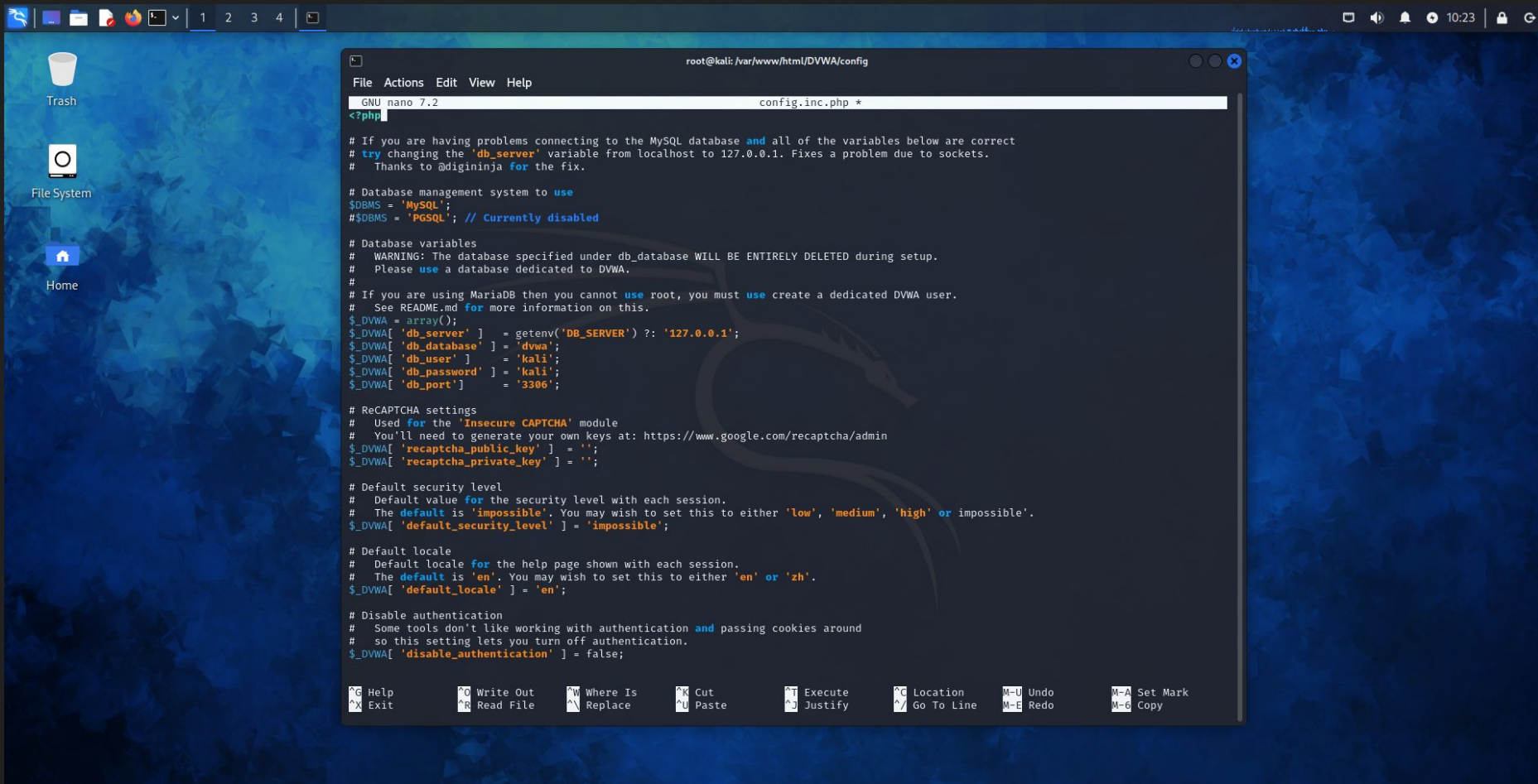
