EPICODE W13D1 - Pratica (2) PDF **Esercizio** Traccia

Traccia:

1. Ripetere l'esercizio di ieri utilizzando questa volta al posto di una shell base una più sofisticata e complessa
2. È possibile reperire delle shell anche online o eventualmente dentro la stessa macchina Kali

In questo esercizio utilizzeremo lo strumento **weevely**, uno strumento di test di penetrazione che consente agli hacker etici e ai ricercatori di sicurezza di eseguire varie operazioni di hacking su un sito web o su un server web. Ecco una spiegazione del comando **Weevely** e di come viene utilizzato:

- Quando eseguiamo **Weevely** dalla riga di comando, lo strumento verrà avviato e verrà chiesto di specificare l'URL del sito web che desideriamo attaccare e una password segreta che verrà utilizzata per autenticare la nostra sessione con il server **Weevely**.

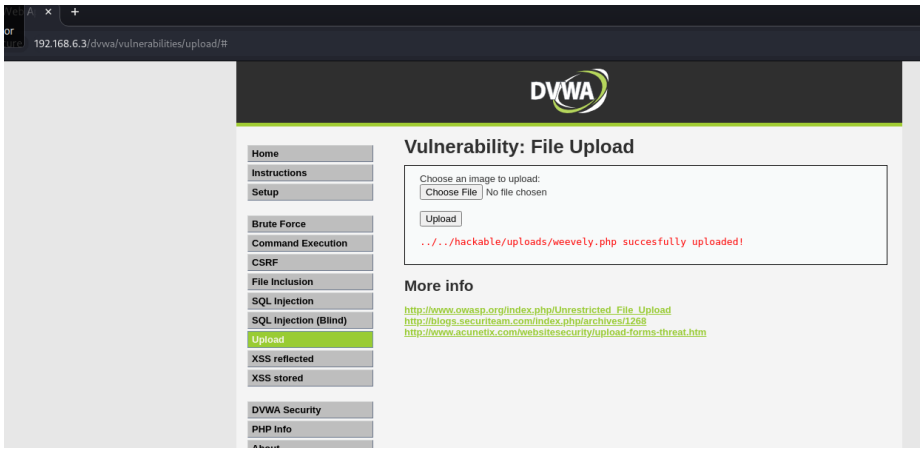
- `weevely generate <password> <output_file>`: Genera uno script di shell backdoor PHP con la password specificata e lo salva in un file specificato.

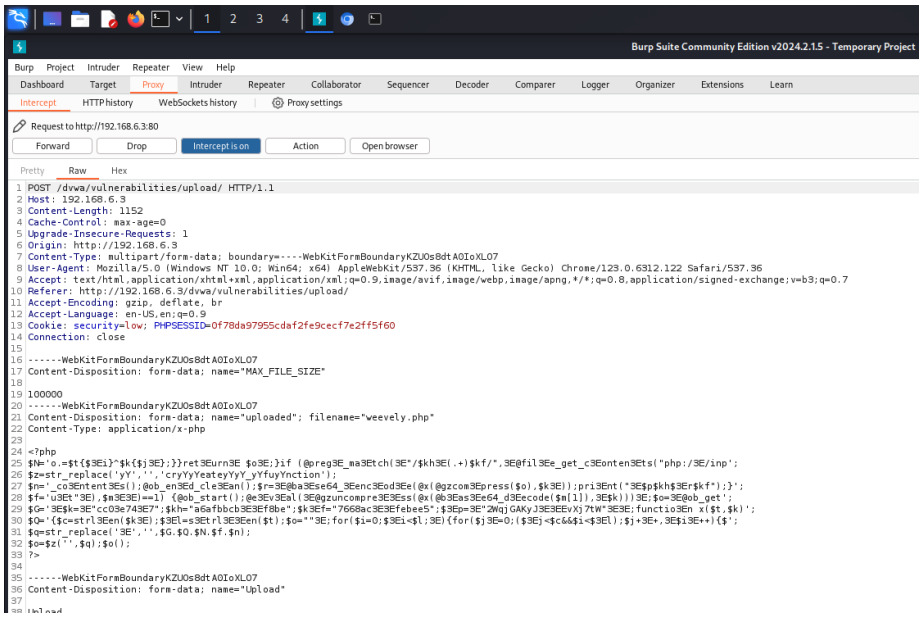
- `weevely <URL_del_sito> <password>`: Avvia una sessione interattiva con il server Weevely situato all'URL specificato, utilizzando la password specificata per autenticarsi. Una volta connesso con successo, potremmo utilizzare una varietà di comandi per eseguire operazioni di hacking sul server remoto. Questi comandi includono l'esecuzione di comandi shell, la modifica dei file, il download e l'upload di file, e molte altre operazioni.

`weevely generate <password> <output_file>`:

```
┌──(kali㉿kali)-[~]
└─$ weevely generate test123 weevely.php
Generated 'weevely.php' with password 'test123' of 751 byte size.
```

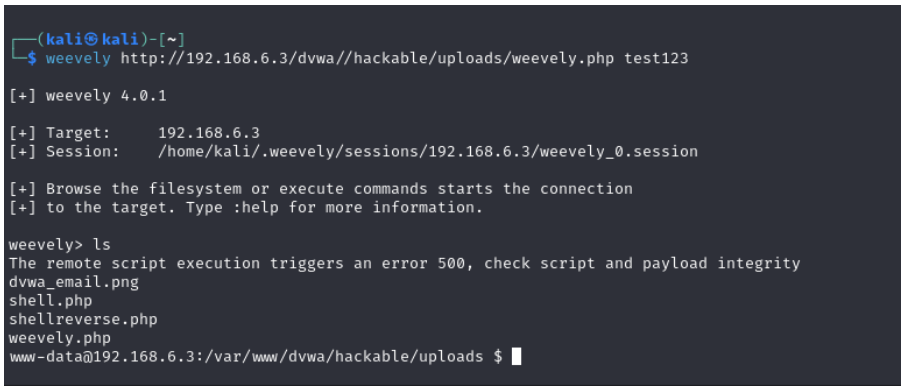
Upload del file weevely.php





Dopo aver caricato il file malevolo su dwva bisogna semplicemente copiare l'url del caricamento e copiarlo nel terminale con la password di autenticazione. Fatto ciò avremo la connessione con la pagina web e possiamo eseguire i comandi direttamente dal terminale di kali.

`weevely <URL_del_sito> <password>`:



Come possiamo notare abbiamo una connessione remota su kali linux e possiamo digitare comandi come **ls** per poter visualizzare il contenuto della pagina web.