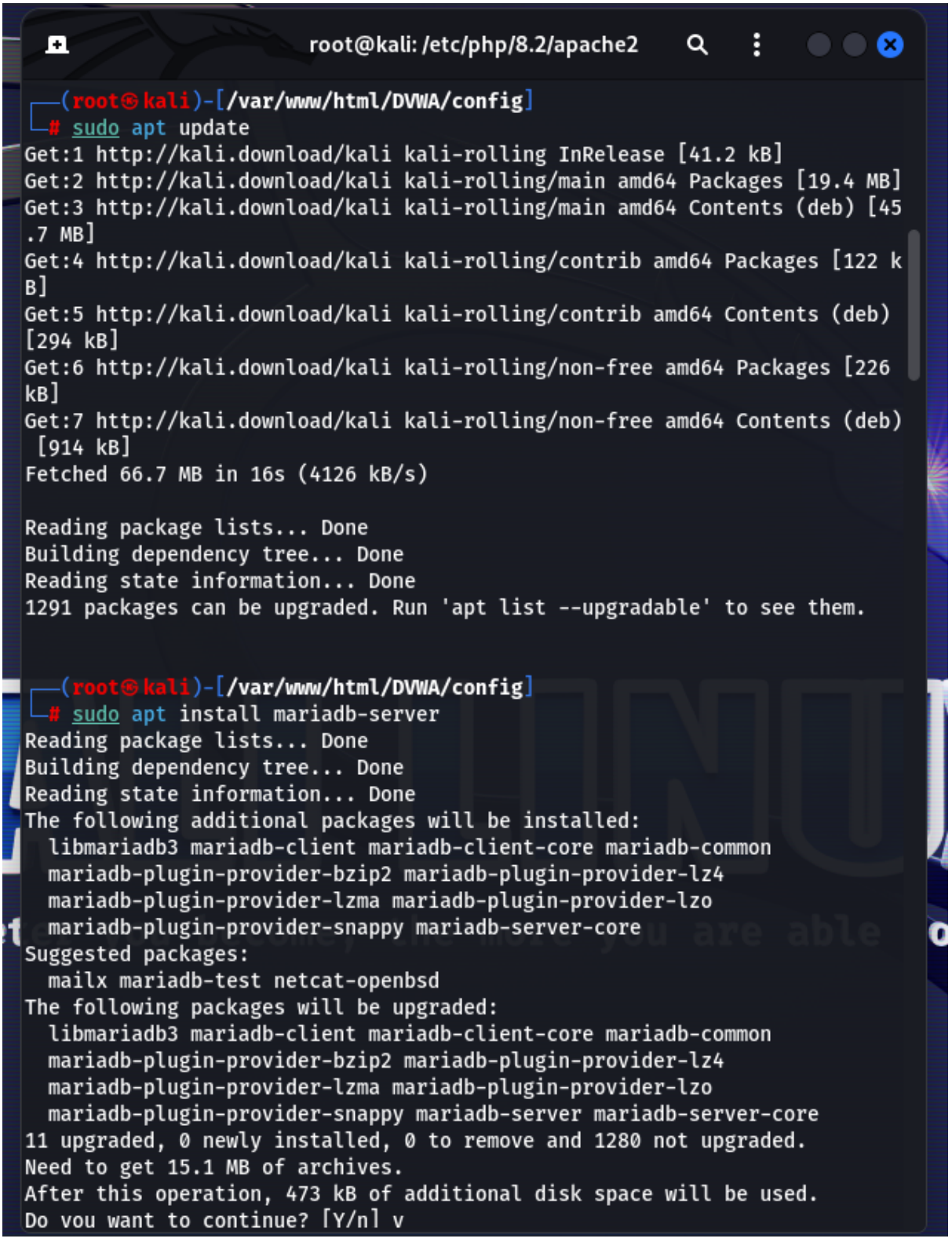
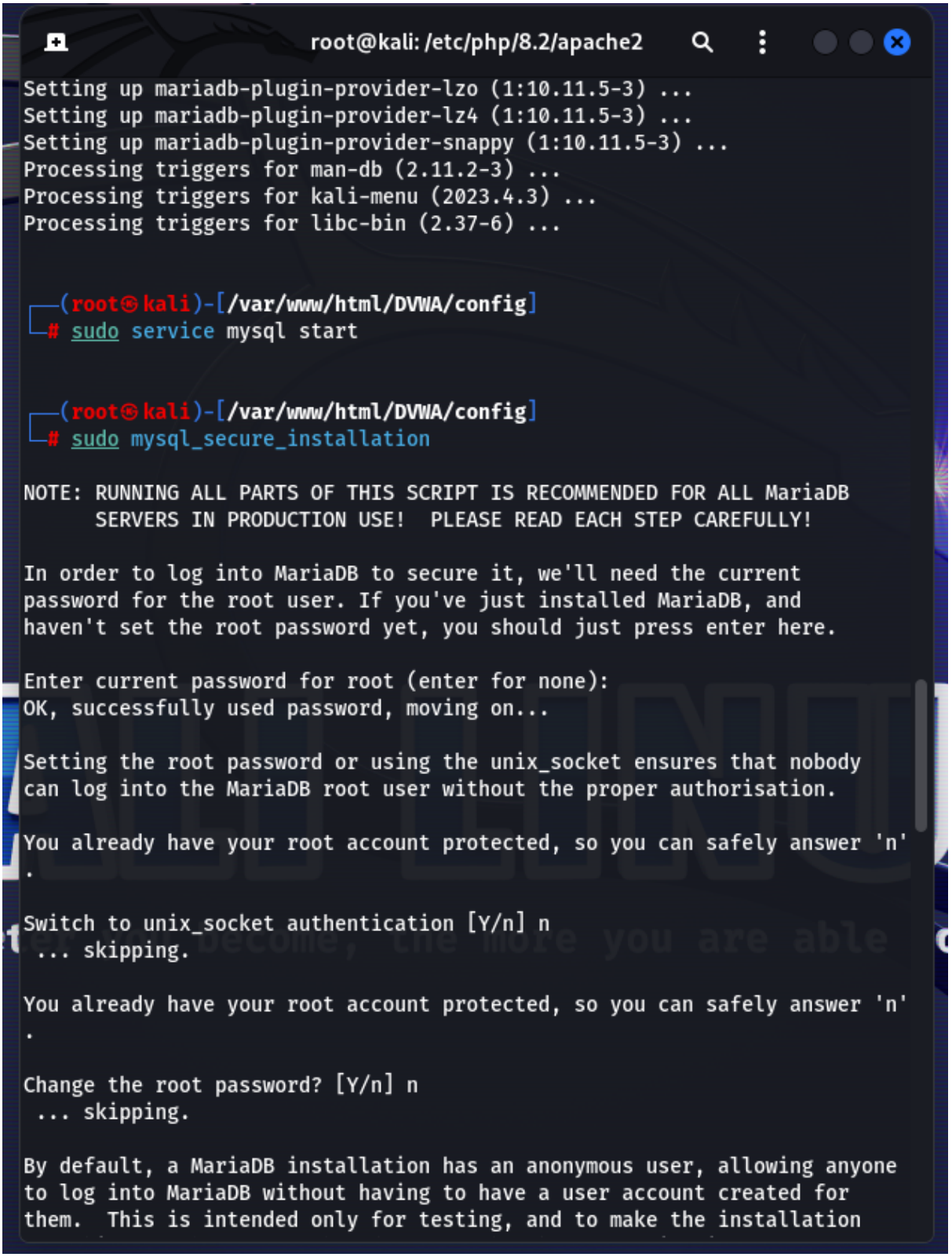
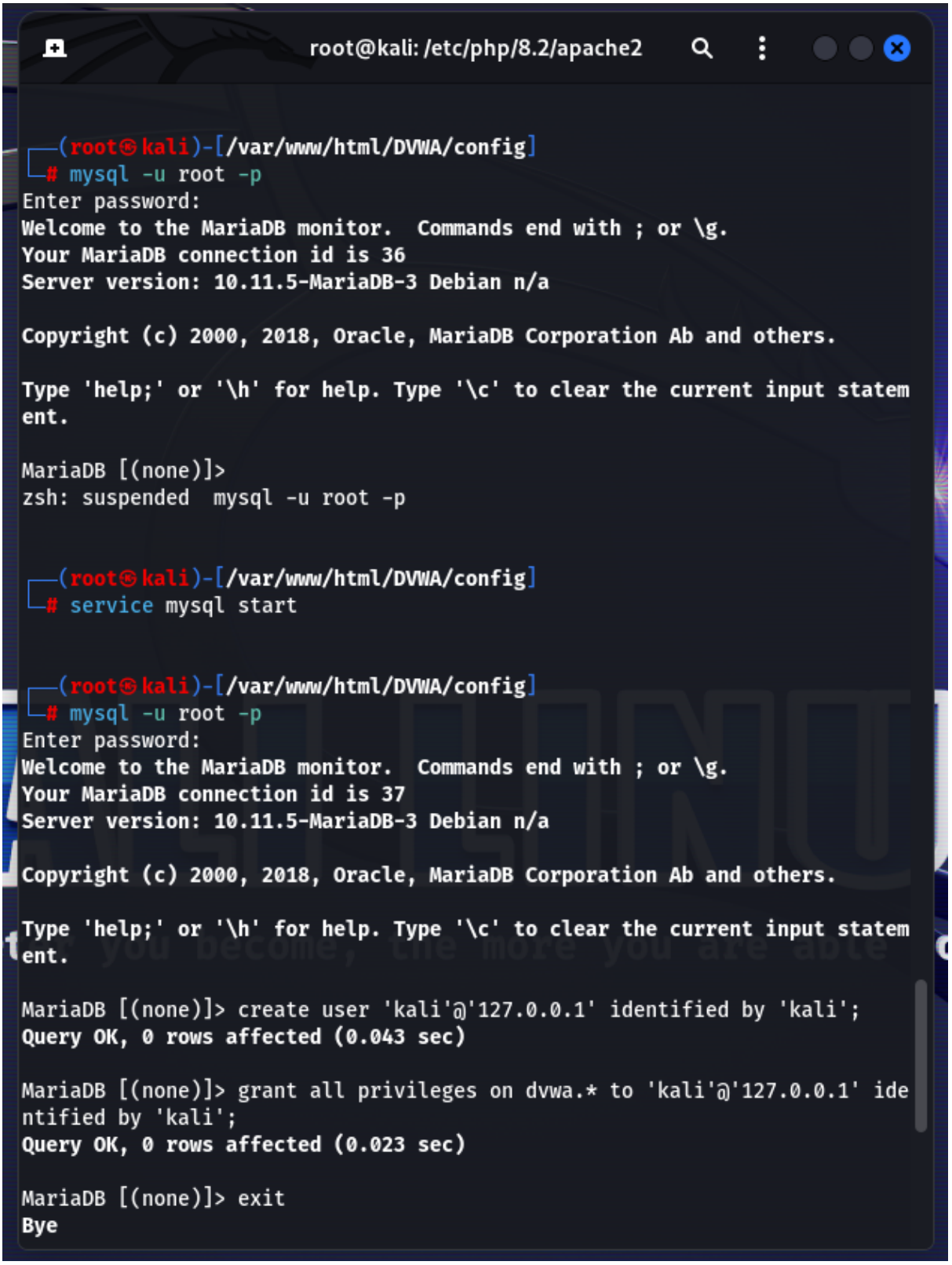
CONSEGNA S3L3

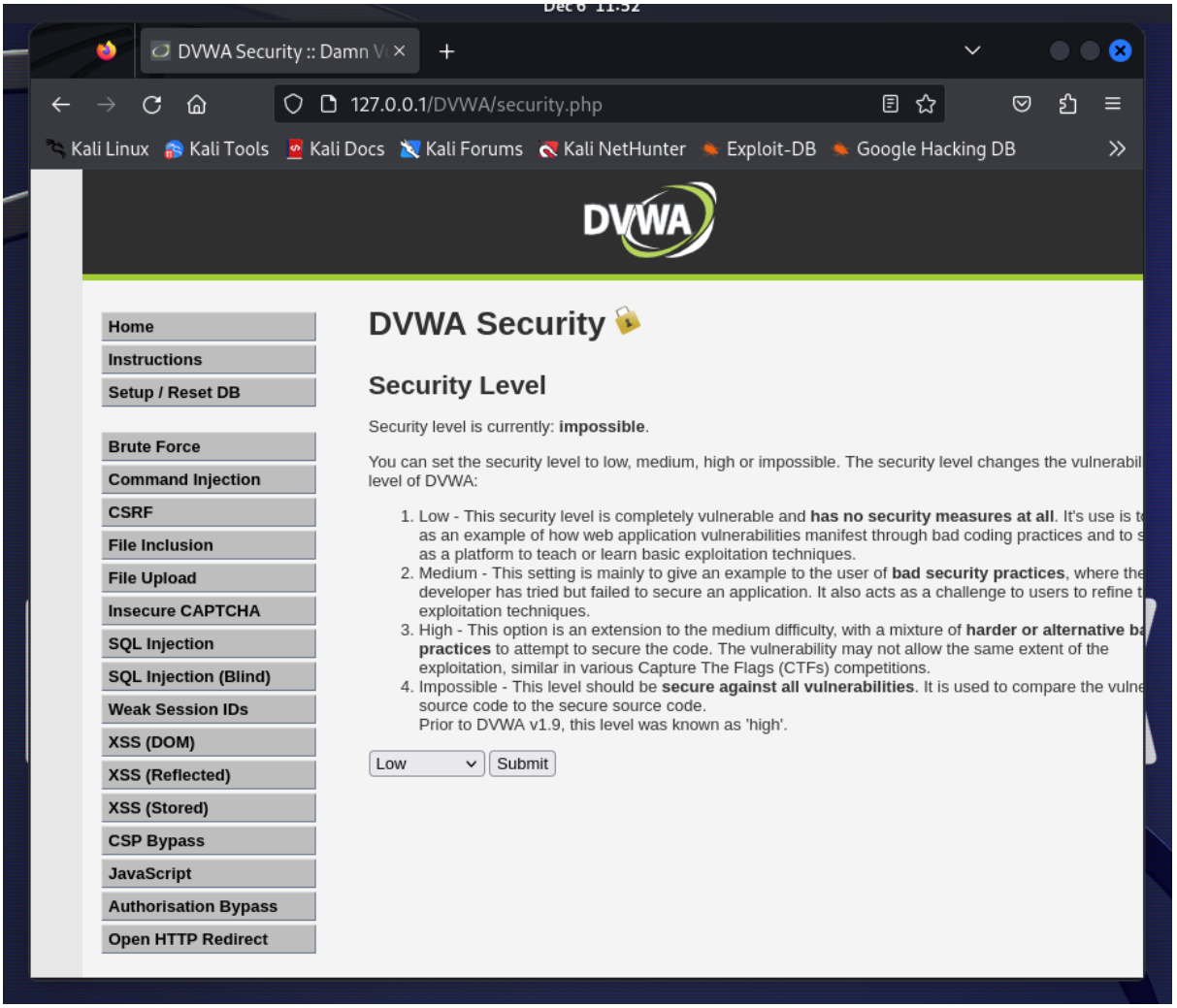
Seguire i passaggi delle slide, riportati negli screen sottostanti.
IMPORTANTE: Kali deve essere impostato con scheda bridge e deve riuscire a collegarsi su internet altrimenti non si può svolgere quanto segue!


root@kali: /etc/php/8.2/apache2
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45
.7 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [122 k
B]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb)
[294 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [226
kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb)
[914 kB]
Fetched 66.7 MB in 16s (4126 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1291 packages can be upgraded. Run 'apt list --upgradable' to see them.
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo apt install mariadb-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libmariadb3 mariadb-client mariadb-client-core mariadb-common
mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4
mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
mariadb-plugin-provider-snappy mariadb-server-core
Suggested packages:
mailx mariadb-test netcat-openbsd
The following packages will be upgraded:
libmariadb3 mariadb-client mariadb-client-core mariadb-common
mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4
mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
mariadb-plugin-provider-snappy mariadb-server mariadb-server-core
11 upgraded, 0 newly installed, 0 to remove and 1280 not upgraded.
Need to get 15.1 MB of archives.
