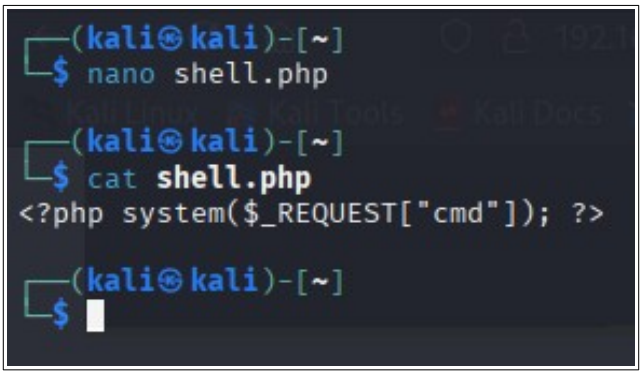
Report Exploit file upload W13D1

In questo esercizio dovremo caricare una shell.php sulla DVWA di Metasploitable 2, prima di cominciare l'esercizio assicuriamoci che le vm di Kali e Metasploitable siano sulla stessa rete e che possano comunicare tra loro.

Step 1 Creiamo un file .php contenente una shell semplice da caricare successivamente sulla DVWA.



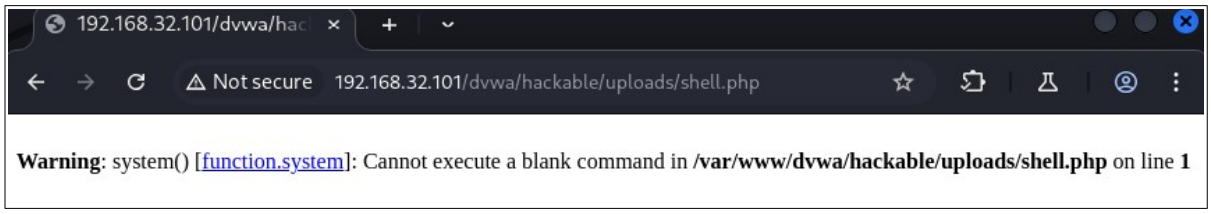
Step 2 Apriamo burpsuite e dal browser del programma colleghiamoci alla DVWA di Metasploitable 2 digitando l'IP della macchina in questione e selezionando la voce DWVA dal menu.

Step 3 Selezioniamo la difficoltà LOW e spostiamoci sulla sezione File Upload del menu e selezioniamo come file da caricare la shell.php creata in precedenza.

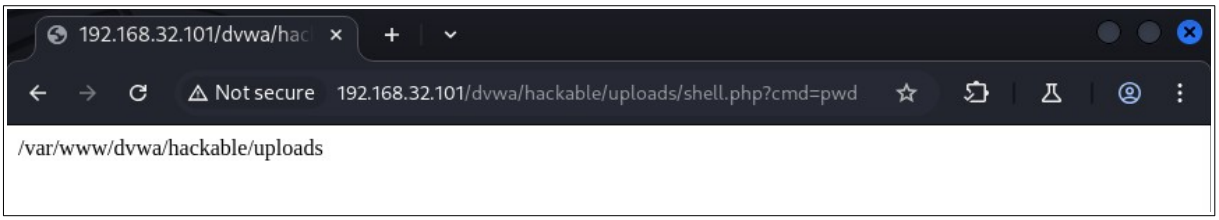
Step 4 Prima di premere Upload, spostiamoci su Burp Suite ed attiviamo l'intercettazione.

Step 5 Carichiamo il file selezionato, apparirà a schermo un messaggio di accettazione del file, possiamo ora copiare il path in rosso ed incollarlo nell'URL della DVWA per attivare la shell.