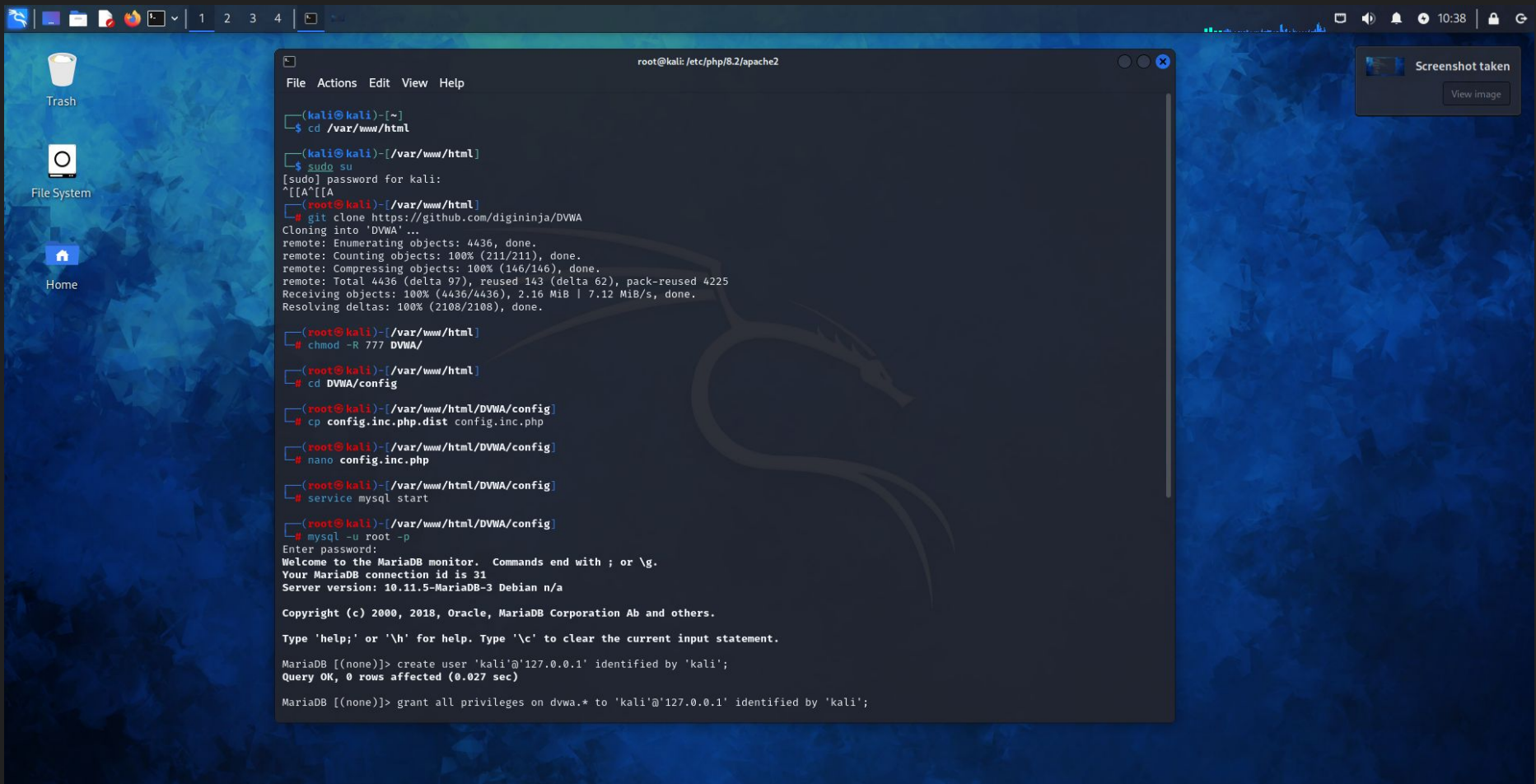


