Computer Security Project Report

Done by

Roy Gebrayel 202111125
, Abbas Hamyeh 202111049

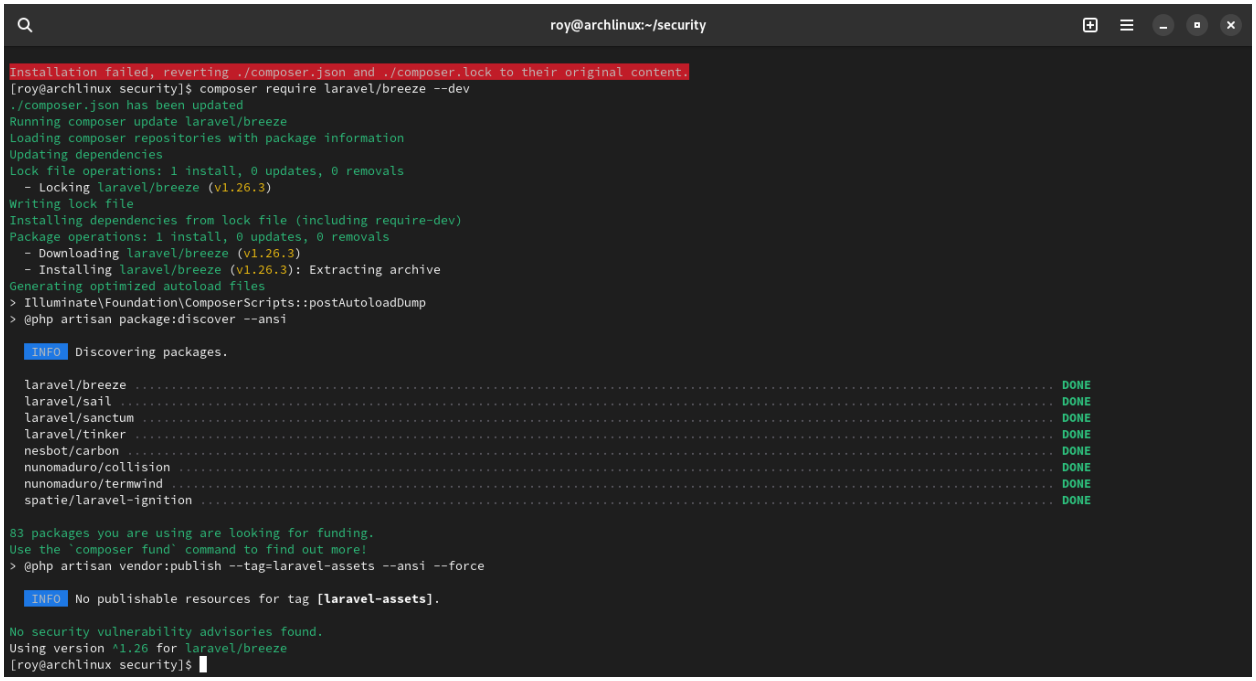
Overview :

- This is a project made in laravel in goal of learning the security and backend implementations and features aimed in this course