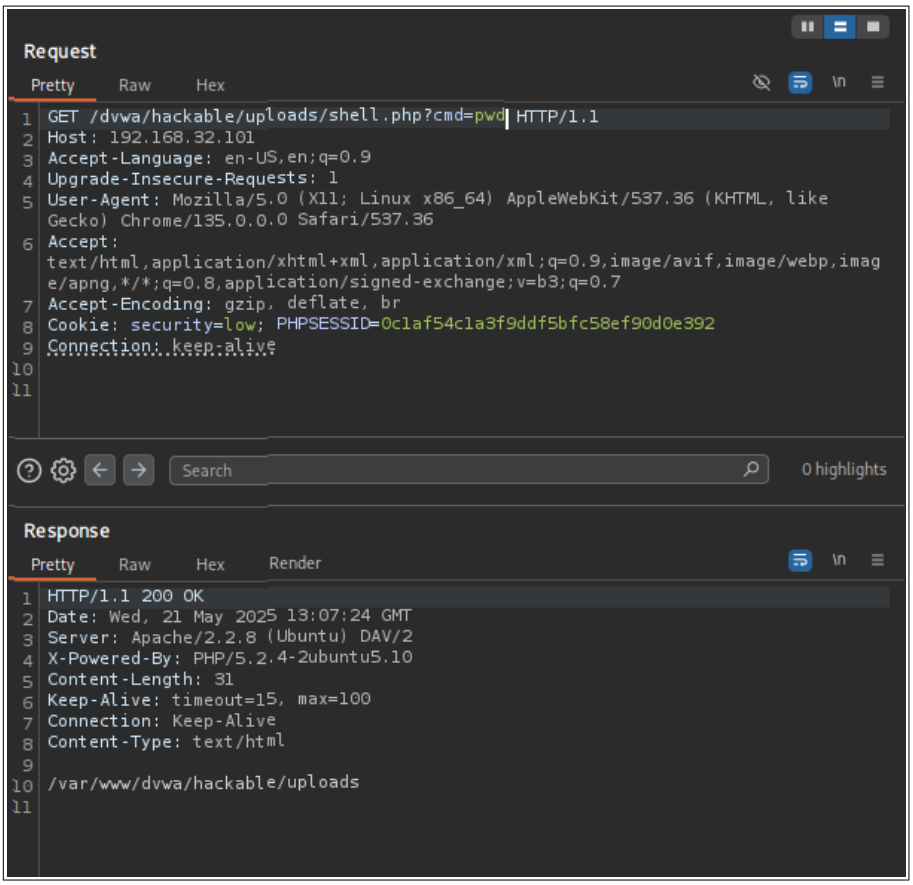
Step 6 La shell è ora attiva ed è in attesa di comandi.