eseguo i comandi per creare il database DVWA

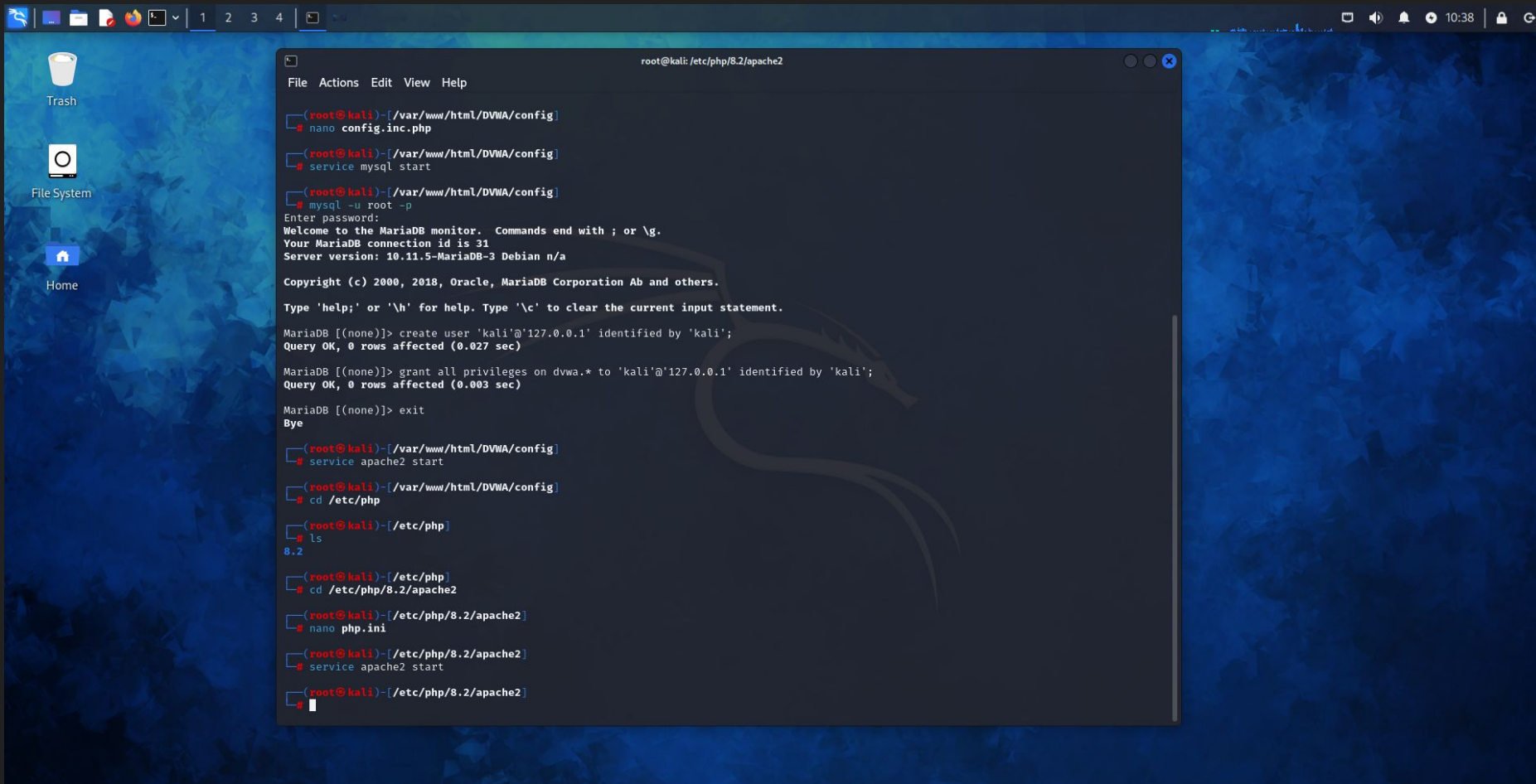


Modifico password e username all'interno del file config

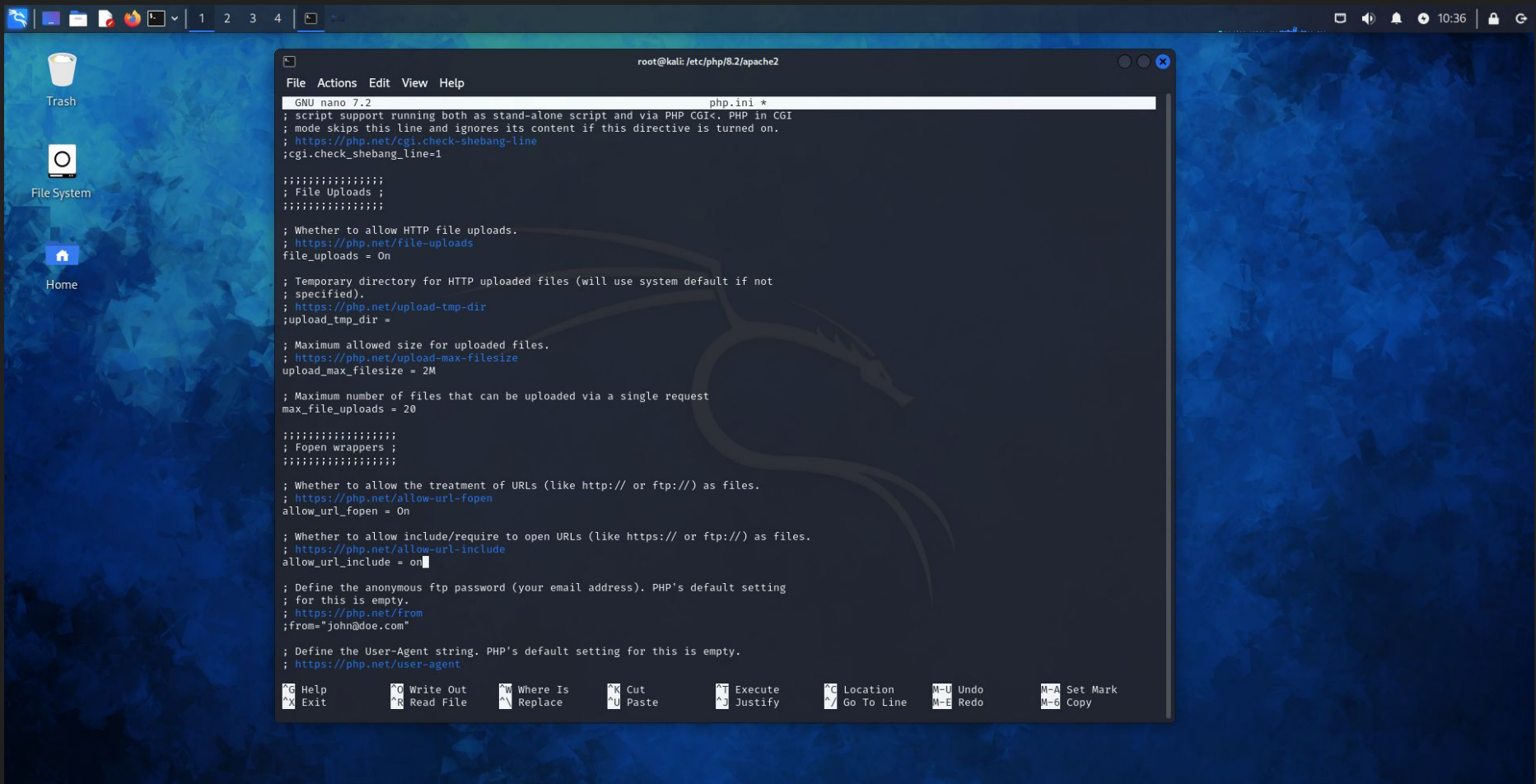


procedo con i comandi per impostare i permessi all'user creato

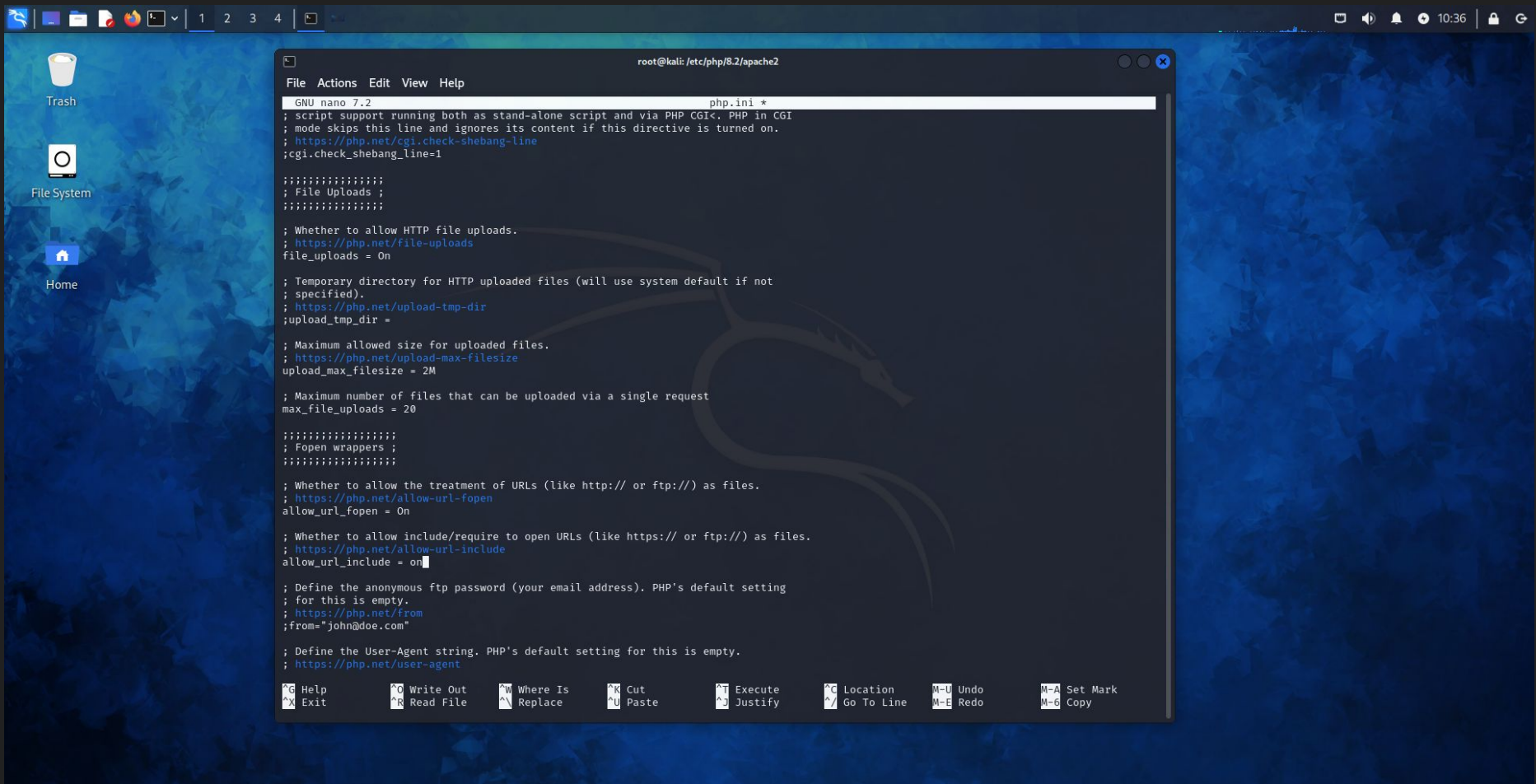




avviamo apache2, modifichiamo il suo file di configurazione(slide seguente) e lo riavviamo



Modifico i campi allow\_url\_fopen allow\_url\_include su on e salvo il file



Modifico i campi allow\_url\_fopen allow\_url\_include su on e salvo il file