After this operation, 473 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

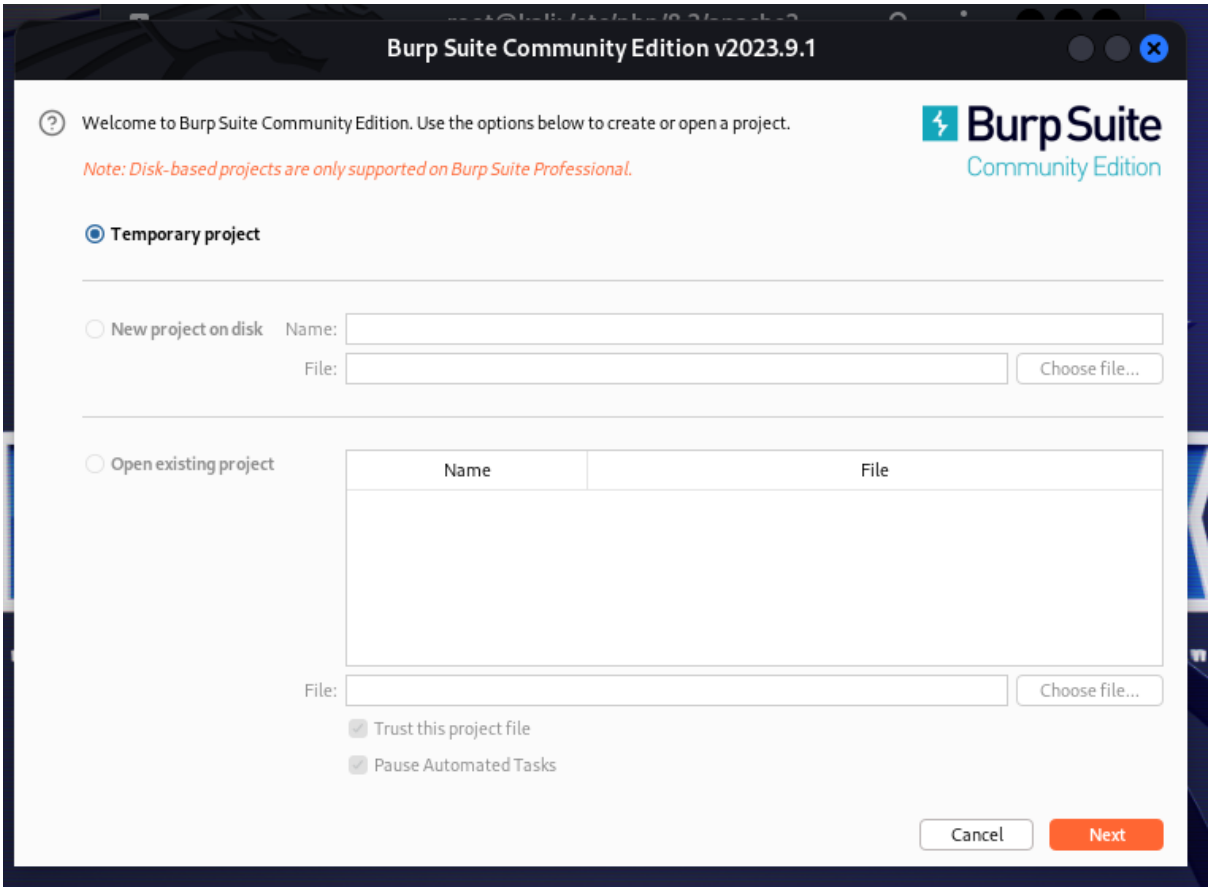

root@kali: /etc/php/8.2/apache2
Setting up mariadb-plugin-provider-lzo (1:10.11.5-3) ...
Setting up mariadb-plugin-provider-lz4 (1:10.11.5-3) ...
Setting up mariadb-plugin-provider-snappy (1:10.11.5-3) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for libc-bin (2.37-6) ...
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo service mysql start
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.
Enter current password for root (enter for none):
OK, successfully used password, moving on...
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.
You already have your root account protected, so you can safely answer 'n'
.
Switch to unix_socket authentication [Y/n] n
... skipping.
You already have your root account protected, so you can safely answer 'n'
.
Change the root password? [Y/n] n
... skipping.
By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation


root@kali: /etc/php/8.2/apache2
┌──(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 36
Server version: 10.11.5-MariaDB-3 Debian n/a
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statem
ent.
MariaDB [(none)]>
zsh: suspended mysql -u root -p
┌──(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 37
Server version: 10.11.5-MariaDB-3 Debian n/a
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statem
ent.
