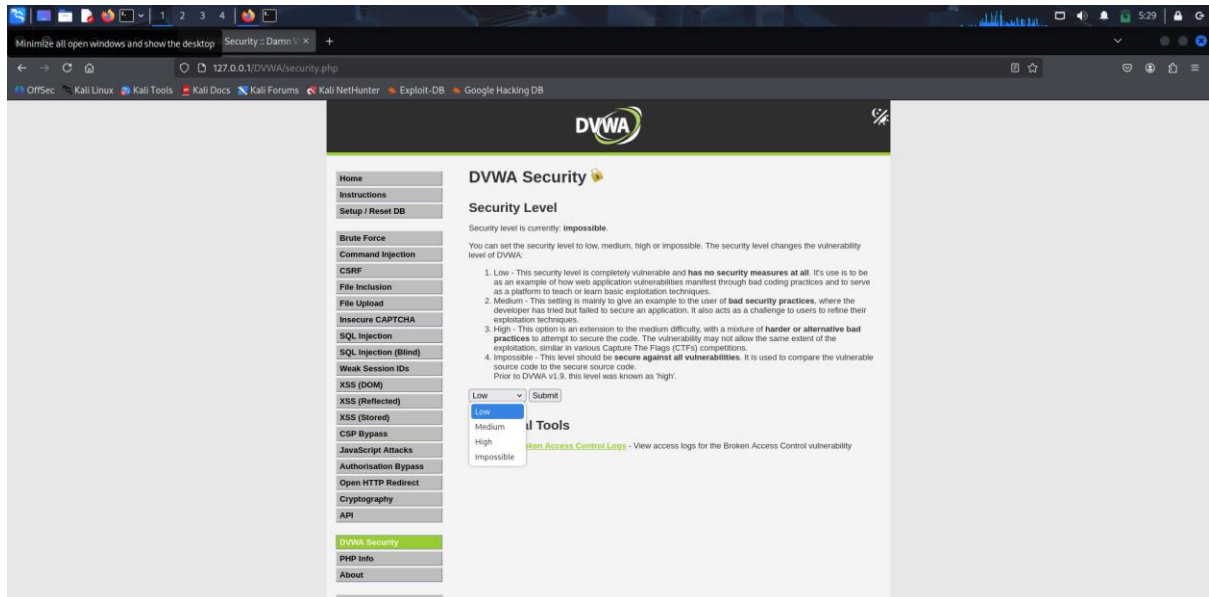
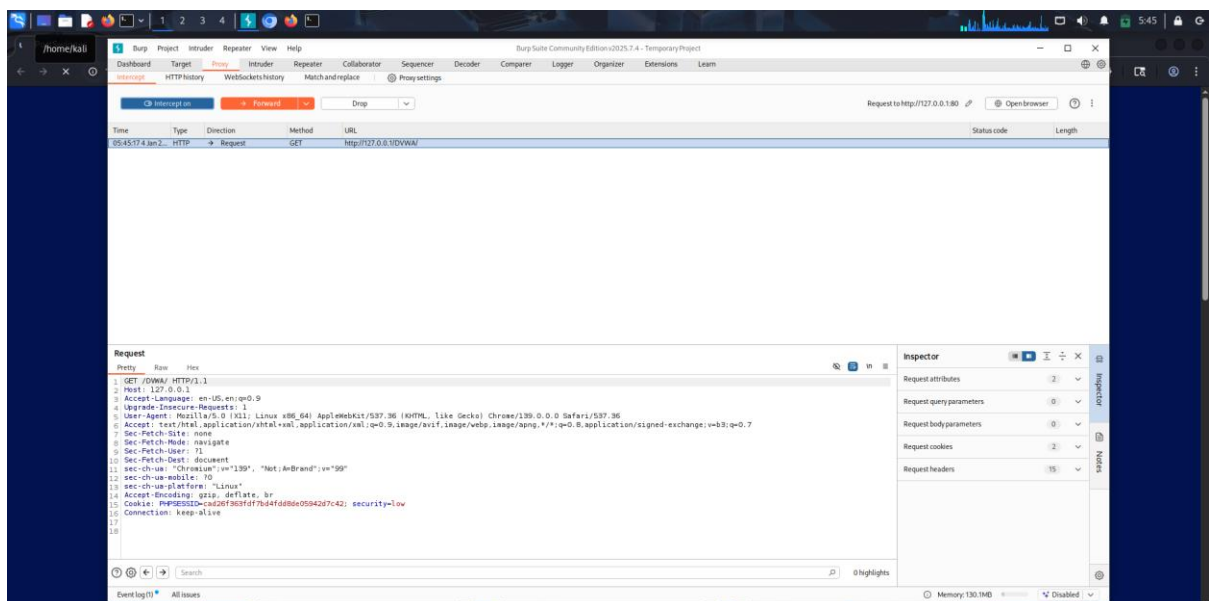


W13D1_ESERCIZIO DVWA- EXPLOIT FILE UPLOAD

Si utilizza la DVWA impostata su un livello di difficoltà basso (estremamente vulnerabile) per andare a vedere le tecniche che consentono di sfruttare le vulnerabilità, in questo caso si sfrutta la vulnerabilità UPLOAD.