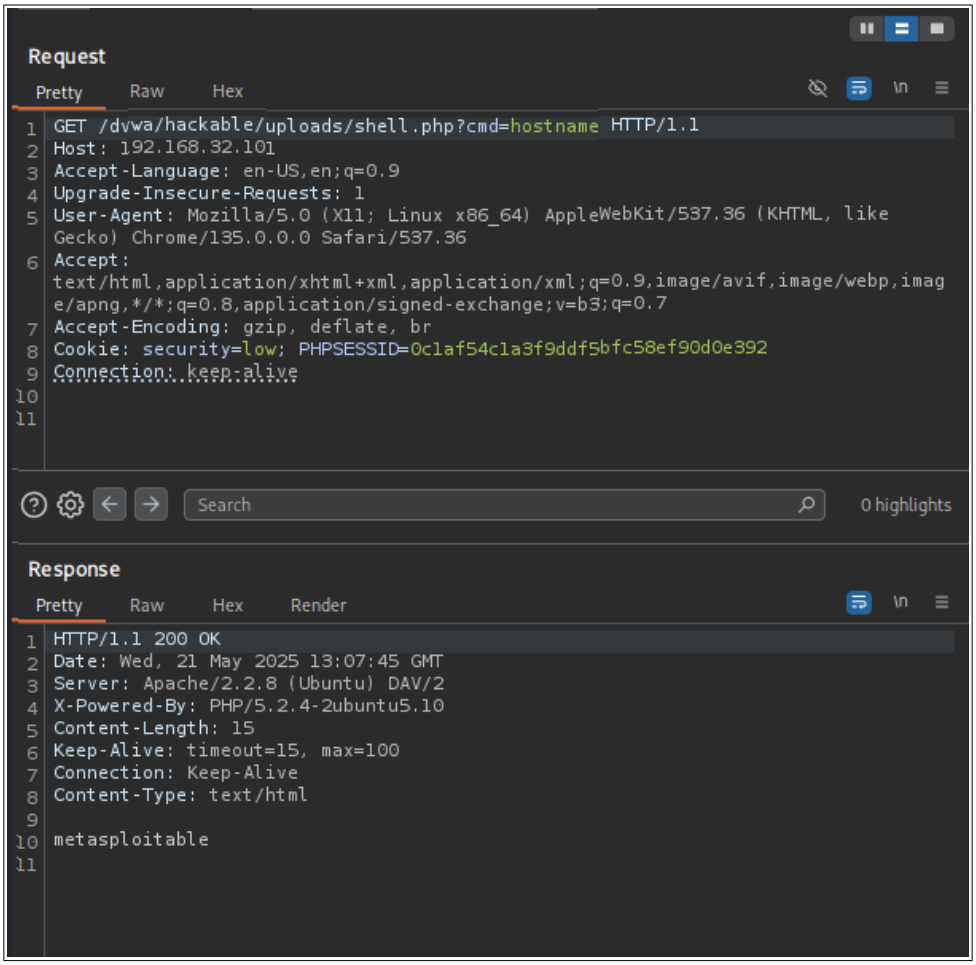
Step 7 Aggiungiamo all'URL: ?cmd=<comando desiderato> per testare la funzionalità della shell.



Step 8 Possiamo eseguire comandi sulla shell anche modificando la richiesta GET catturata con Burp Suite, selezioniamo la richiesta GET contenente il comando e con il tasto destro selezioniamo Repeater.



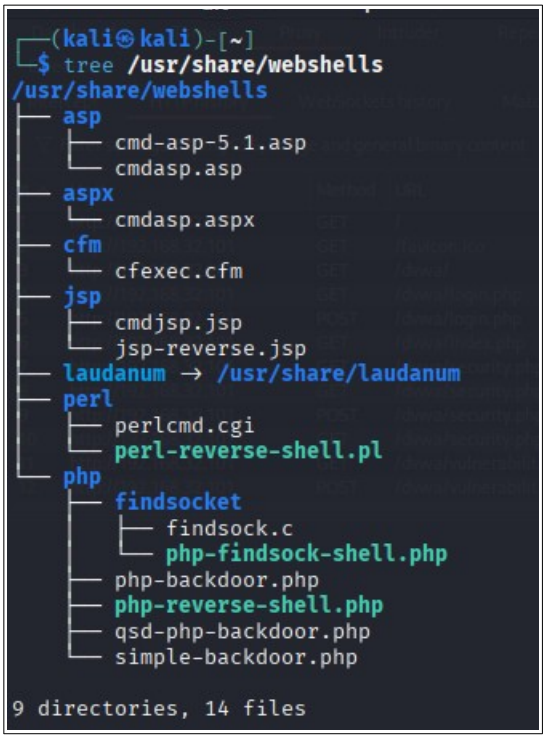
Step 9 Possiamo ora modificare il comando da “pwd” a ciò che desideriamo eseguire ed osservare l’output direttamente da Burp Suite.