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.043 sec)
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' ide
ntified by 'kali';
Query OK, 0 rows affected (0.023 sec)
MariaDB [(none)]> exit
Bye

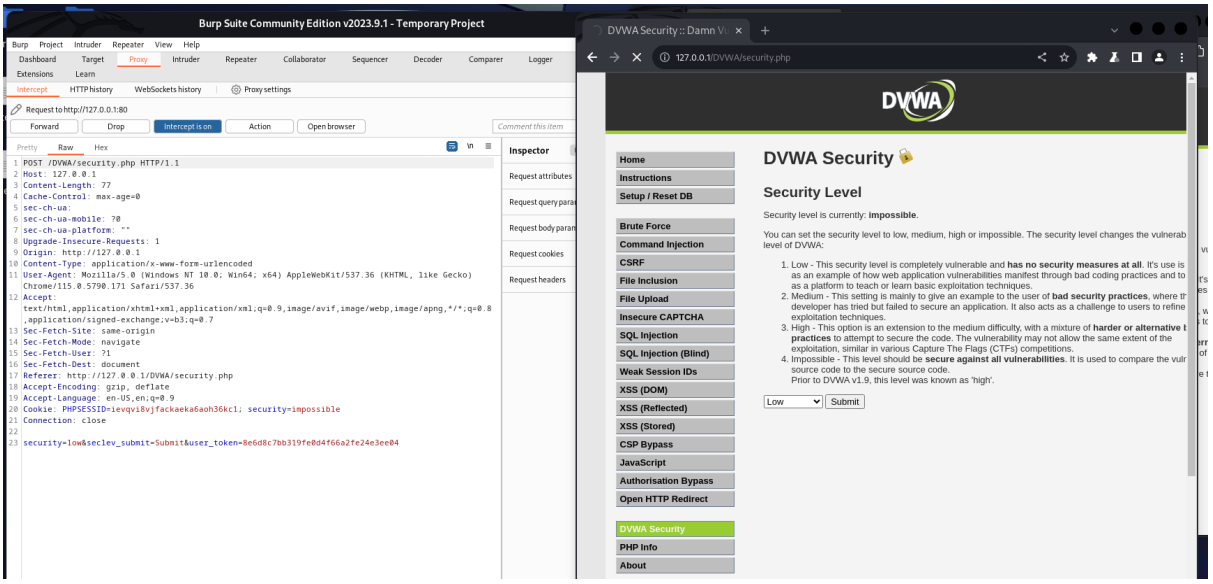

(root㉿kali)-[/var/www/html/DVWA/config]
service apache2 start
(root㉿kali)-[/var/www/html/DVWA/config]
cd /etc/php
(root㉿kali)-[/etc/php]
ls
8.2
(root㉿kali)-[/etc/php]
cd /etc/php/8.2/apache2
(root㉿kali)-[/etc/php/8.2/apache2]
nano php.ini
(root㉿kali)-[/etc/php/8.2/apache2]
service apache2 start
(root㉿kali)-[/etc/php/8.2/apache2]
#



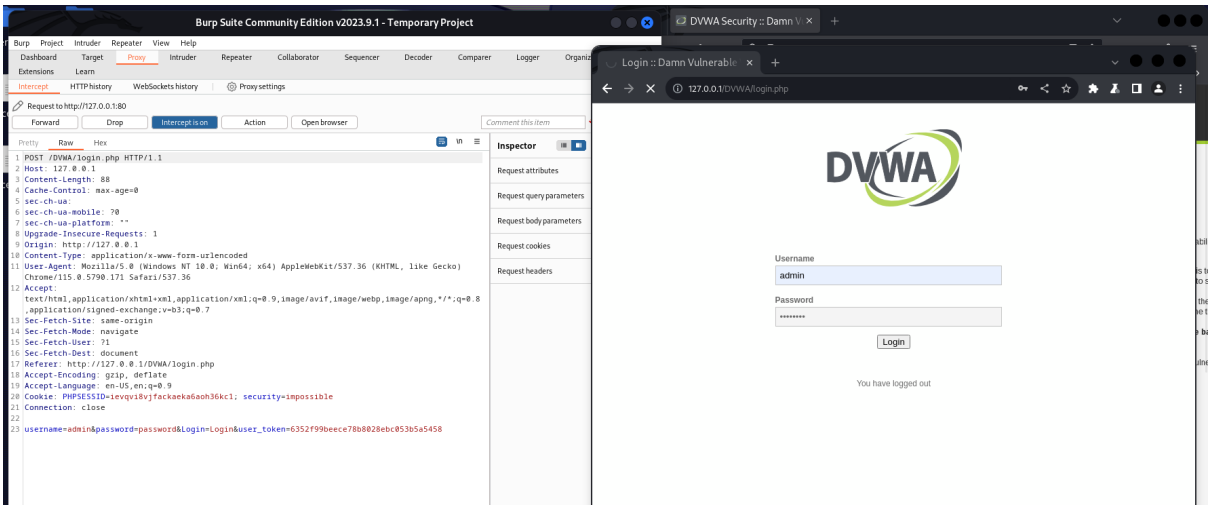
Apertura di **DVWA** (127.0.0.1/DVWA) e conseguente login (con “admin” e “password”) per modificare il livello di sicurezza, in questo caso **low**.



