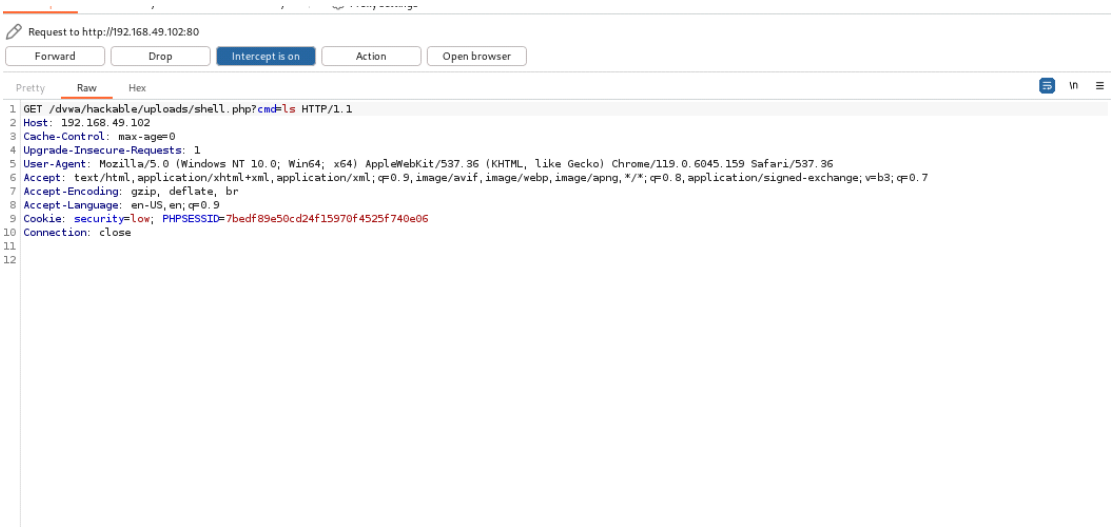
Report

Quello che abbiamo effettuato oggi è un attacco web app nei confronti della macchina Metasploitable, scrivendo una shell per eseguire comandi su meta da remoto (tramite URL). Per comprendere il funzionamento e per immedesimarci nei panni di un hacker etico abbiamo utilizzato burpsuite per analizzare i pacchetti che passano, quello che abbiamo visto è:



Come possiamo notare la richiesta GET ci permette di capire che siamo in un file chiamato "shell.php" dentro gli uploads.

Ritornando all'attacco, quello che spunta a video è:

Screenshot 2024-02-22 at 10-47-06 Metasploitable_hvqy3m.pdf.png dvwa_email.png shell.php

Vediamo che all'interno degli uploads c'è uno screenshot (che abbiamo

precedentemente inserito per verificare il funzionamento della shell). Questa non è l'unica cosa che possiamo vedere, perchè possiamo modificare nell'URL il comando da eseguire (in questo caso ls), andando a inserire ad esempio "echo "Hello World"" e vedremo che spunta a video Hello World. Possono essere eseguiti tutti i comandi di linux.