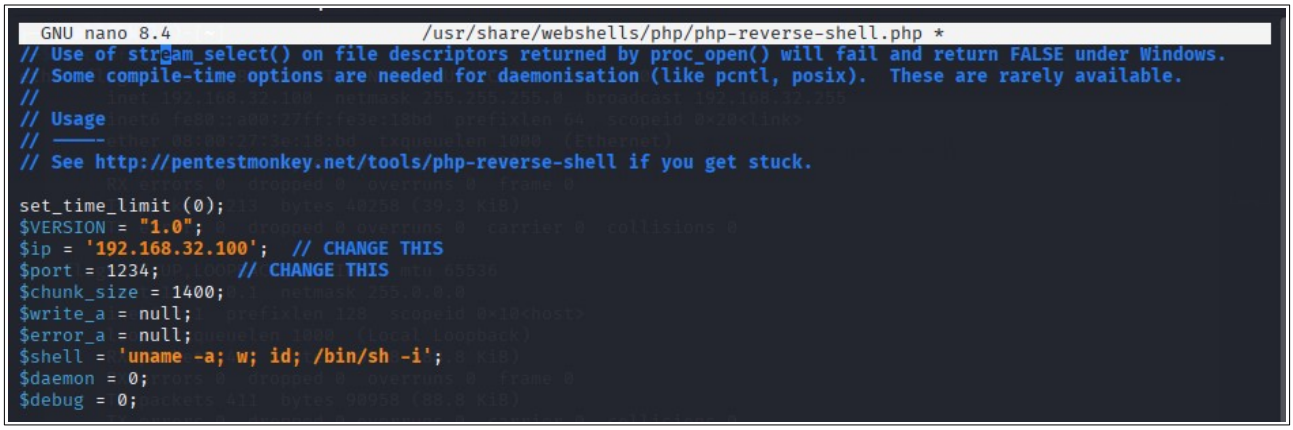
Facoltativo

L’esercizio facoltativo richiede di utilizzare una shell.php più complessa, nel mio caso ho scelto una shell già presente su Kali e ne ho testato l’output.

Step 1 Da Kali spostiamoci nella directoty contenente il file php-reverse-shell-php.



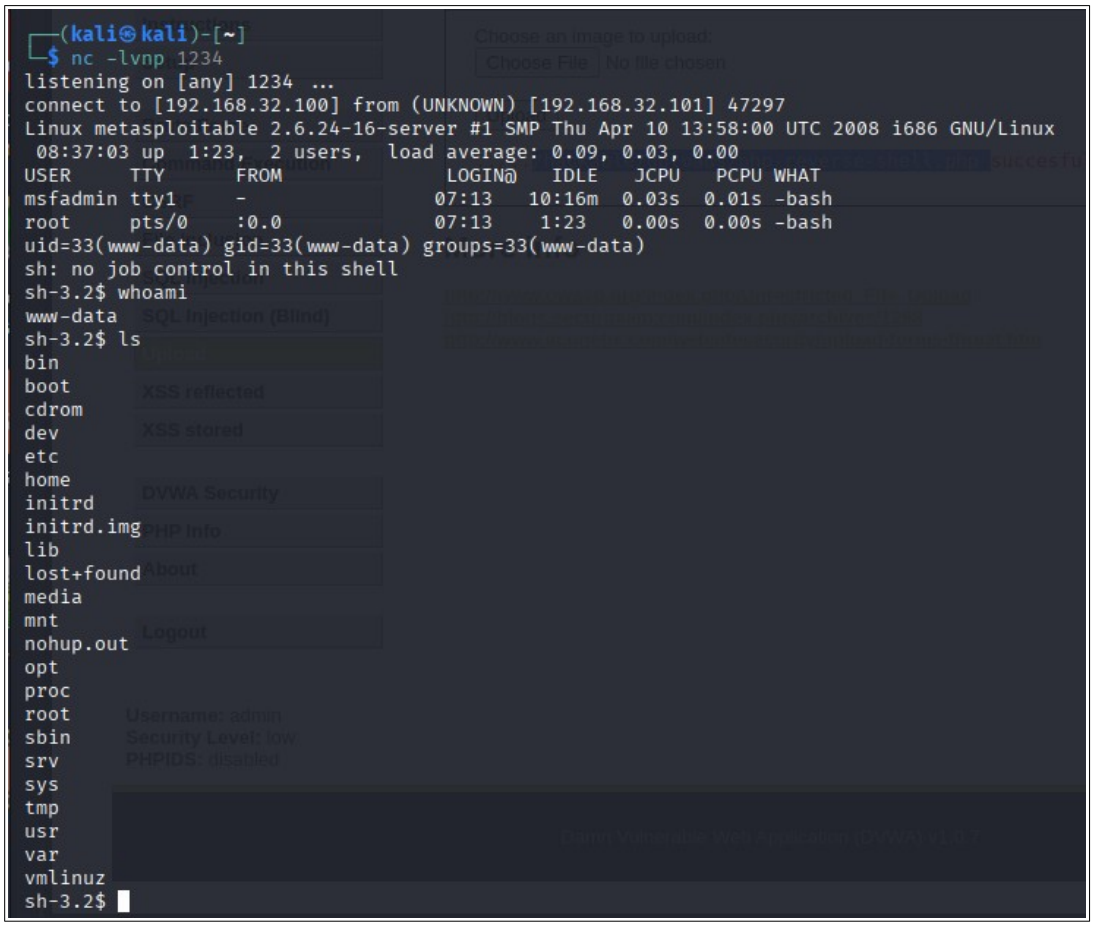
Step 2 Modifichiamo il file in modo che contenga l’IP di Kali.



