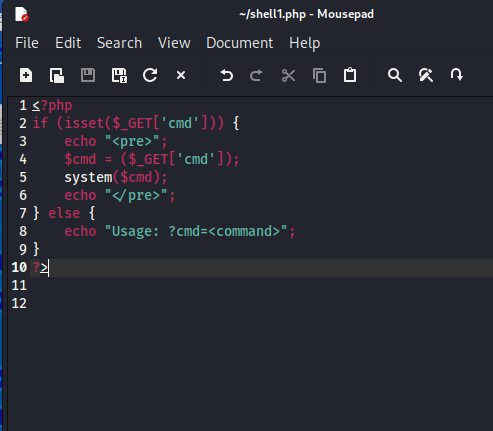
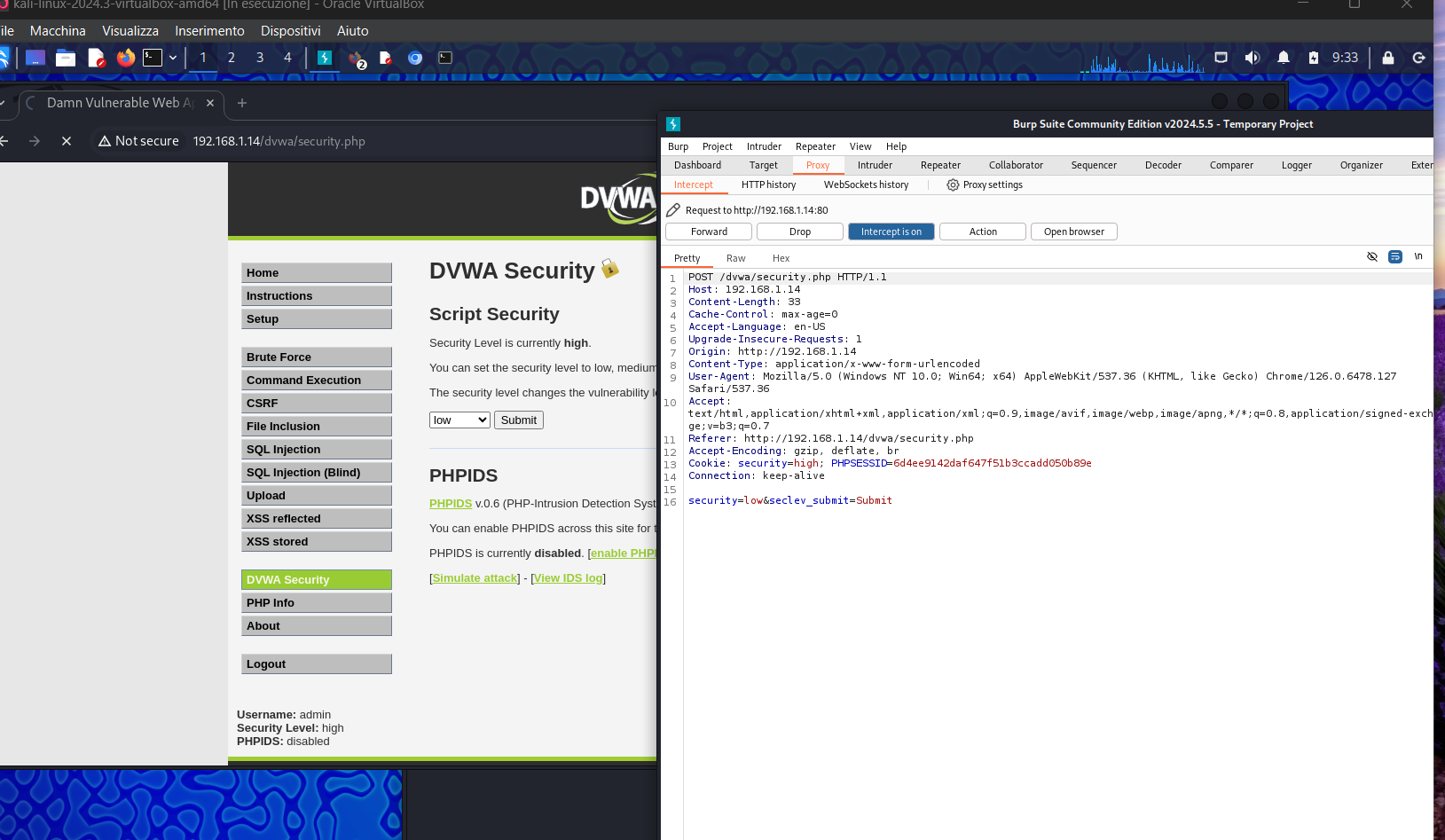
**S6 L1**