In contemporanea, con l'avvio di Burpsuite, si intercettano le richieste che possono essere modificate grazie all'avvio di una pagina web ed inserendo l'indirizzo della DVWA (damn vulnerable web application).



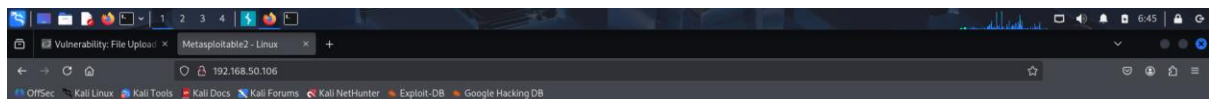
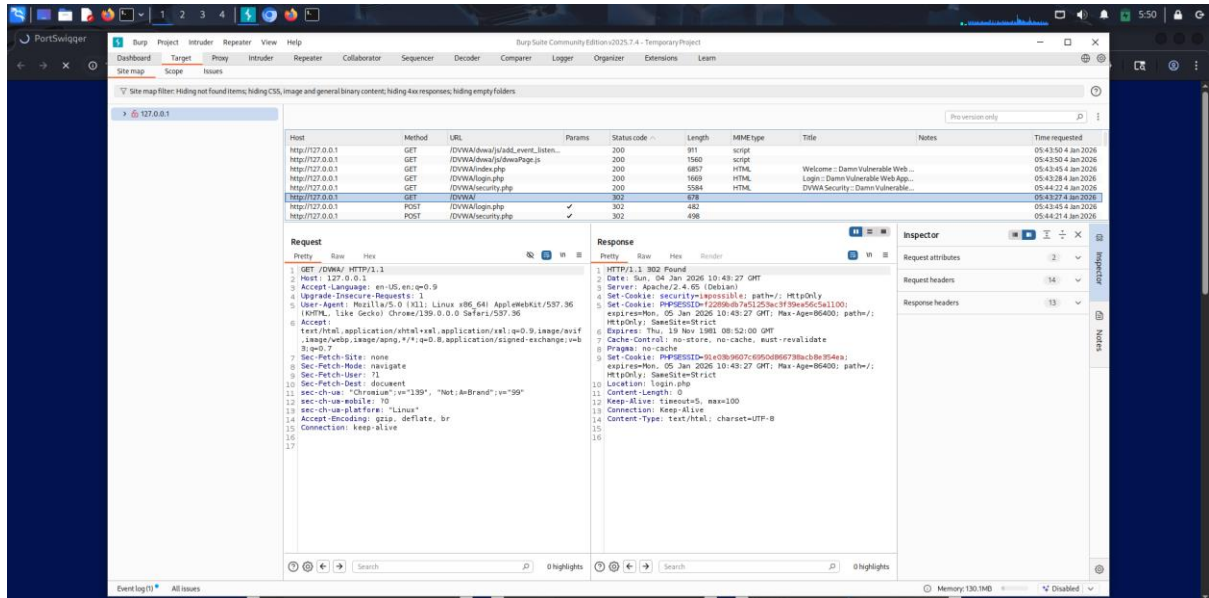
Si iniziano a vedere le prime informazioni raccolte che sono:

