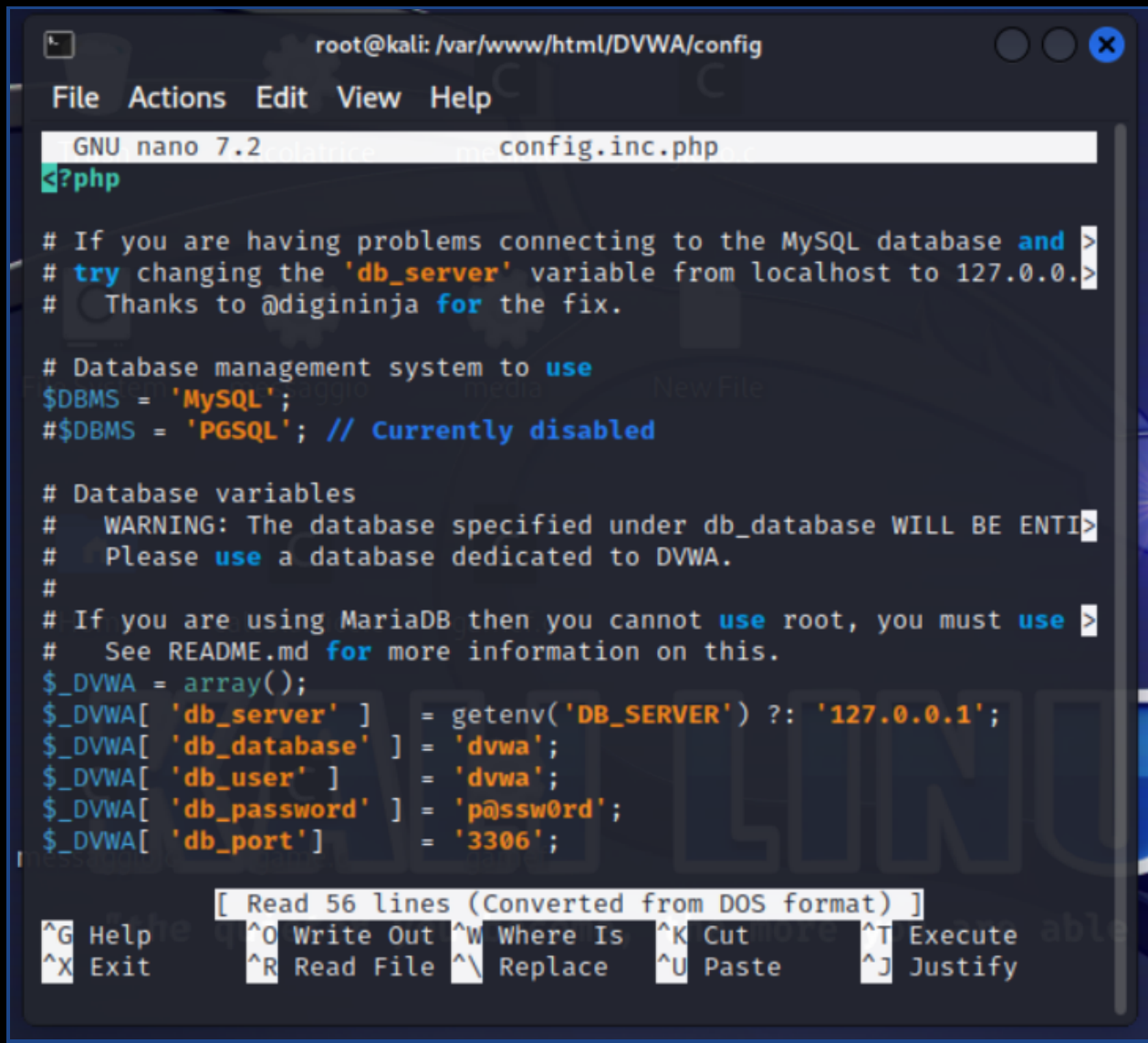


Pratica S3L2

Configurazione DVWA e utilizzo pratico del tool Burpsuite.

