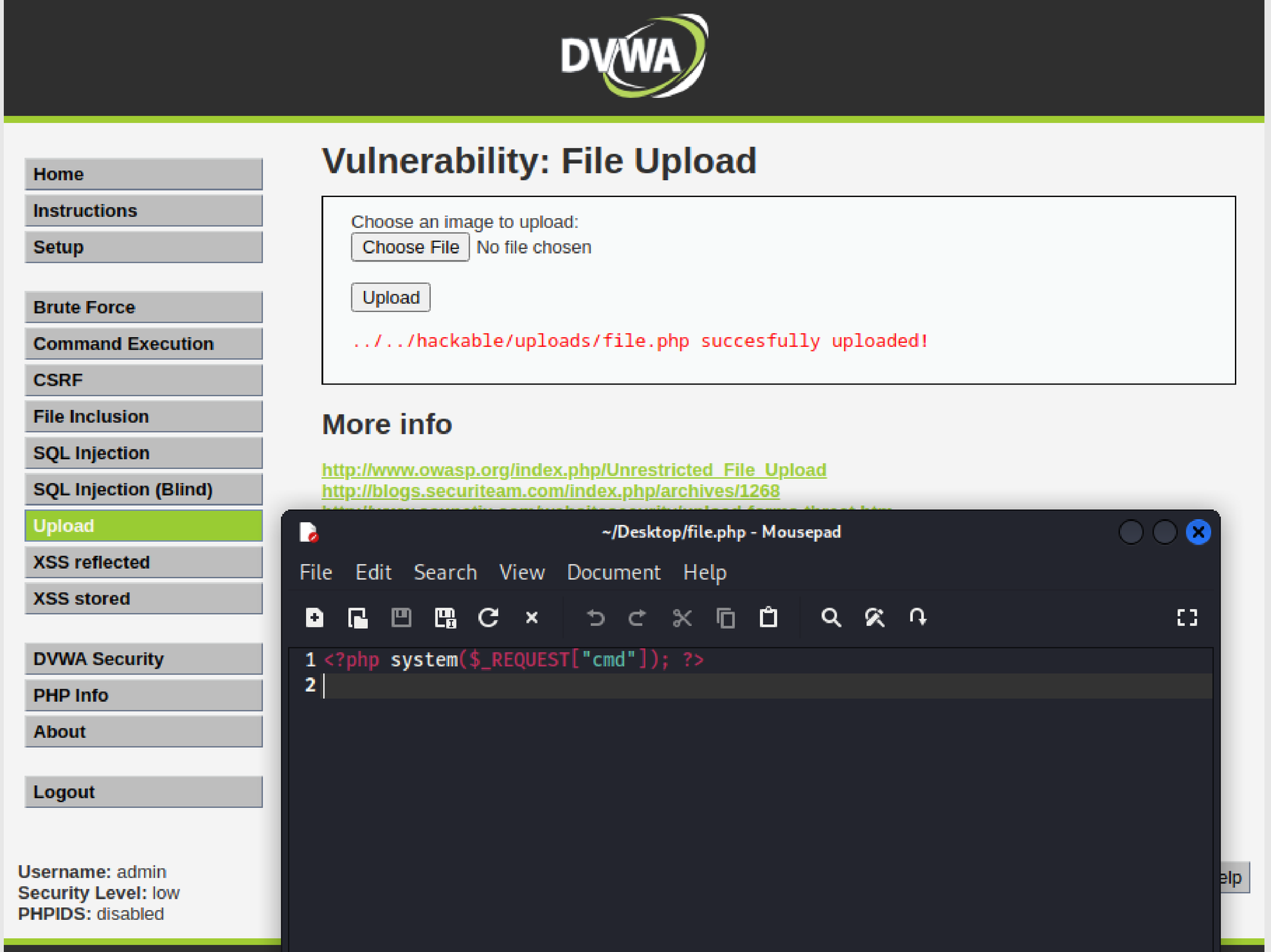
S6 L1

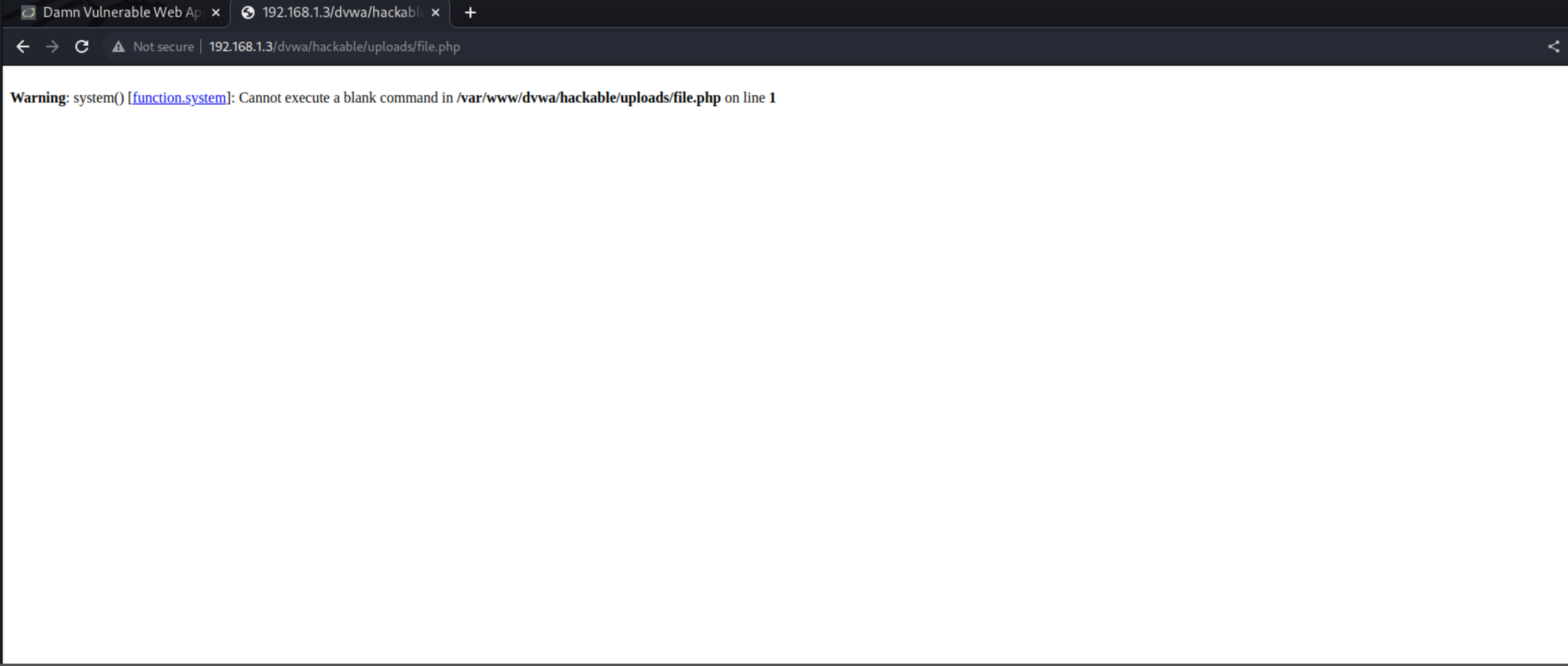
Nel esercizio di oggi Vedremo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP.
Monitoreremo tutti gli step con BurpSuite.

Come detto in precedenza avviamo Burpsuite, che ci permetterà di tenere tracci di tutte le richieste che andremo ad effettuare e analizzare il codice, apriamo il browser e raggiungiamo il server dwva

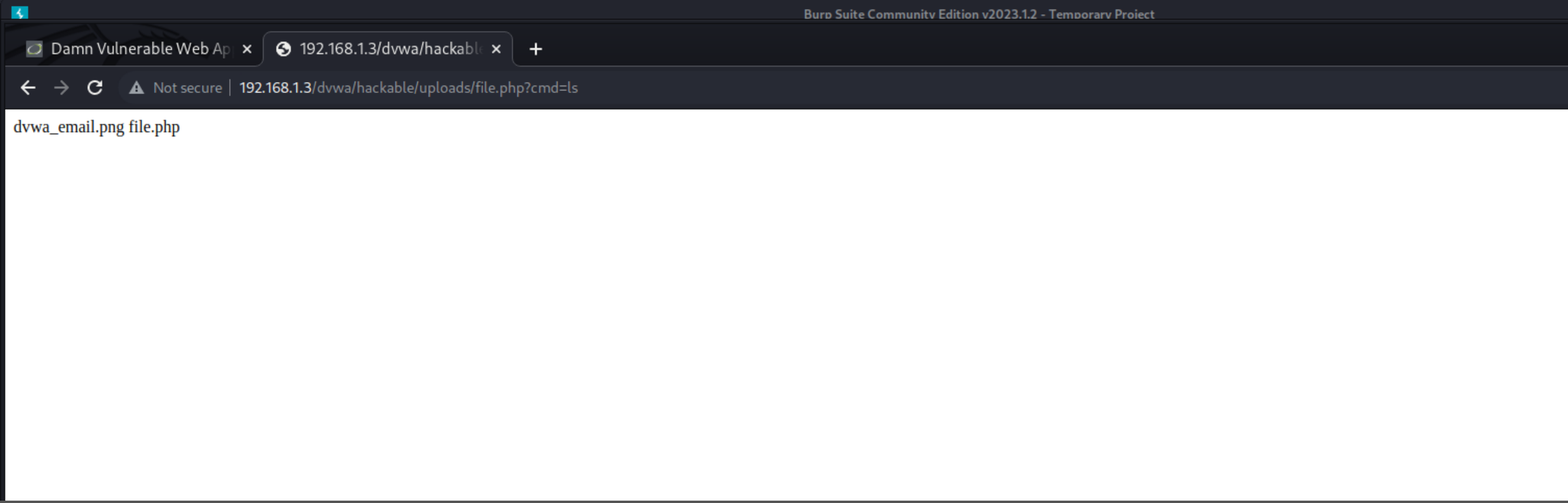
N.B. Ricordiamoci di impostare il livello di sicurezza a “Low” in quanto, altrimenti, non ci permette di caricare il file nella specifica finestra di upload



Come possiamo vedere dall'immagine affianco, siamo andati a caricare il file.php. con lo script sotto riportato



Questo è il primo risultato che otteniamo non appena andiamo a inserire l'url nella barra di ricerca, come possiamo notare ci da un errore, poichè manca un comando importante per accedere. Andiamo quindi a inserire "cmd=ls" e vediamo cosa succede



Ed ecco che una volta aggiunto il comando “cmd=ls” come cambia la schermata che visualizziamo