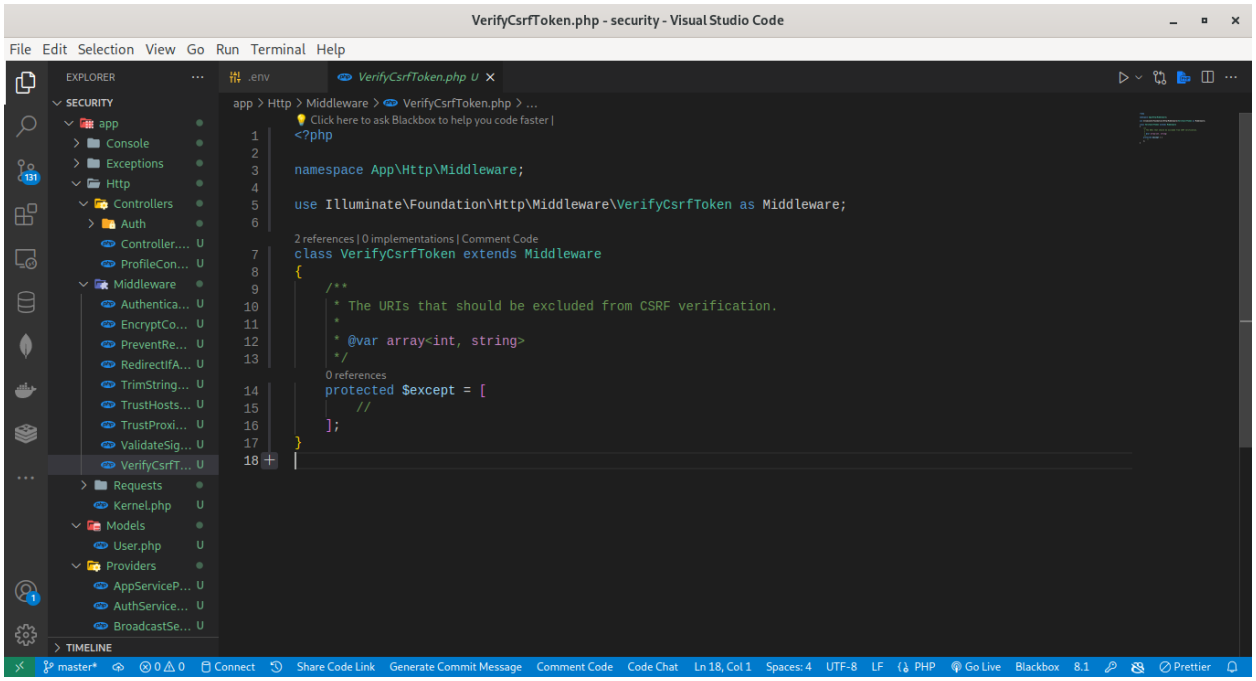
- We tried to work on laravel 10 having to deal with most of the security implementations and flows in the web app

- This is a hospital management system where patients , doctors , users and admins are found

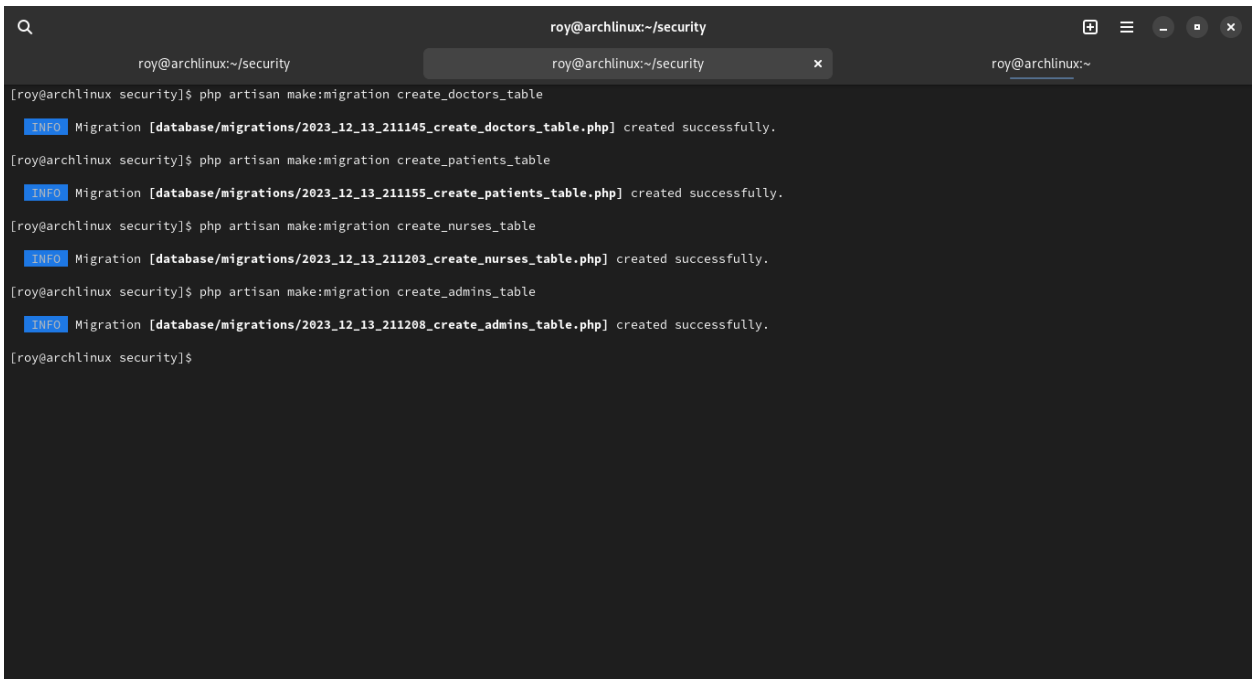
1. User Authentication :



