Traccia:

Si richiede alla studente di scaricare la macchina .OVA da uno dei due link proposti di seguito.

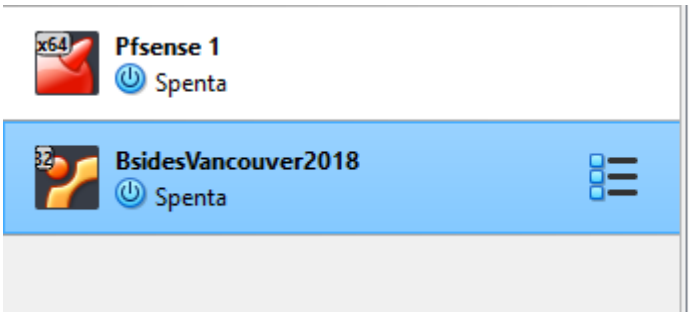
- https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/
- https://github.com/samiux/samiux.github.io/blob/master/ctf-bsides-vancouver-2018.md

Una volta completato il download, un doppio click dovrebbe essere sufficiente per lanciare la nuova macchina all'interno del virtualizzatore.

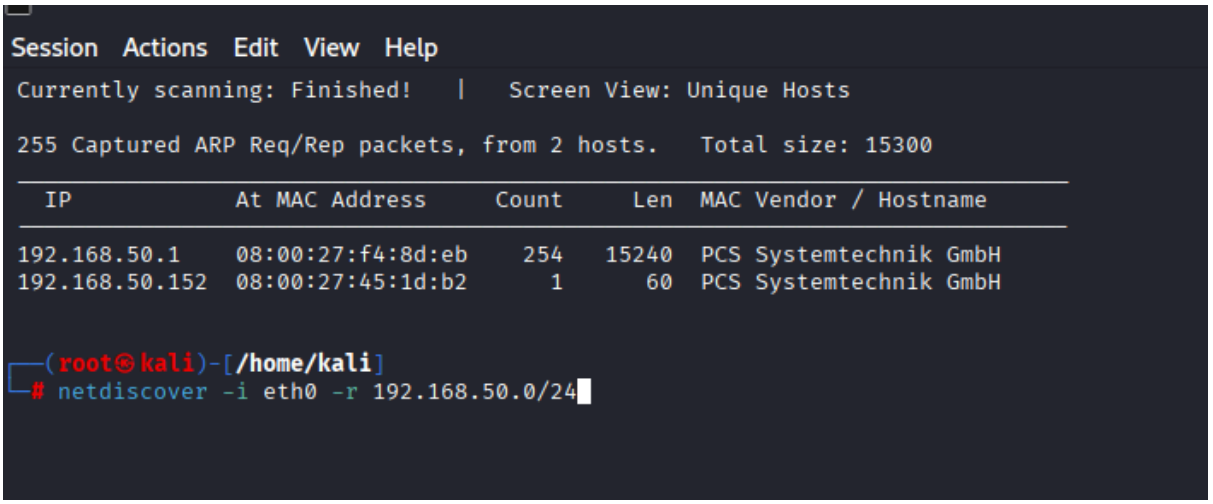
L'obiettivo dello studente è quello di eseguire un VA/PT completo sulla macchina bersaglio, e documentare efficacemente il suo lavoro al fine di produrre un report esaustivo.

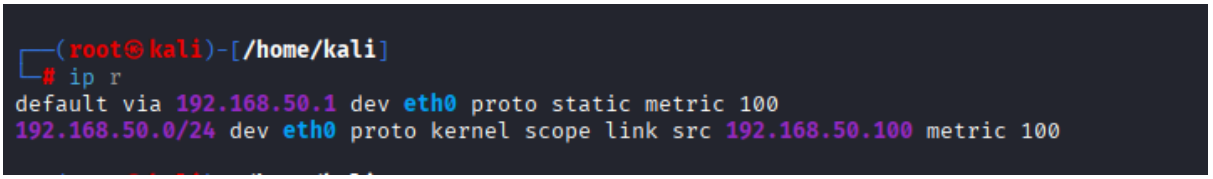
Il lavoro deve essere svolto individualmente.

SVOLGIMENTO:



ho scaricato e importato la macchina da uno dei 2 link proposti dalla traccia dell'esercizio ho innanzitutto impostato la macchina dalle impostazioni di rete in rete interna perchè se fosse stato in NAT come era di default non avrebbe funzionato.

