Esercitazione S6/L1

In questa esercitazione ho sfruttato una vulnerabilità del metodo “PUT” ed effettuato un exploit per inserire una shell in PHP.
Per svolgerer l’esercitazione ho utilizzato:

- Kali
- Metaspoitable (DVWA)
- Burpsuite

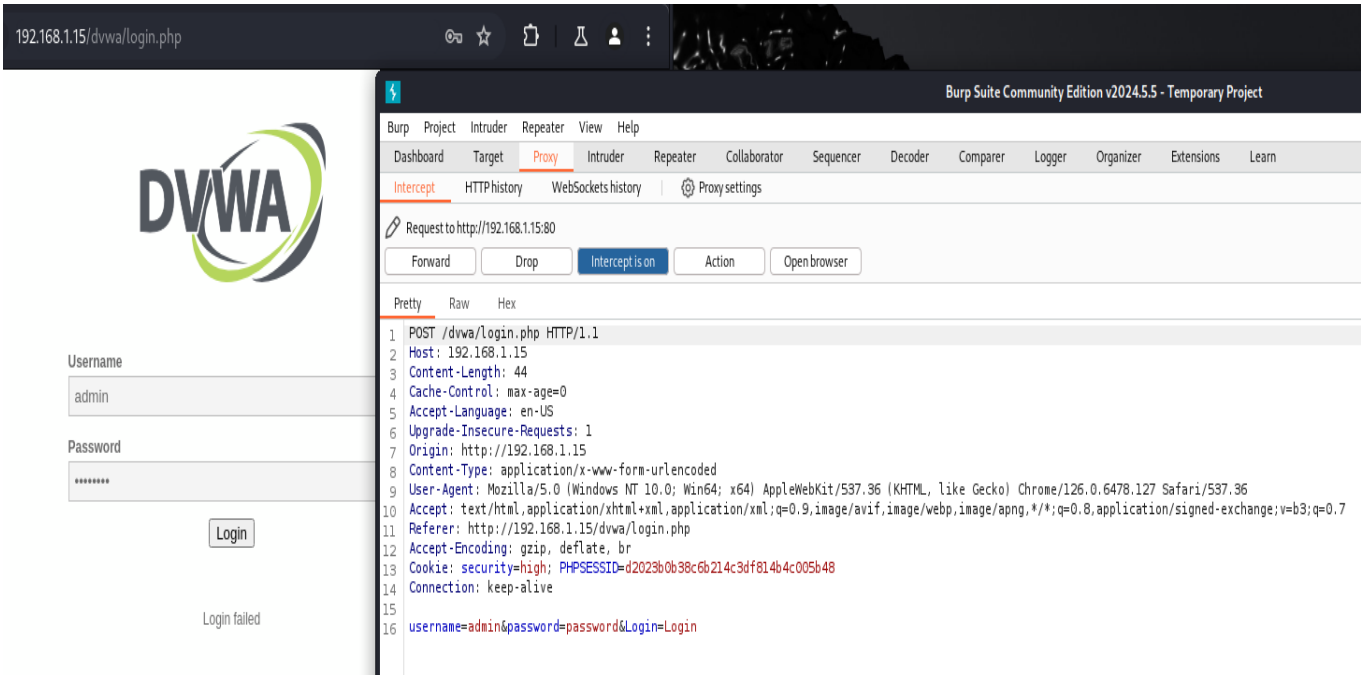
Configurazione:

Dopo aver configurato Kali e Metaspoitable e verificato la connessione tra le due macchine ho effettuato l’accesso a DVWA da Kali.
DVWA è un server apposito per test, con molte vulnerabilità, e ho sfruttato una di quelle per questa esercitazione. Ho impostato in “low” il grado di sicurezza della macchina e creato un file shell.php per poterlo caricare in DVWA.