The screenshot shows a Kali Linux desktop environment with a web browser open to the DVWA (Damn Vulnerable Web Application) setup page. The browser's address bar shows the URL `127.0.0.1/DVWA/setup.php`. The page has a sidebar on the left with three tabs: 'Setup DVWA' (highlighted in green), 'Instructions', and 'About'. The main content area is titled 'Database Setup' and contains the following text:

Click on the 'Create / Reset Database' button below to create or reset your database.  
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**  
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

---

**Setup Check**

Web Server SERVER\_NAME: `127.0.0.1`

Operating system: `*nix`

PHP version: `8.2.10`  
PHP function display\_errors: **Disabled**  
PHP function display\_startup\_errors: **Disabled**  
PHP function allow\_url\_include: **Disabled**  
PHP function allow\_url\_fopen: **Enabled**  
PHP module gd: **Missing - Only an issue if you want to play with captchas**  
PHP module mysqli: **Installed**  
PHP module pdo\_mysql: **Installed**

Backend database: **MySQL/MariaDB**  
Database username: `kali`  
Database password: `*****`  
Database database: `dvwa`  
Database host: `127.0.0.1`  
Database port: `3306`

reCAPTCHA key: **Missing**

Writable folder `/var/www/html/DVWA/hackable/uploads/`: **Yes**  
Writable folder `/var/www/html/DVWA/config/`: **Yes**