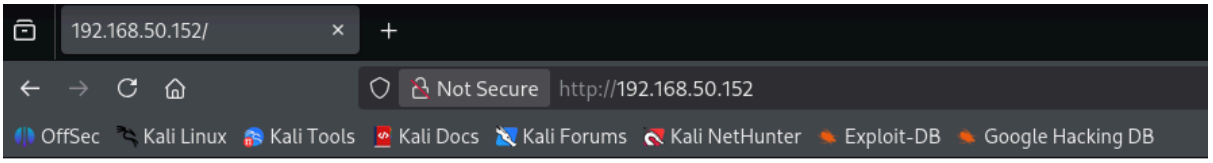




ho lanciato il comando netdiscover come nello screenshot sopra e ha trovato 2 ip per identificare quello della macchina target ho fatto un ip r per vedere l'indirizzo del gateway ed escluderlo, l'ip della nostra macchina target è quindi 192.168.50.152.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.152 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 12:42 EST
Nmap scan report for 192.168.50.152
Host is up (0.000047s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:45:1D:B2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
```

avendo l'ip della macchina ho lanciato un nmap per vedere quali porte erano aperte.



It works!

This is the default web page for this server.

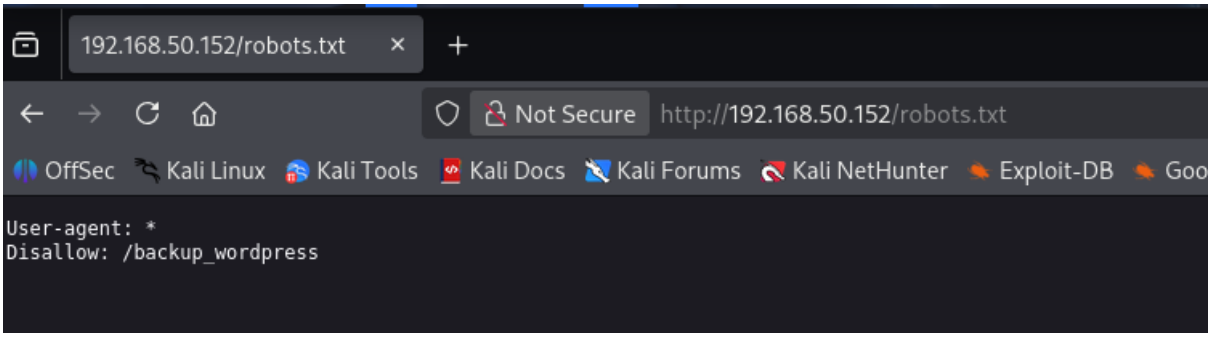
The web server software is running but no content has been added, yet.

ci sono 3 porte aperte ho deciso di provare la porta 80 con il servizio HTTP e ha funzionato

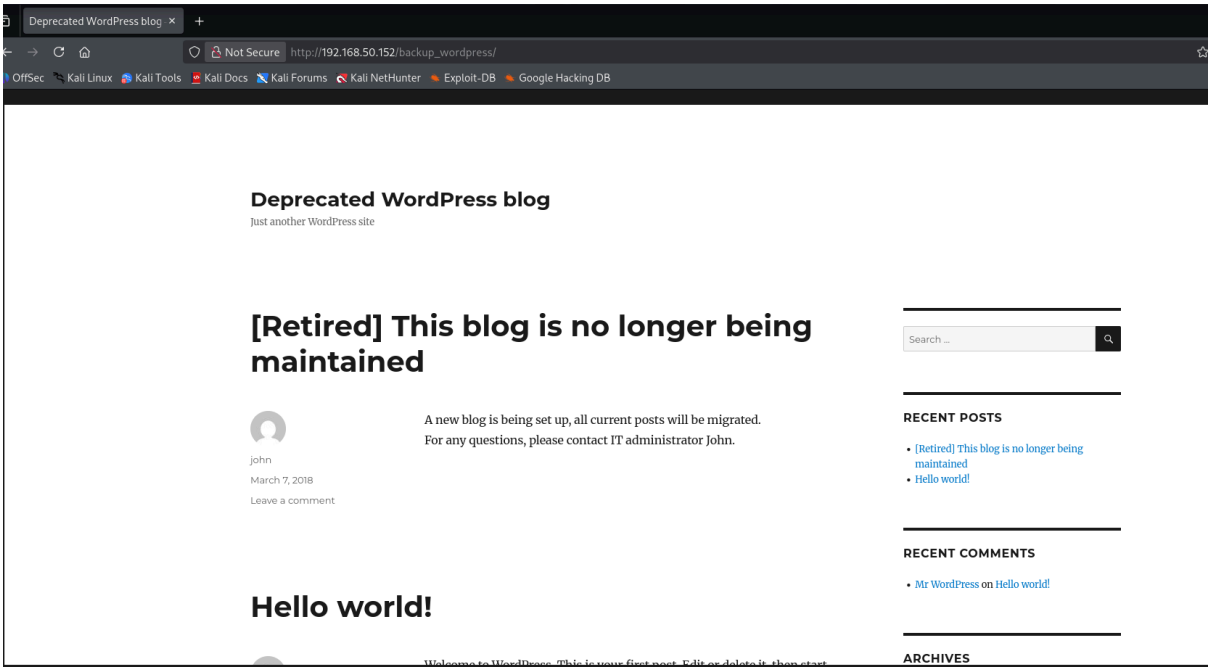
```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://192.168.50.152