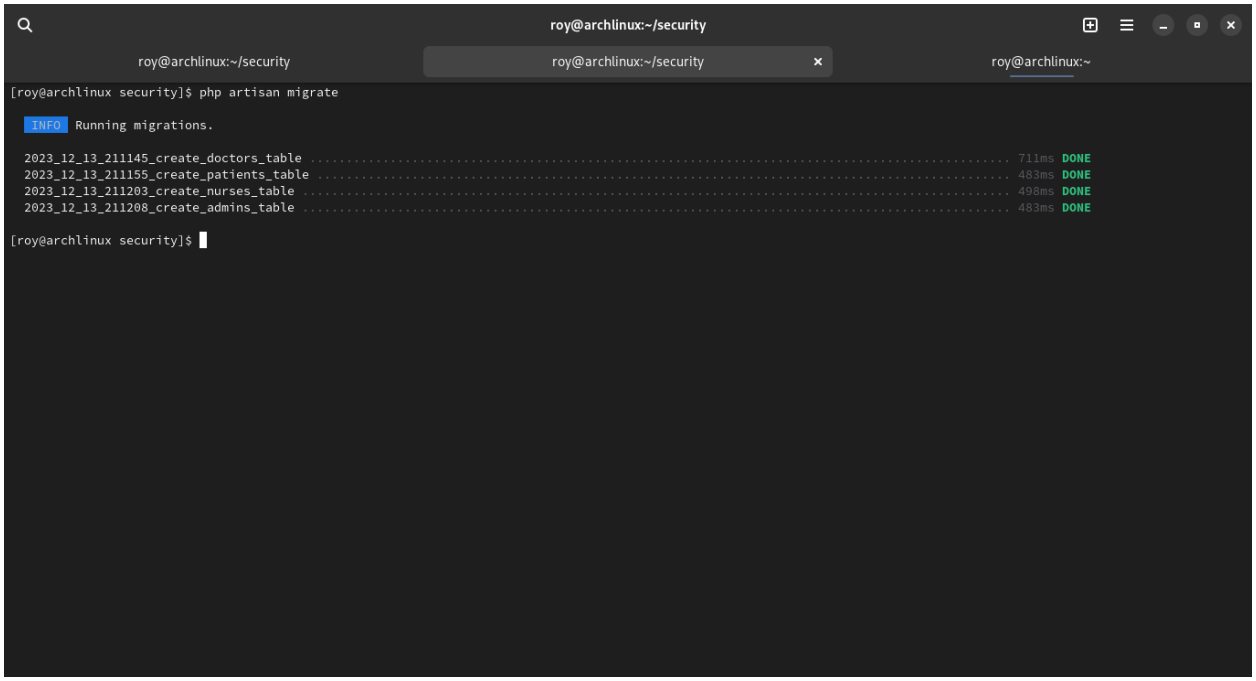
Installing laravel breeze to help us in the authentication flow