**Status in red**, indicate there will be an issue when trying to complete some modules.

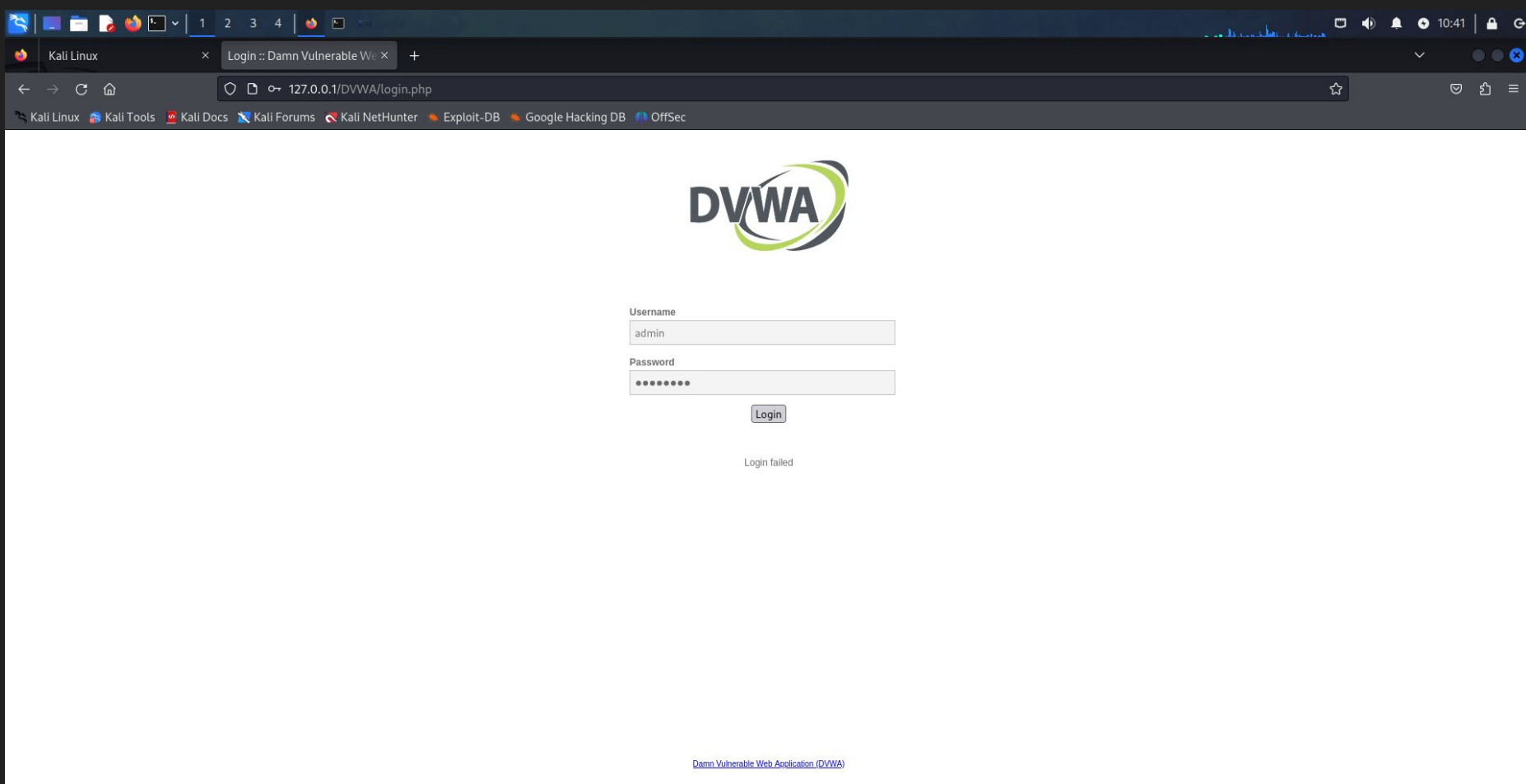
If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

`allow_url_fopen = On`  
`allow_url_include = On`

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

At the bottom of the page, there is a button labeled 'Create / Reset Database'.

accedo all'indirizzo `127.0.0.1/DVWA/setup.php` e clicco Create/Reset Database



accedo con l'username "admin" e la password "password"



The image shows a web browser window on the left displaying the DVWA (Damn Vulnerable Web Application) login page. The page has a logo at the top and a login form with fields for 'Username' and 'Password', and a 'Login' button. The browser's address bar shows the URL '127.0.0.1/DVWA/login.php'.

