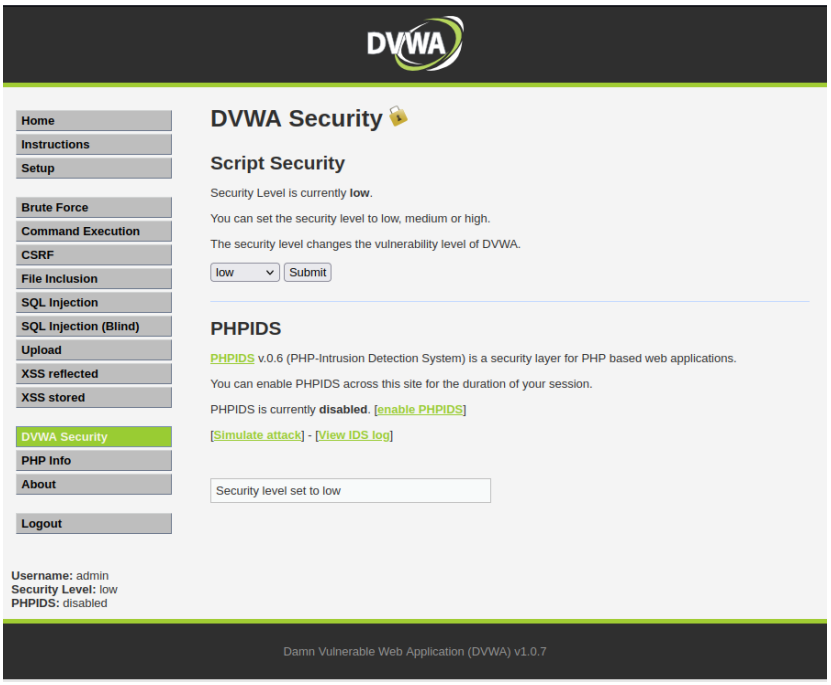
Exploit File Upload

Obiettivo: Sfruttare un file Upload sulla DVWA

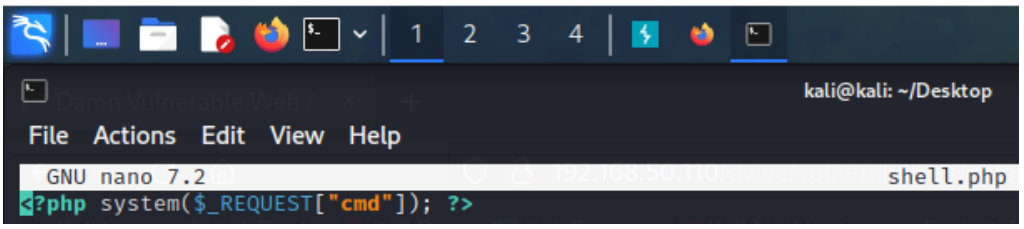
1) Livello di Sicurezza della **DVWA**

Ho iniziato l'esercizio aprendo la **DVWA** di **Metasploitable** per poter settare il *Livello di Sicurezza* su **LOW** come suggerito dalla traccia.



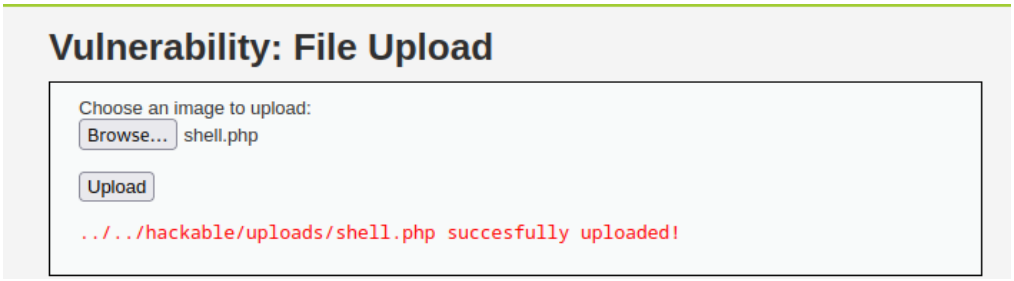
2) Caricamento della Shell

Successivamente ho copiato la shell della traccia con l'editor nano per fare una semplice prova e l'ho caricata sulla **DVWA**.



