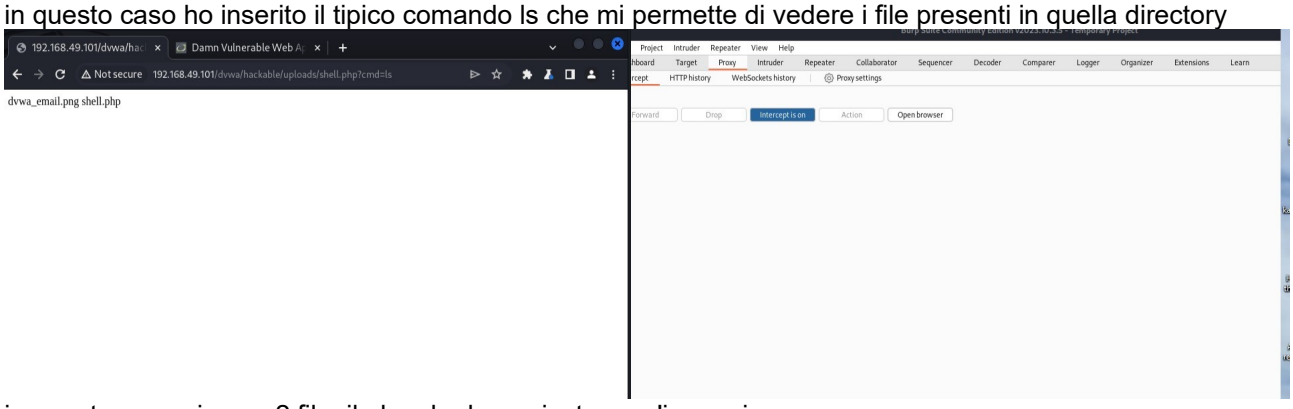




appare una pagina html che chiede di inserire comandi sull' url in quanto il verbo della pagina e' GET e non prevede il trasporto di dati dal payload bensi' e' possibile farlo dall' header



in questo caso ho inserito il tipico comando ls che mi permette di vedere i file presenti in quella directory



in questo caso ci sono 2 file, il php che ho caricato e un'immagine png