Configurazione DVWA

1°



```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 7.2 config.inc.php
<?php

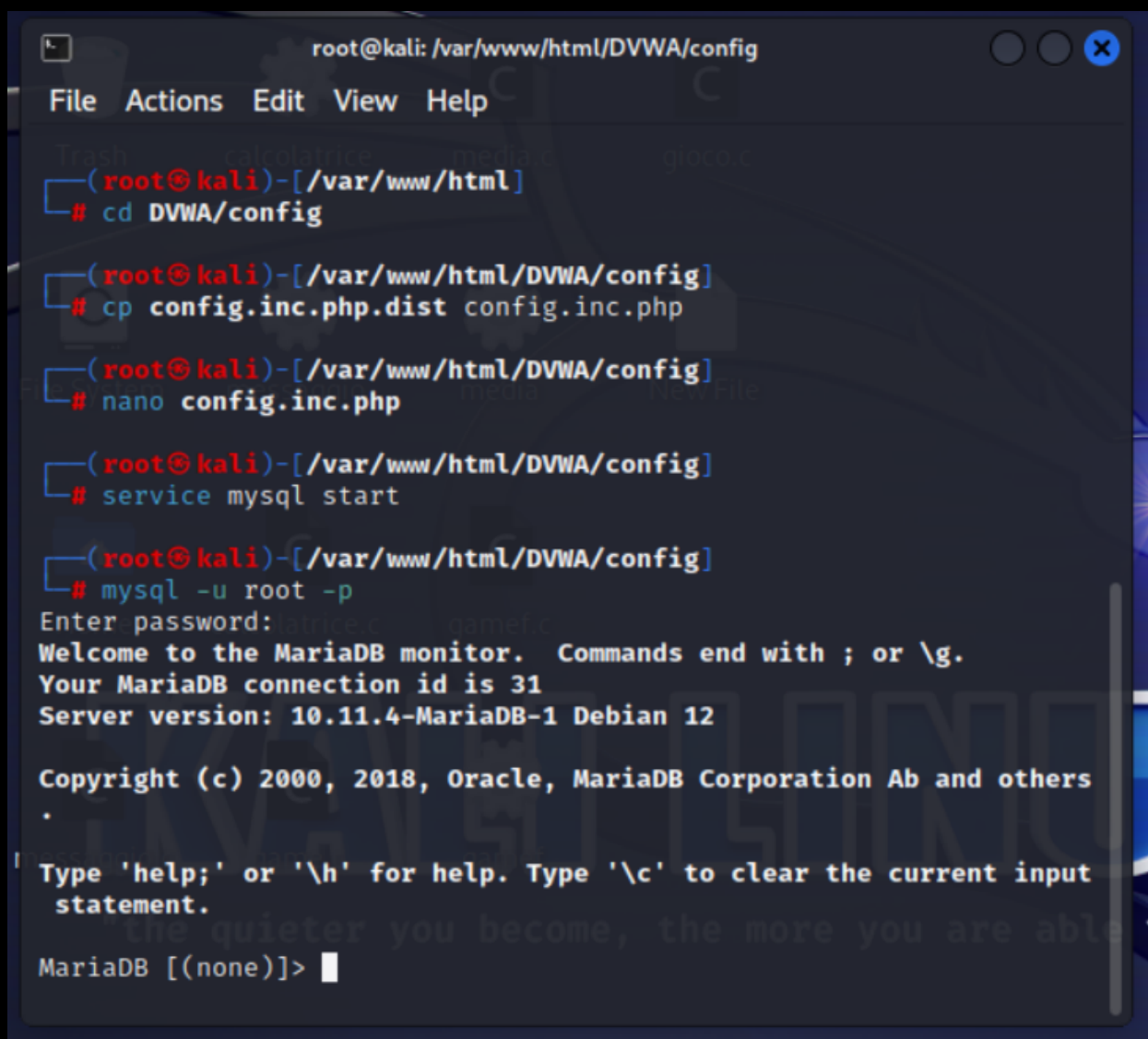
# If you are having problems connecting to the MySQL database and >
# try changing the 'db_server' variable from localhost to 127.0.0.1 >
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY >
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use >
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv( 'DB_SERVER' ) ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port' ] = '3306';

[ Read 56 lines (Converted from DOS format) ]
^G Help ^O Write Out ^W Where Is ^K Cut more ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

2°

A terminal window titled 'root@kali: /var/www/html/DVWA/config' with standard window controls. The terminal shows a series of commands being executed to configure DVWA. The commands are: 'cd DVWA/config', 'cp config.inc.php.dist config.inc.php', 'nano config.inc.php', and 'service mysql start'. After the last command, the terminal displays the MySQL/MariaDB command-line interface. It shows the prompt 'Enter password:', a welcome message, connection ID '31', server version '10.11.4-MariaDB-1 Debian 12', copyright information, and a help message. The prompt 'MariaDB [(none)]>' is shown at the bottom with a cursor.