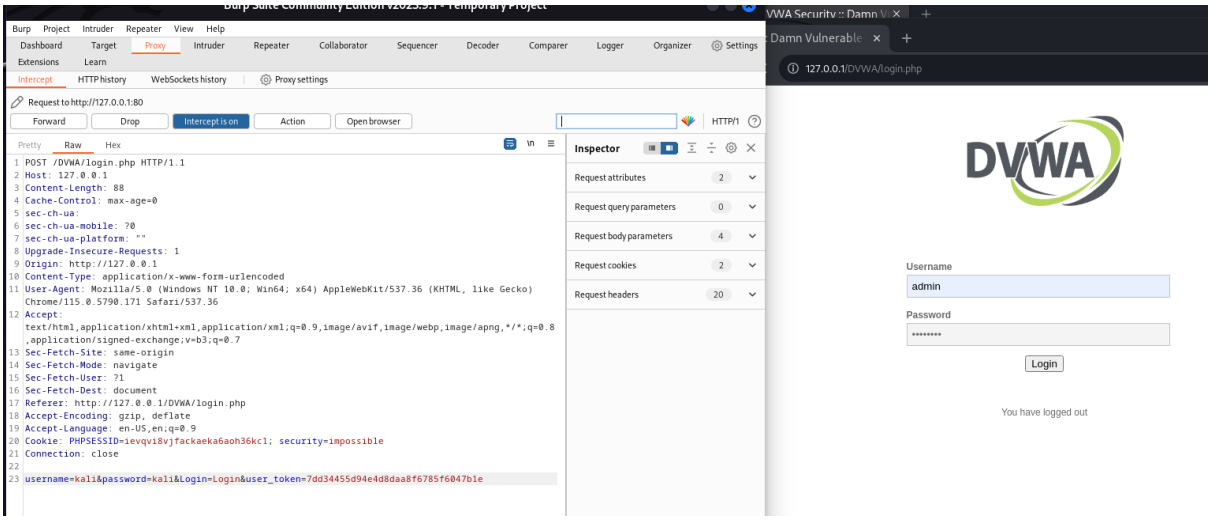
Apertura del software **Burp Suite** -preinstallato su Kali- e creazione di un **temporary project**.



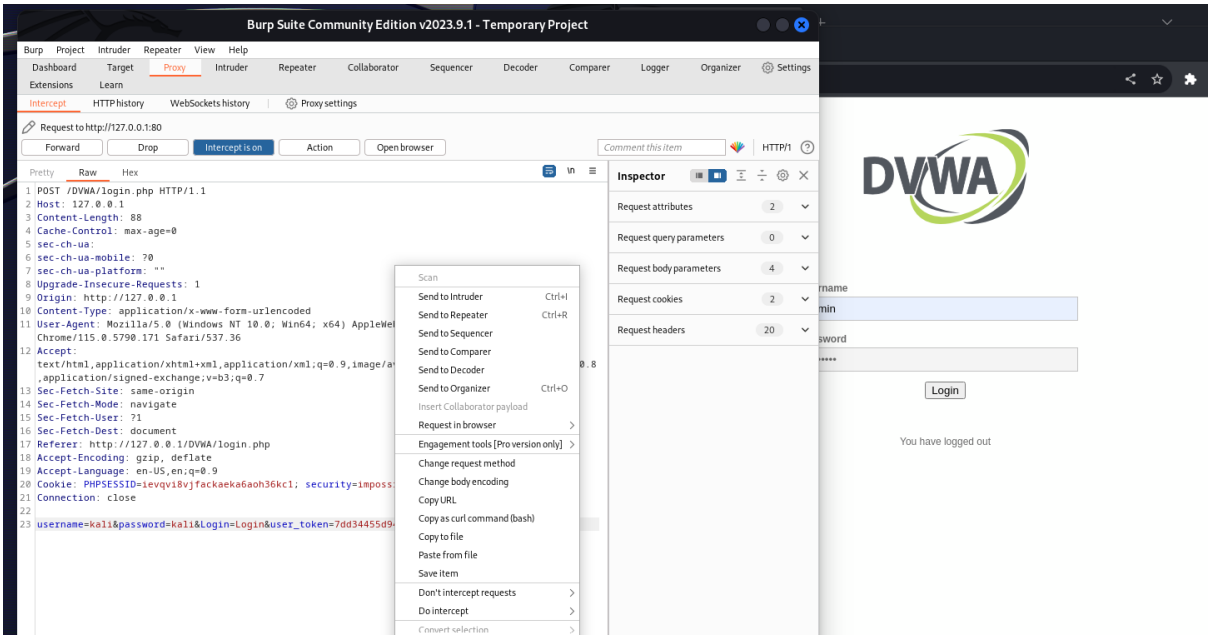
Si inizia a catturare il traffico di rete di DVWA Security, prima avviando la cattura cliccando su “**intercept is off**” e impostandolo su **on** e poi aprendolo sul browser, cliccando “**Open in browser**”.