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Nov  3 13:02:05 2025
URL_BASE: http://192.168.50.152/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.50.152/ ----
+ http://192.168.50.152/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.50.152/index (CODE:200|SIZE:177)
+ http://192.168.50.152/index.html (CODE:200|SIZE:177)
+ http://192.168.50.152/robots (CODE:200|SIZE:43)
+ http://192.168.50.152/robots.txt (CODE:200|SIZE:43)
+ http://192.168.50.152/server-status (CODE:403|SIZE:295)

-----------------
END_TIME: Mon Nov  3 13:02:06 2025
DOWNLOADED: 4612 - FOUND: 6
```

ho usato la dirb che è un comando di directory brute force per il web ha dato informazioni su quando è iniziata la scansione quante parola ha generato 4612 il codice 200 ha identificato

che ce una risorsa il codice 403 la risorsa esiste ma è forbidden quindi l’accesso è proibito potrebbero esserci protezioni o permessi.



a questo punto da dirb ho notato un robots.txt con una risposta 200 quindi ho provato ad andare di nuovo sul web aggiungendo robots.txt per vedere cosa mi diceva.
mi ha dato un'altra informazione /backup_wordpress



ci ha indirizzato su un sito wordpress e in alla sinistra possiamo notare che non e più in manutenzione.

```
┌──(root㉿kali)-[/home/kali]
└─# wpscan http://192.168.50.152/backup_wordpress/
One of the following options is required: --url, --update, --help, --hh, --version

Please use --help/-h for the list of available options.

┌──(root㉿kali)-[/home/kali]
└─# wpscan --url  http://192.168.50.152/backup_wordpress/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.50.152/backup_wordpress/ [192.168.50.152]
[+] Started: Mon Nov  3 13:43:00 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.2.22 (Ubuntu)
 |  - X-Powered-By: PHP/5.3.10-1ubuntu3.26
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.50.152/backup_wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

```
[+] XML-RPC seems to be enabled: http://192.168.50.152/backup_wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.50.152/backup_wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.50.152/backup_wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.5 identified (Insecure, released on 2016-04-12).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.50.152/backup_wordpress/?feed=rss2, <generator>https://wordpress.org/?v=4.5</generator>
 |  - http://192.168.50.152/backup_wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.5</generator>

[+] WordPress theme in use: twentysixteen
 | Location: http://192.168.50.152/backup_wordpress/wp-content/themes/twentysixteen/
 | Last Updated: 2025-08-05T00:00:00.000Z
 | Readme: http://192.168.50.152/backup_wordpress/wp-content/themes/twentysixteen/readme.txt
 | [!] The version is out of date, the latest version is 3.6
 | Style URL: http://192.168.50.152/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthead wi ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.50.152/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5, Match: 'Version: 1.2'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <
```

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 <=========================================

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Nov  3 13:43:05 2025
[+] Requests Done: 187
[+] Cached Requests: 5
[+] Data Sent: 51.382 KB
[+] Data Received: 22.698 MB
[+] Memory used: 278.324 MB
[+] Elapsed time: 00:00:05

┌──(root㉿kali)-[/home/kali]
└─# 
```

ho effettuato una scansione con wpscan per identificare le vulnerabilità e ne ha trovate alcune.