```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
Trash calculatrice media.c gioco.c
(root@kali)-[/var/www/html]
# cd DVWA/config
(root@kali)-[/var/www/html/DVWA/config]
# cp config.inc.php.dist config.inc.php
(root@kali)-[/var/www/html/DVWA/config]
# nano config.inc.php
(root@kali)-[/var/www/html/DVWA/config]
# service mysql start
(root@kali)-[/var/www/html/DVWA/config]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.4-MariaDB-1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others
.
Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
MariaDB [(none)]>
```

3°

```
root@kali: /home/kali
File Actions Edit View Help
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
    '> Ctrl-C -- exit!
Aborted

(root@kali)-[/home/kali] media New File
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 46
Server version: 10.11.4-MariaDB-1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
Query OK, 0 rows affected (0.059 sec)

MariaDB [(none)]> exit
Bye

(root@kali)-[/home/kali] er you become, the more you are able to hear"
#
```

4°

```
root@kali: /etc/php/8.2/apache2
File Actions Edit View Help
chmod: changing permissions of 'php.ini': Operation not permitted

(kali@kali)-[/etc/php/8.2/apache2]
$ sudo su
[sudo] password for kali:
(root@kali)-[/etc/php/8.2/apache2]
# edit php.ini
Warning: unknown mime-type for "php.ini" -- using "application/octet-stream"
Error: no "edit" mailcap rules found for type "application/octet-stream"

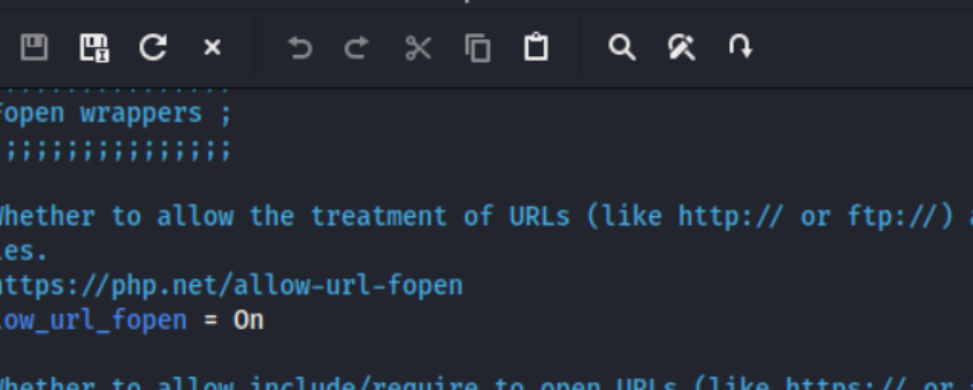
(root@kali)-[/etc/php/8.2/apache2]
# chmod +rwx php.ini

(root@kali)-[/etc/php/8.2/apache2]
# edit php.ini
Warning: unknown mime-type for "php.ini" -- using "application/octet-stream"
Error: no "edit" mailcap rules found for type "application/octet-stream"

(root@kali)-[/etc/php/8.2/apache2]
# open php.ini

(root@kali)-[/etc/php/8.2/apache2]
#
(mousepad:39547): dconf-WARNING **: 10:25:11.645: failed to commit changes to dconf: Fa
```

5°



```
861 ; Fopen wrappers ;
862 ;;;;;;;;;;;;;;;;;
863
864 ; Whether to allow the treatment of URLs (like http:// or ftp://) as
  files.
865 ; https://php.net/allow-url-fopen
866 allow_url_fopen = On
867
868 ; Whether to allow include/require to open URLs (like https:// or ftp://)
  as files.
869 ; https://php.net/allow-url-include
870 allow_url_include = On
871
872 ; Define the anonymous ftp password (your email address). PHP's default
  setting
873 ; for this is empty.
874 ; https://php.net/from
875 ;from="john@doe.com"
876
877 ; Define the User-Agent string. PHP's default setting for this is empty.
878 ; https://php.net/user-agent
879 ;user_agent="PHP"
880
```

6°

```

[Language: en-US, en-gb=0, 0]
[ (root@kali) - [/etc/php/8.2/apache2] possible
# service apache2 start