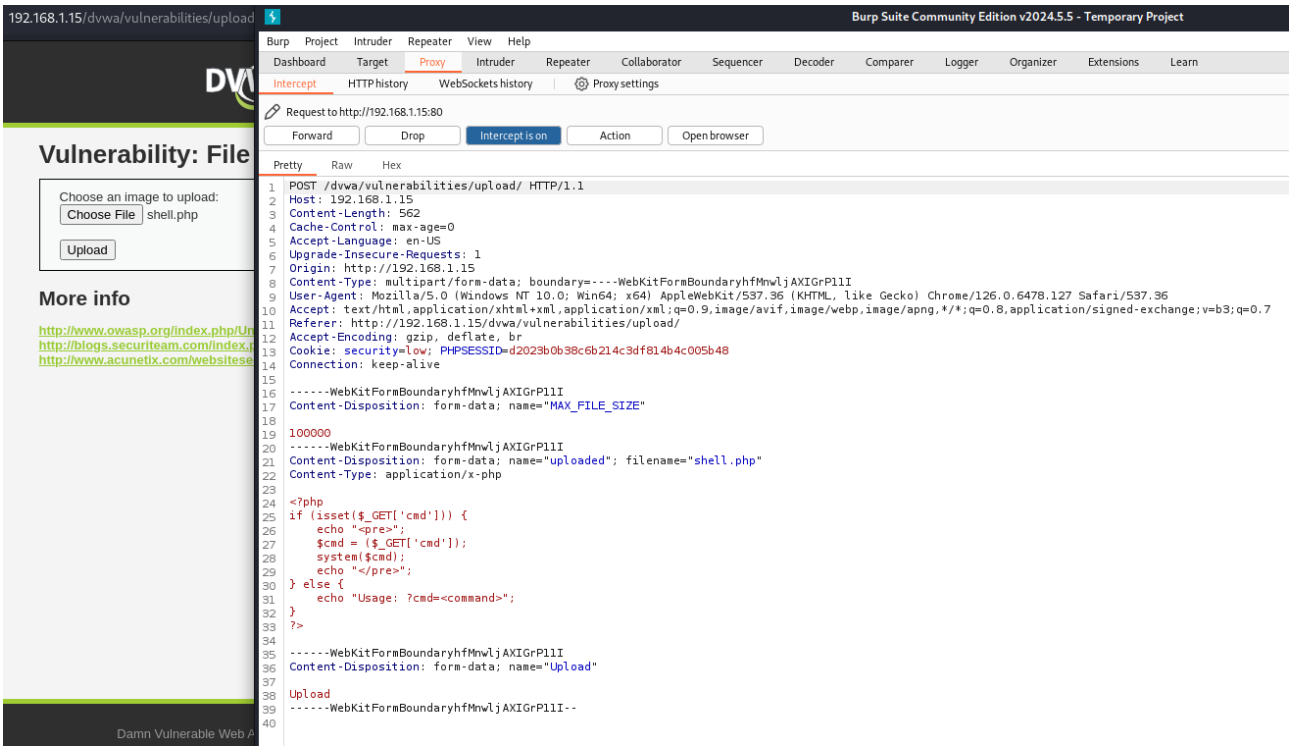
Burpsuite:

Ho utilizzato Burpsuite per intercettare le richieste HTTP/HTTPS tra kali e DVWA nella fase di upload ed esecuzione della shell.

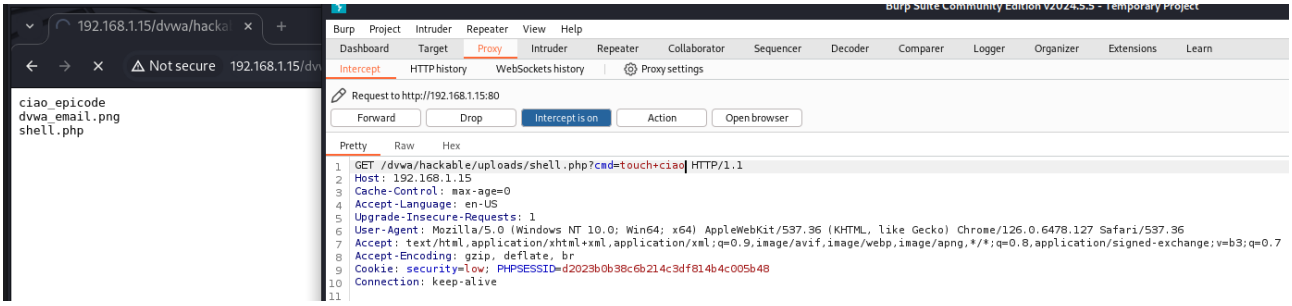
Svolgimento:



Avendo impostato burpsuite come proxy posso quindi intercettare le richieste come si può notare nel precedente screen, quelle sono quindi le richieste per l’accesso al server DVWA
Andando nella sezione upload di DVWA andiamo a caricare la nostra shell.php come vediamo nell’immagine seguente.



Qui possiamo sfruttare il metodo PUT di HTTP.
PUT ci permette di caricare,modificare,creare o sovrascrivire una risorsa sul server, se abilitata è molto pericolosa in quanto un attaccante può sfruttarla per agire direttamente sul server.
DVWA, essendo un server appositamente creato per test, ha il metodo PUT abilitato, può essere quindi sfruttato.



Inserendo il comando “touch+ciao” nella 1° riga ho potuto quindi creare la parola “ciao” all’interno del server.
Ricaricando la pagina si avrà quindi la visione del testo modificato.