-GET

-LIVELLO SICUREZZA

-SISTEMA OPERATIVO

-COOKIE

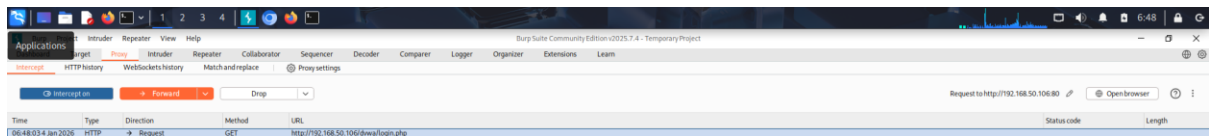


metasploit

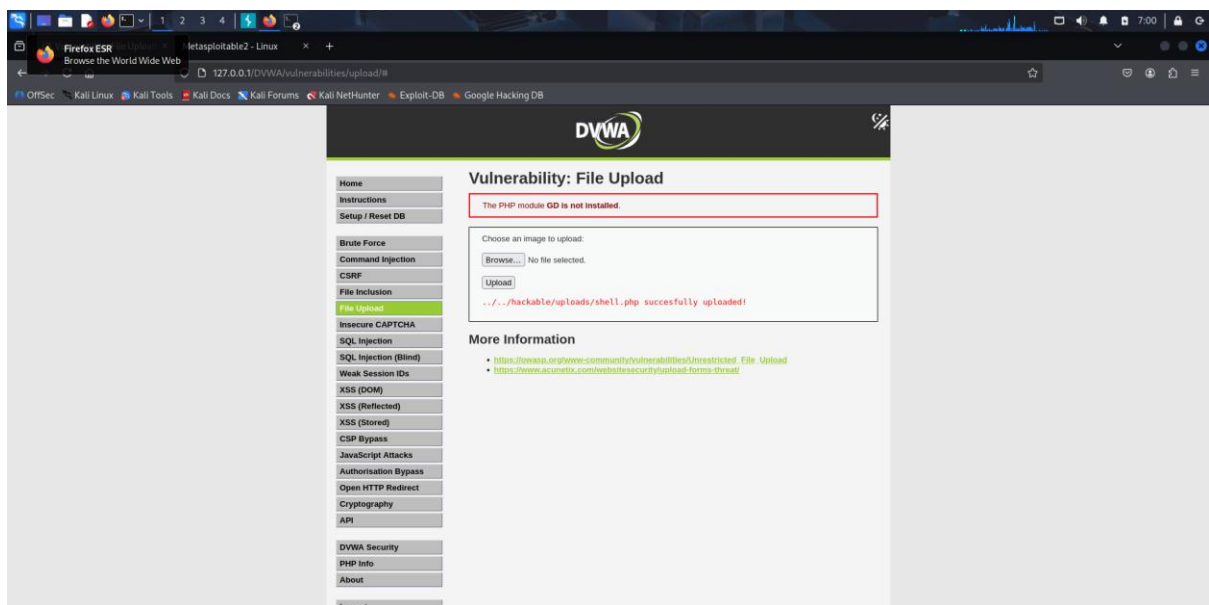
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

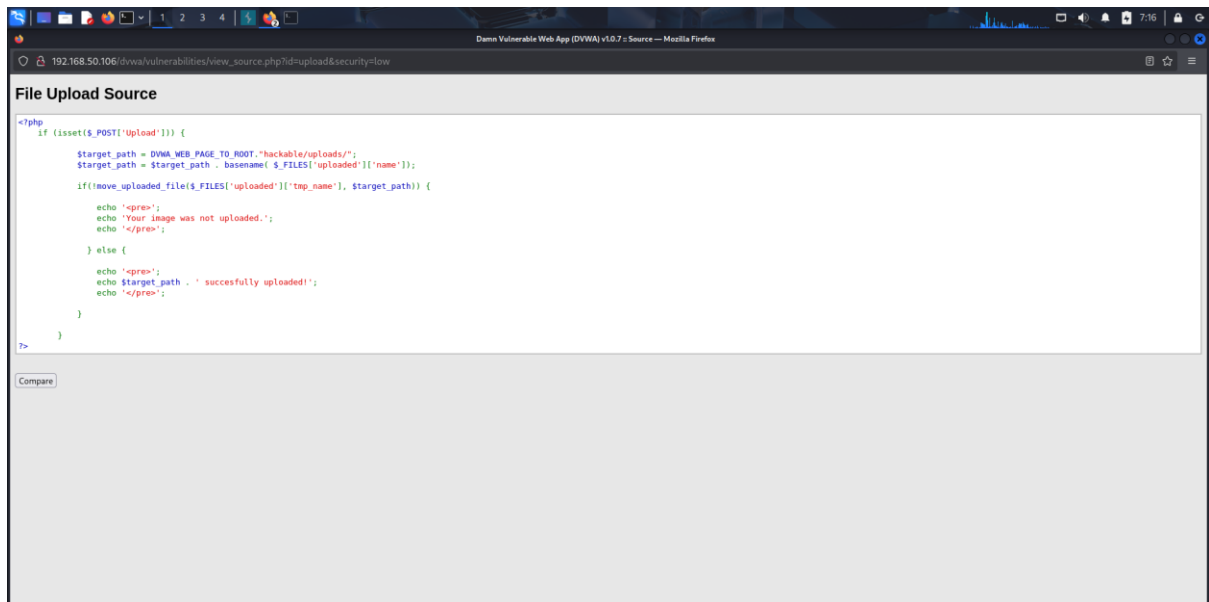
- [TWiki](#)
- [phpMyAdmin](#)
- [Mutiillidae](#)
- [DVWA](#)
- [WebDAV](#)

Si esegue tramite burpsuite la connessione a metaspotable e si lascia attiva l'attività di cattura.



Si prosegue caricando sulla DVWA una shell.php andando a sfruttare la vulnerabilità upload come già detto.





The screenshot shows a web browser window with the address bar displaying `192.168.50.106/dvwa/vulnerabilities/view_source.php?id=upload&security=low`. The page title is "File Upload Source". The main content area displays the PHP source code for the file upload functionality. The code includes a check for the 'Upload' POST variable, sets a target path to `DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/"`, and uses `move_uploaded_file` to upload the file. It also includes echo statements to provide feedback to the user.

```
<?php
if (isset($_POST['Upload'])) {
    $target_path = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path = $target_path . basename( $_FILES['uploaded']['name']);

    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 . " successfully uploaded!";
        echo "</pre>";
    }
}
?>
```

Below the code, there is a "Compare" button.

La shell.php è stata correttamente caricata come restituisce anche il risultato del caricamento.