```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.50.152
Connected to 192.168.50.152.
220 (vsFTPd 2.3.5)
Name (192.168.50.152:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||52275|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||42354|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> 
```

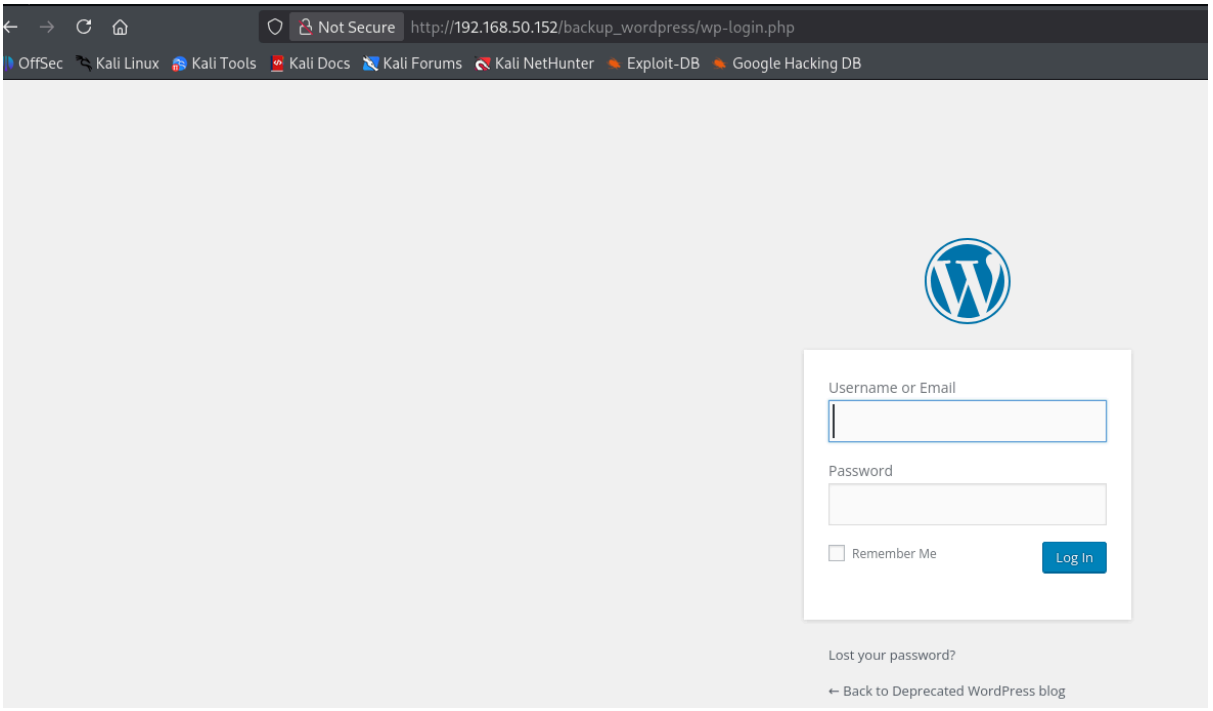
attraverso il comando ftp che mi permette di connettersi in maniera interattiva ad un server ftp di navigare nelle directory era presente una directory pubblica infatti da ftp ho notato la presenza di un file user.txt.bk.

```
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||22583|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****************************************************************************************************************************************************************************************|    31       32.72 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (32.72 KiB/s)
ftp> 
```

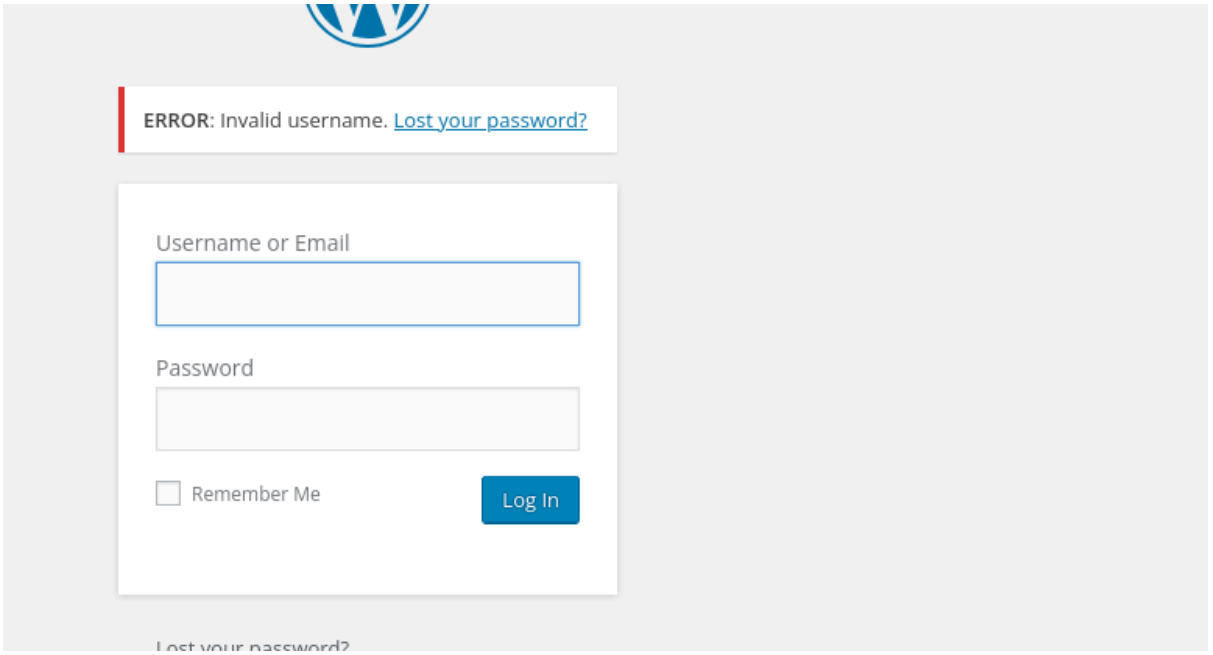
ho scaricato il file trovato