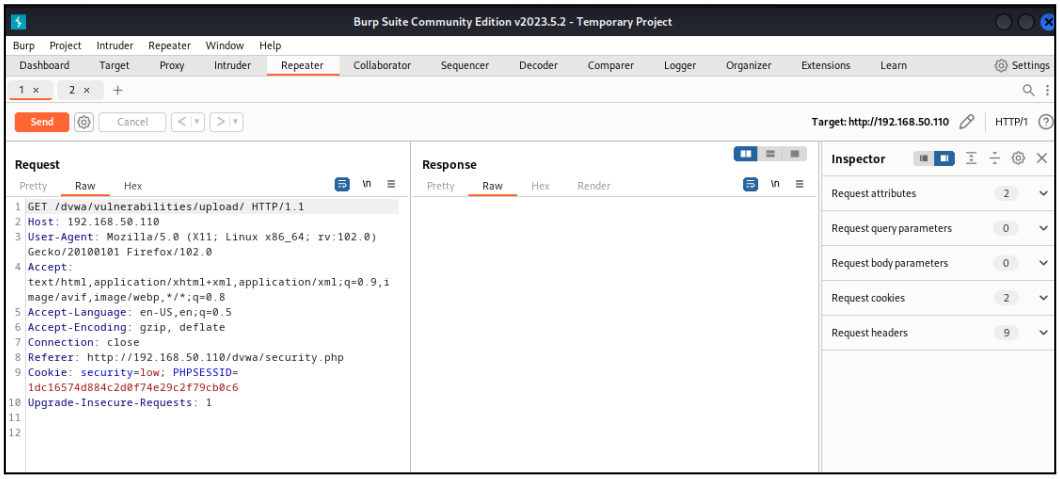
Questa è una shell con la quale si può dare un comando direttamente da URL o come nel mio caso utilizzando il *Repeater* di **Burp Suite**.

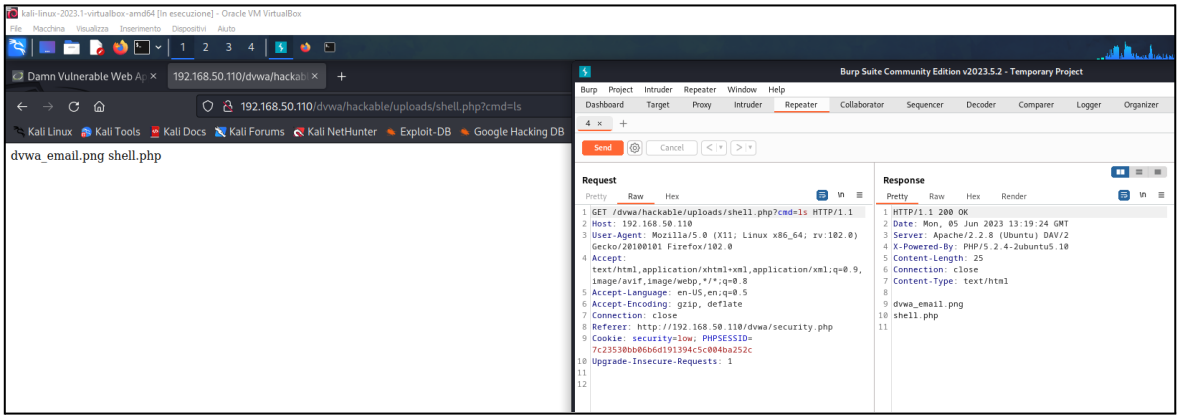
Nell'immagine successiva si può vedere l'upload della shell con il relativo percorso.



3) Burp Suite

Aprendo **Burp Suite** ho intercettato le richieste alla **DVWA** (configurando il proxy su Firefox dato che nel mio caso è più veloce) e con il *Repeater* del programma ho potuto modificare il percorso della richiesta che il browser chiedeva.