Step 3 Spostiamoci su un altro terminale e mettiamoci in ascolto con Netcat sulla porta selezionata.

Step 4 Carichiamo il file modificato php-reverse-shell-php sulla DVWA, copiamo il link in rosso ed aggiungiamolo correttamente all'URL della DVWA.

Step 5 Ora dal terminale con Netcat in ascolto potremo eseguire i comandi sulla shell.



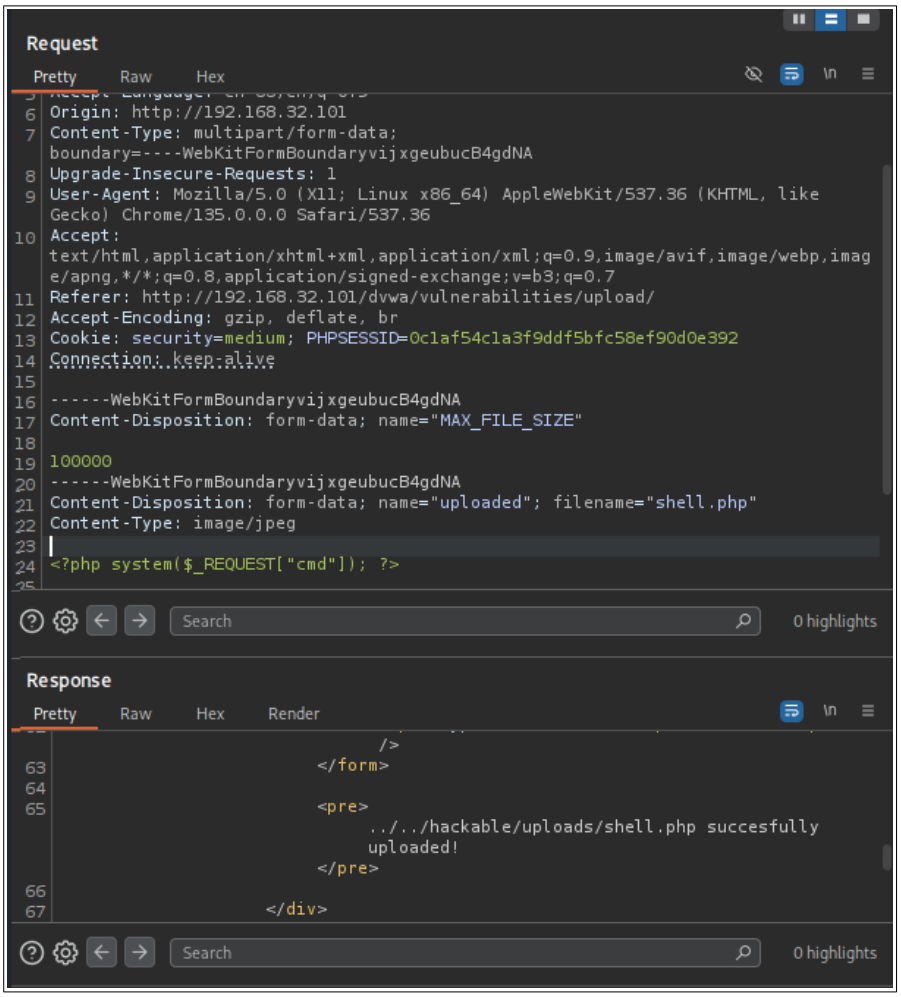
Pratica Extra

Ripetere l’upload della shell in difficoltà MEDIUM e HARD.

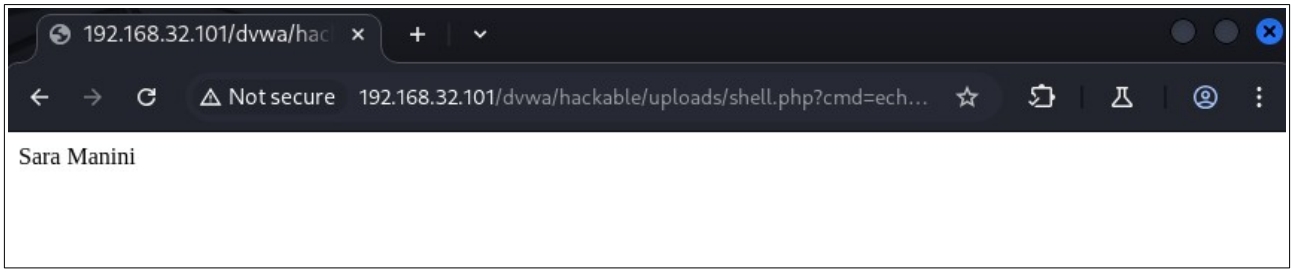
Difficoltà MEDIUM.

Step 1 Se proviamo a caricare il file shell.php come in precedenza, apparirà un messaggio di errore che ci informa che la nostra immagine non è stata caricata. Questo ci fa capire che il file che DVWA si aspetta non è .php ma .jpeg .

Step 2 Catturiamo la richiesta POST con Burp Suite e una volta inviata al Repeater, modifichiamo il campo Content-Type con: “image/jpeg”. Inviamo la richiesta e come possiamo vedere dalla sezione response avremo un messaggio di file caricato correttamente. Potremo ora copiare il path in rosso ed aggiungerlo all’URL della DVWA per accedere alla shell.



Step 3 Aggiungiamo “?cmd=<comando>” per l’esecuzione dei comandi desiderati.



Difficoltà HARD

Step 1 Come visto per la difficoltà MEDIUM, proviamo a caricare il file shell.php normalmente, ma ci apparirà un messaggio di errore che ci informa che la nostra immagine non è stata caricata. Analizziamo il source code della pagina per avere più informazioni, da qui potremo notare che il file che DVWA si aspetta dovrà rispettare diversi parametri.