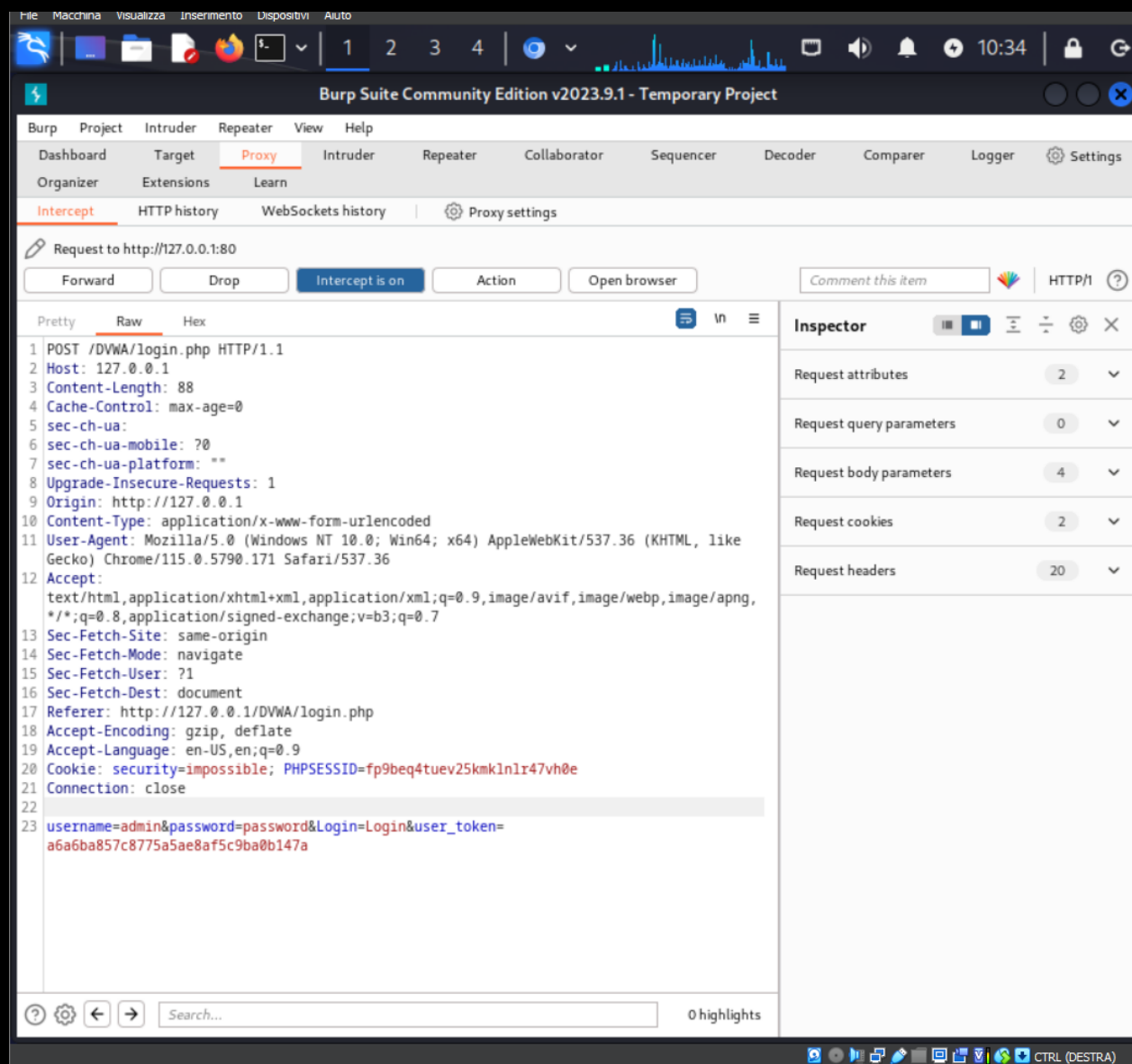
[ (root@kali) - [/etc/php/8.2/apache2] =6306edf30755b235125f27dc45c82b19
# █

```

Utilizzo tool Burpsuite

Cambio delle credenziali login corrette e verifica richiesta tramite repeater.

1°



2°

```
Cookie: PHPSESSID=fp9beq4tuev25kmln1r47vh0e; security=impossible
Connection: close

username=Giorgio&password=ciao1234&Login=Login&user_token=6306edf30755b235125f2fdc45c82b19
```

3°

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays the raw HTTP request for a login attempt. The 'Response' pane on the right shows the server's response, which includes a message indicating that the login failed. A red arrow points to the text 'Login failed' in the response.

Request:

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua:
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: ""
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 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
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=fp9beq4tuev25kmln1r47vh0e; security=impossible
19 Connection: close
20
21
```

Response:

```
50
51
52
53 <p class="submit">
54   <input type="submit" value="Login" name="Login">
55 </p>
56
57 </fieldset>
58
59 <input type="hidden" name="user_token" value="
60 d9435d01048ca5c83bcb55bde3545e62" />
61
62 </form>
63
64 <div class="message">
65   Login failed
66 </div>
67
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73 <br />
74 </div>
<!--<div id="content">-->
```

Richiesta di login fallita.