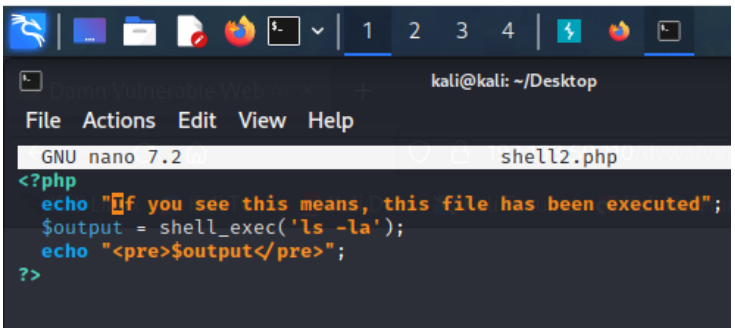




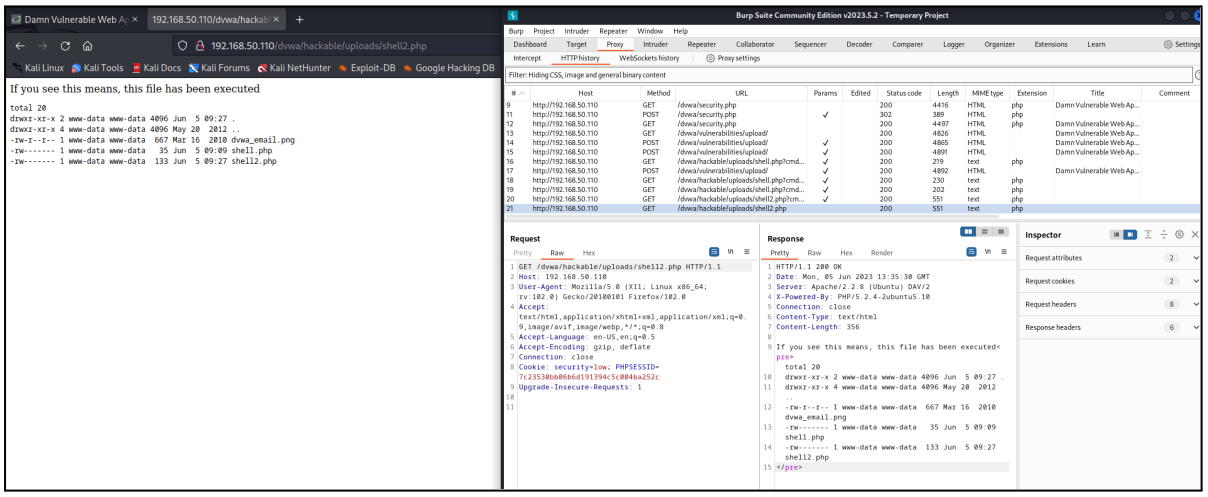
Nella prima immagine ho catturato la semplice richiesta **GET** del browser sull'opzione di upload della **Web App** mentre nella seconda ho modificato l'intero percorso secondo quello dove era stata caricata la shell precedente. Trattandosi di una shell nella quale bisogna dare un comando che verrà poi eseguito, ho dato il comando "***ls***" per mostrare i file presenti nella directory. Il risultato come si vede nell'immagine sopra è che **Burp Suite** mi elenca due file, ovvero la shell e un'immagine precaricata; per controprova sono entrato da browser nello stesso percorso ed effettivamente i due file sono presenti.

4) Seconda Shell

Ho voluto fare una nuova prova con una shell diversa trovata su Internet



Questa è una semplice shell che mostra direttamente se eseguita il comando "***ls -la***" ovvero mostra tutte le directory e file, compresi quelli invisibili, con i rispettivi privilegi.

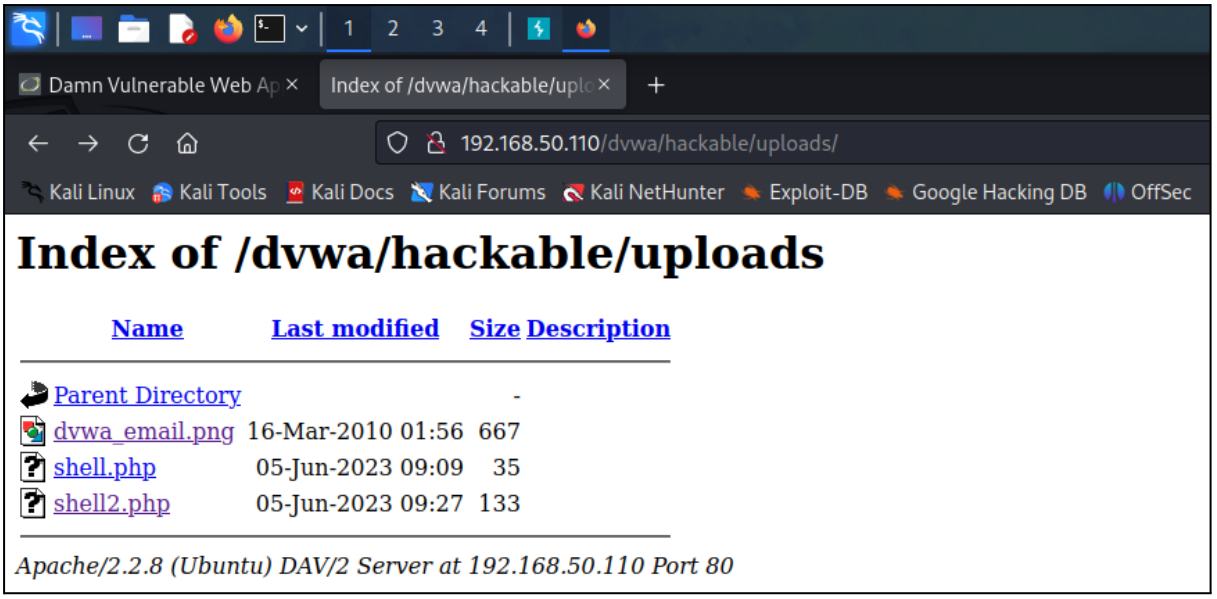


Usando lo stesso procedimento di prima la shell mostra sia sul **Burp Suite** che su browser l'elenco dei file presenti nella **DVWA**.

5) Informazioni aggiuntive

Informazioni aggiuntive che si possono estrapolare grazie all'utilizzo del software **Burp Suite** possono essere:

- Il tipo di Server della macchina che viene intercettata
- La lunghezza e il tipo di contenuto che si va ad analizzare
- La data di "scadenza" dei cookie trattandosi in questo caso di una **Web App**
- Il **Sistema Operativo**
- Eventuali altri file presenti nelle Directory, come il file .png della **DVWA**



Se nella macchina, come in questo caso, è possibile accedere alla *Directory Listing* informazioni sul tipo di Server e sul **Sistema Operativo** è possibile leggerle tranquillamente nella pagina stessa.