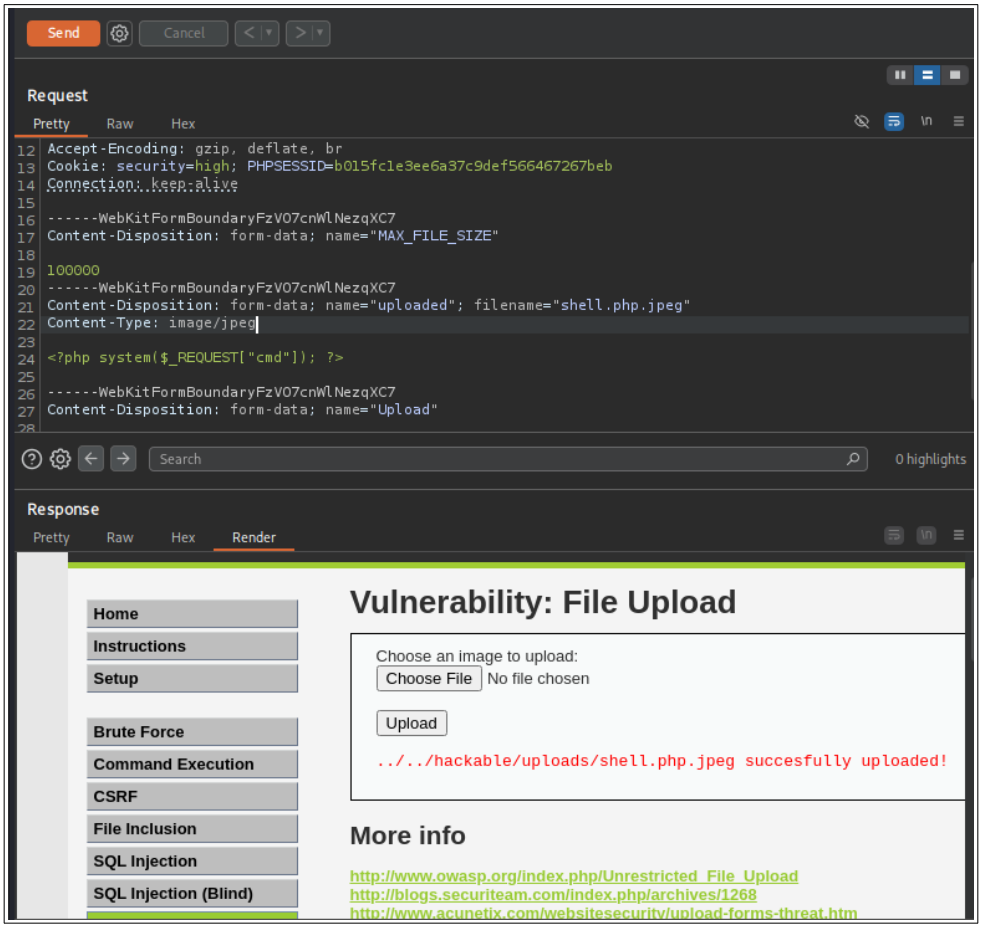
File Upload Source

```
<?php
if (isset($_POST['Upload'])) {

            $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
            $target_path = $target_path . basename($_FILES['uploaded']['name']);
            $uploaded_name = $_FILES['uploaded']['name'];
            $uploaded_ext = substr($uploaded_name, strrpos($uploaded_name, '.') + 1);
            $uploaded_size = $_FILES['uploaded']['size'];

            if (($uploaded_ext == "jpg" || $uploaded_ext == "JPG" || $uploaded_ext == "jpeg" ||
 $uploaded_ext == "JPEG") && ($uploaded_size < 100000)){


                if(!move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path)) {

                    echo '<pre>';
                    echo 'Your image was not uploaded.';
                    echo '</pre>';

                  } else {

                    echo '<pre>';
                    echo $target_path . ' succesfully uploaded!';
                    echo '</pre>';

                    }
            }

            else{

                echo '<pre>';
                echo 'Your image was not uploaded.';
                echo '</pre>';

            }
        }

?>
```

Step 2 Come visto in precedenza, catturiamo con Burp Suite la richiesta POST, inviamola al Repeater e modifichiamo i seguenti campi nella richiesta:

- Filename: shell.php.jpeg
- Content-Type: image/jpeg

Clicchiamo su Send e per visualizzare meglio la risposta selezionaimo Render.
Come possiamo vedere dall'immagine la richiesta è andata a buon fine, possiamo quindi aggiungere il path in rosso all'URL ed accedere alla shell.



Step 3 Aggiungere: ?cmd=<comando> all'URL per poter immettere comandi.