On the right, the Burp Suite Community Edition interface is visible. The 'Proxy' tab is active, and the 'Intercept' button is highlighted. The 'Intercept is on' button is also visible. The 'Request to http://127.0.0.1:80' is being intercepted. The 'Raw' tab is selected, showing the raw HTTP request data. The request is a POST to '/DVWA/login.php' with the following headers and body:

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 91
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=8kvjub44s160vid2d0m5lih91r; security=impossible
21 Connection: close
22
23 username=username&password=password&Login=Login&user_token=a4c97593e5d2ffb16996d540072daf5
```

The 'Inspector' tab on the right shows the request details, including request attributes, query parameters, body parameters, cookies, and headers.

Avvio burpsuit e attivo proxy e browser, inserisco i dati d'accesso

The image shows a web browser window displaying the DVWA (Damn Vulnerable Web Application) login page. The page has a logo at the top and a login form with fields for "Username" and "Password", and a "Login" button. The browser address bar shows the URL "127.0.0.1/DVWA/login.php".

Overlaid on the browser window is the Burp Suite Community Edition v2023.10.3.5 interface. The "Repeater" tab is active, showing a list of requests. The selected request is a POST to "/DVWA/login.php" with the following details:

- Method: POST
- URL: /DVWA/login.php
- Host: 127.0.0.1
- Content-Length: 96
- Cache-Control: max-age=0
- sec-ch-ua: "Chromium";v="119", "Not?A\_Brand";v="24"
- sec-ch-ua-mobile: ?0
- sec-ch-ua-platform: "Linux"
- Upgrade-Insecure-Requests: 1
- Origin: http://127.0.0.1
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
- 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
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-User: ?1
- Sec-Fetch-Dest: document
- Referer: http://127.0.0.1/DVWA/login.php
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.9
- Cookie: PHPSESSID=8kvjub44s160v1d2d0m5liH91r; security=impossible
- Connection: close
- username=ciao&password=passwordSbagliata&Login=Login&user\_token=a4c975939e5d2ffb16936d540072daf5

The response is an HTTP 302 Found status, indicating a redirect. The response headers show "Content-Type: text/html; charset=UTF-8".


The Burp Suite interface also shows the "Inspector" tab on the right, which displays the request and response details in a structured format.

mando il pacchetto al repeater, apro la scheda "repeater" e clicco send e follow redirection

1 2 3 4

Login :: Damn Vulnerable

127.0.0.1/DVWA/login.php



Username

username

Password

\*\*\*\*\*

Login

Damn Vulnerable Web Application (DVWA)

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

1 x +

Send Cancel < >

Target: http://127.0.0.1 HTTP/1

Request

Raw

1 GET /DVWA/login.php

2 HTTP/1.1

3 Host: 127.0.0.1

4 Cache-Control: max-age=0

5 sec-ch-ua: "Chromium";v="119", "NotA.Brand";v="24"

6 sec-ch-ua-mobile: ?0

7 sec-ch-ua-platform: "Linux"

8 Upgrade-Insecure-Requests: 1

9 Origin: http://127.0.0.1

10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

11 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

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: navigate

14 Sec-Fetch-User: ?1

15 Sec-Fetch-Dest: document

16 Referer: http://127.0.0.1/DVWA/login.php

17 Accept-Encoding: gzip, deflate, br

18 Accept-Language: en-US,en;q=0.9

19 Cookie: PHPSESSID=8kvjub44s16ov1d2d0w51ih9lr; security=impossible

20 Connection: close

Response

Pretty Raw Hex Render

50 Password

51 </label>

52 <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">

53 <br />

54 <p class="submit">

55 <input type="submit" value="Login" name="Login">

56 </p>

57 </fieldset>

58 <input type="hidden" name="user\_token" value="58Se393991c7b4d67f68606ebb1bd702" />

59 </form>

60 <br />

61 <div class="message">

62 Login failed

63 </div>

64 <br />

65 <br />

66 <br />

67 <br />

68 <br />

69 <br />

70 <br />

71 <br />

72 <br />

73 </div>

74 <!--<div id="content">-->

75 <div id="footer">

76 <p>

77 <a href="https://github.com/digininja/DVWA/" target="\_blank">

78 Damn Vulnerable Web Application (DVWA)

79 </a>

80 </p>

81 </div>

82 <!--<div id="footer"> -->

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 18

Response headers 9

0 highlights

0 highlights

1,672 bytes | 1 millis

Come dovrebbe succedere, il server manda una pagina con messaggio "login failed"