```
?Invalid command.
ftp> exit
221 Goodbye.

┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop    Downloads  esercizio.OLD  gameshell.1        gameshell.sh        mechiamopippo.nmap  Music     Public                scansionemeta.xml.nmap  Templates  Videos
Documents  esercizio  gameshell      gameshell-save.sh  mechiamopippo.gnmap  mechiamopippo.xml   Pictures  scansionemeta.xml.gnmap  scansionemeta.xml.xml   users.txt.bk

┌──(root㉿kali)-[/home/kali]
└─# cat users.txt.bk
abatchy
john
mai
anne
doomguy

┌──(root㉿kali)-[/home/kali]
└─# 
```

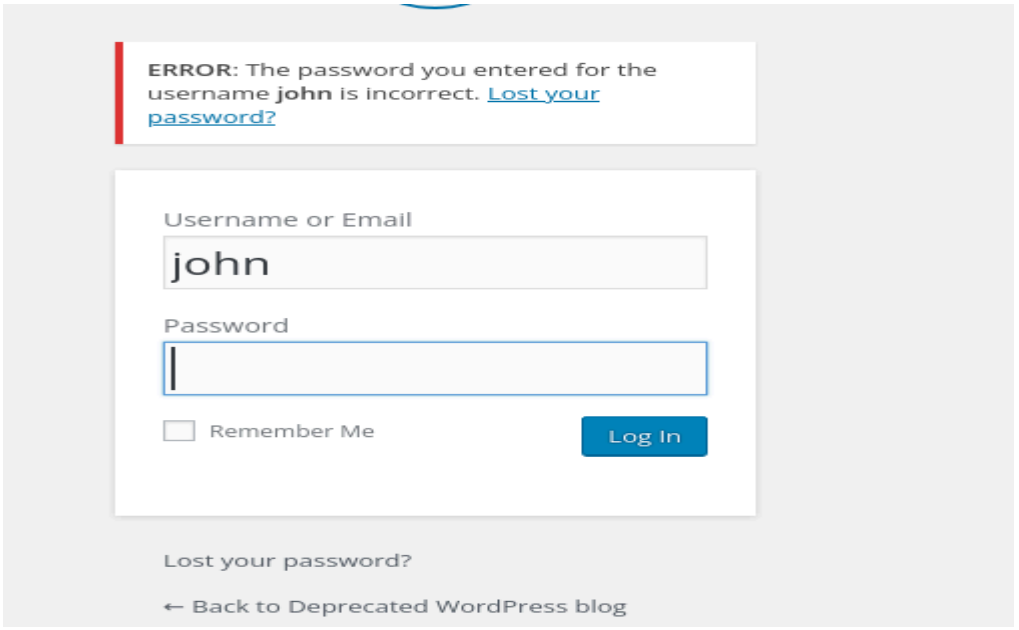
ho aperto il documento trovato



sono andata sul sito per provare le credenziali trovate sul documento



ho provato con anne ma mi dice invalid username



john è un username valido ma la password è sbagliata.
purtroppo mi sono bloccata qua anche a causa delle macchine virtuali che avevano problemi (e la scadenza incombeva la didattica mi ha aperto la consegna per 24 ore) mi dispiace non essere potuta andare avanti.