**AMATO SARA**

**EXPLOIT FILE UPLOAD**

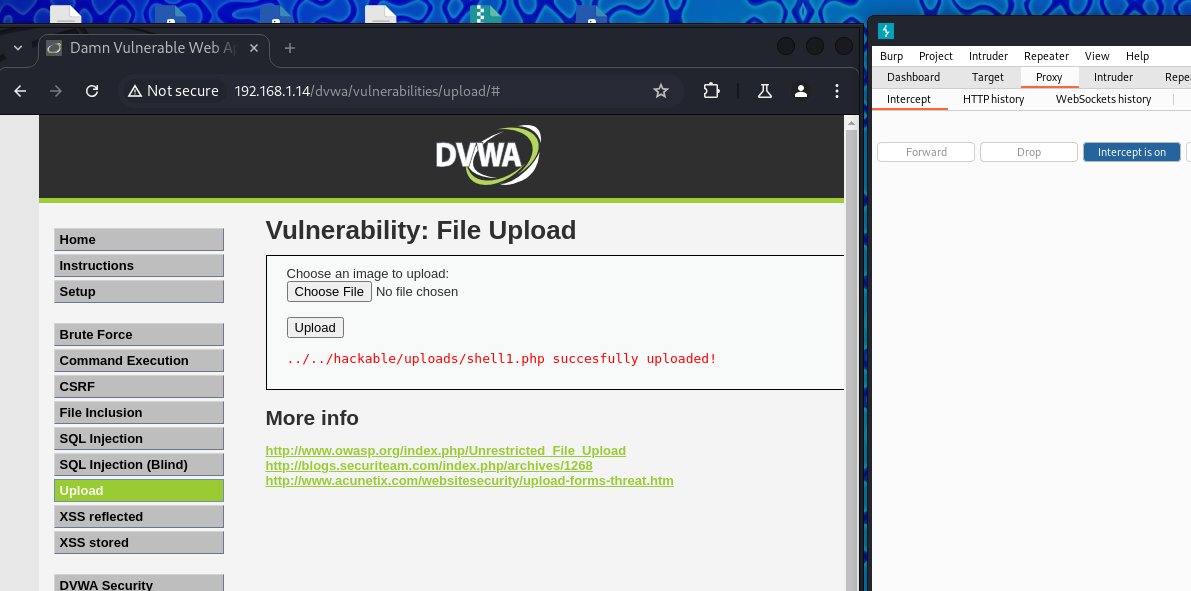
L’ambiente è stato configurato utilizzando due macchine virtuali: Metasploitable, che ospita la DVWA vulnerabile, e Kali Linux, che funge da macchina dell’attaccante. Dopo aver avviato entrambe le macchine, è stata verificata la connettività tramite un semplice ping da Kali Linux a Metasploitable, assicurandosi così che la comunicazione bidirezionale fosse correttamente configurata.