A questo punto il software ci mostrerà diverse informazioni.
Per mandare avanti la connessione si deve premere in alto su **Forward**: questo passaggio va fatto ogni volta per ricevere o mandare una richiesta del sito.



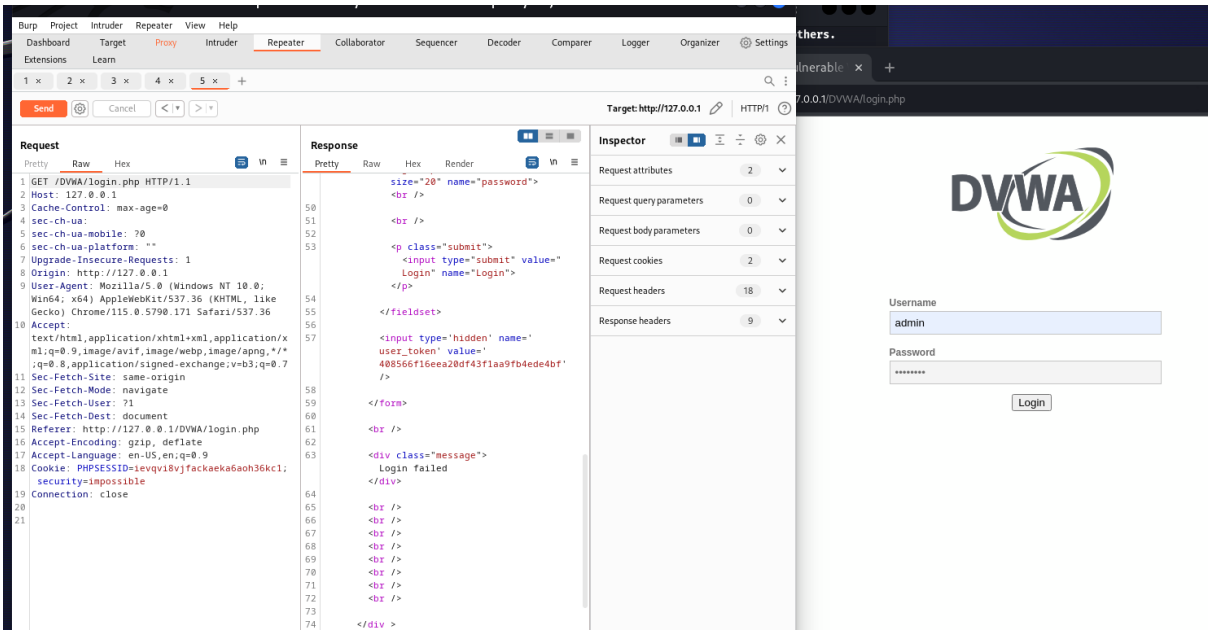
Qua abbiamo la cattura di quando andiamo a fare il **login** sul browser con *username* e *password*: il programma ci mostrerà a schermo quanto inserito nell'ultima riga in basso nei campi "username" e "password", in questo caso rispettivamente **admin** e **password**.



Modifichiamo a piacimento l'**username** e la **password** negli appositi campi dell'ultima riga. Io ho messo "kali" e "kali".



Facciamo tasto destro e poi clicchiamo su “**Send to repeater**”, poi dobbiamo andare in alto ed entrare nella sezione **Repeater**, due spazi dopo “Proxy”.
Questa sezione permetterà di inoltrare la richiesta al sito con le informazioni che abbiamo modificato precedentemente.



Da questa schermata clicchiamo sul pulsante arancione “**Send**” e poi su “**Follow Redirection**”.
Ora dobbiamo scorrere nel body dell’http responsive del sito che si è caricato e possiamo leggere, nella classe “*message*”, un bel **login failed**.
Ovviamente non ci si aspettava diversamente, visto che abbiamo inserito username e password diversi da quelli corretti per il login.