**Caricamento della Shell PHP**

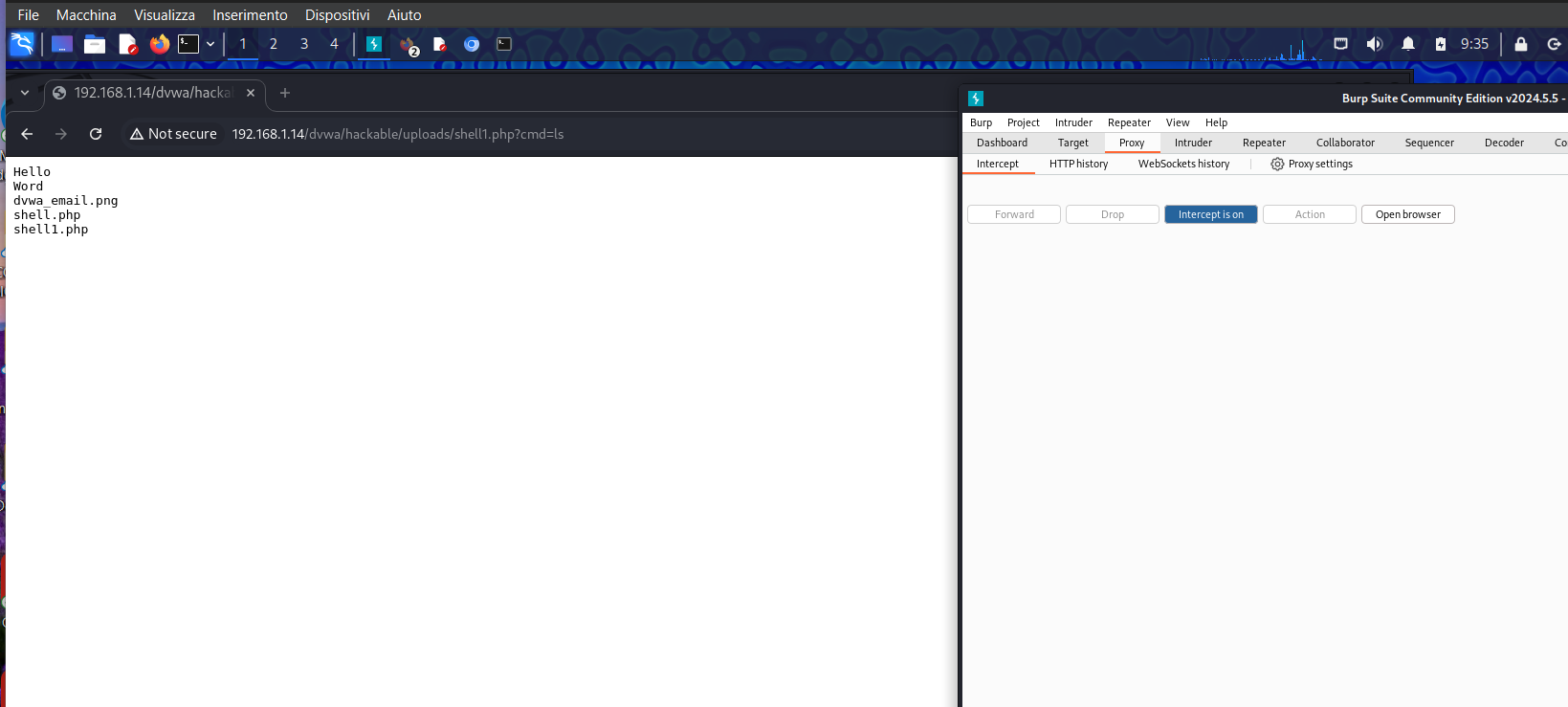


Dopo aver confermato la connessione, siamo passati al caricamento della shell PHP. Utilizzando il browser di Kali, abbiamo acceduto alla DVWA sulla macchina Metasploitable. All’interno della sezione File Upload della DVWA, è stato caricato un file PHP (denominato `shell.php`) con una semplice shell in grado di eseguire comandi da remoto. Una volta caricato, si è verificato che il file fosse stato salvato correttamente nella directory di upload della DVWA.

**Esecuzione della Shell PHP**

****

Dopo aver caricato la shell, l'abbiamo eseguita tramite il browser. Accedendo all’URL del file `shell.php` e inserendo comandi tramite parametri URL (`cmd`), siamo riusciti a eseguire comandi di sistema sulla macchina Metasploitable. Questa fase ha permesso di esplorare ulteriormente la vulnerabilità, simulando il tipo di accesso che un attaccante potrebbe ottenere.



Questo esercizio ha dimostrato come una vulnerabilità di upload di file, se non adeguatamente protetta, possa essere sfruttata per ottenere accesso non autorizzato a un sistema. La configurazione di strumenti come BurpSuite ha fornito un’ulteriore comprensione dell’attacco, evidenziando la necessità di controlli di sicurezza robusti per evitare l'esecuzione di file malevoli.