This is the folder where our auth folder is located

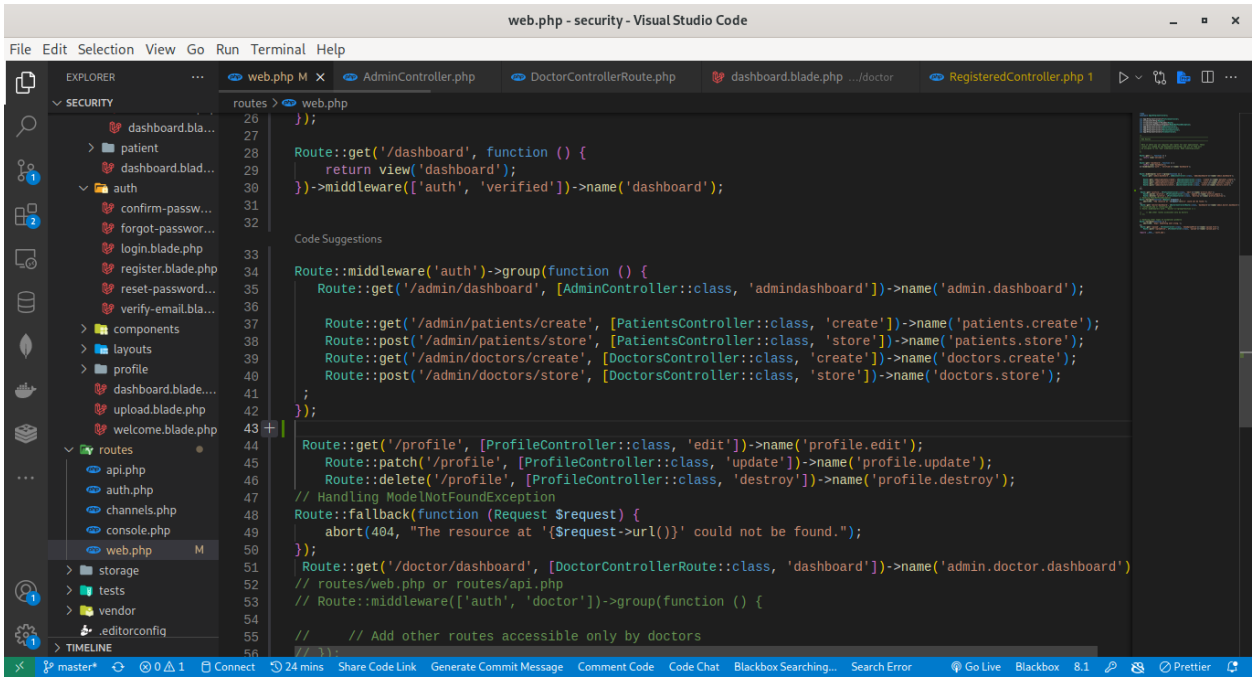


Creating the databases :

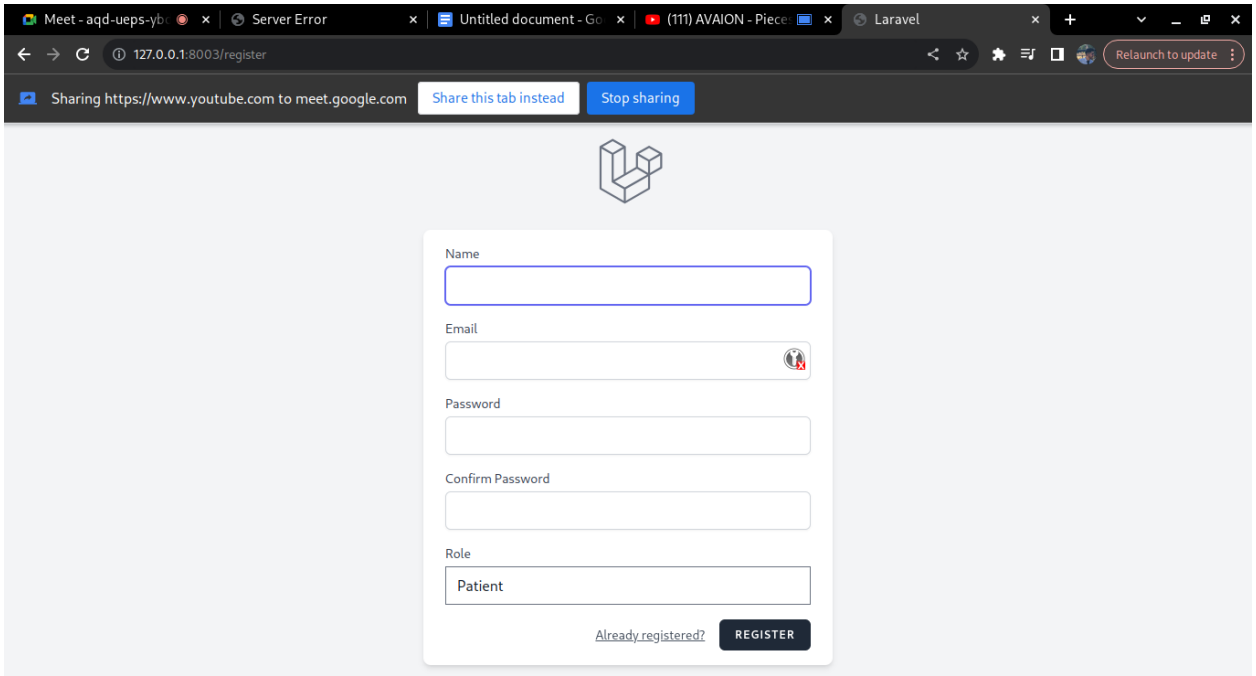


Deploying them into the hosted BaaS postgres database with php artisan migrate

Those are the created databases in elephantSQL

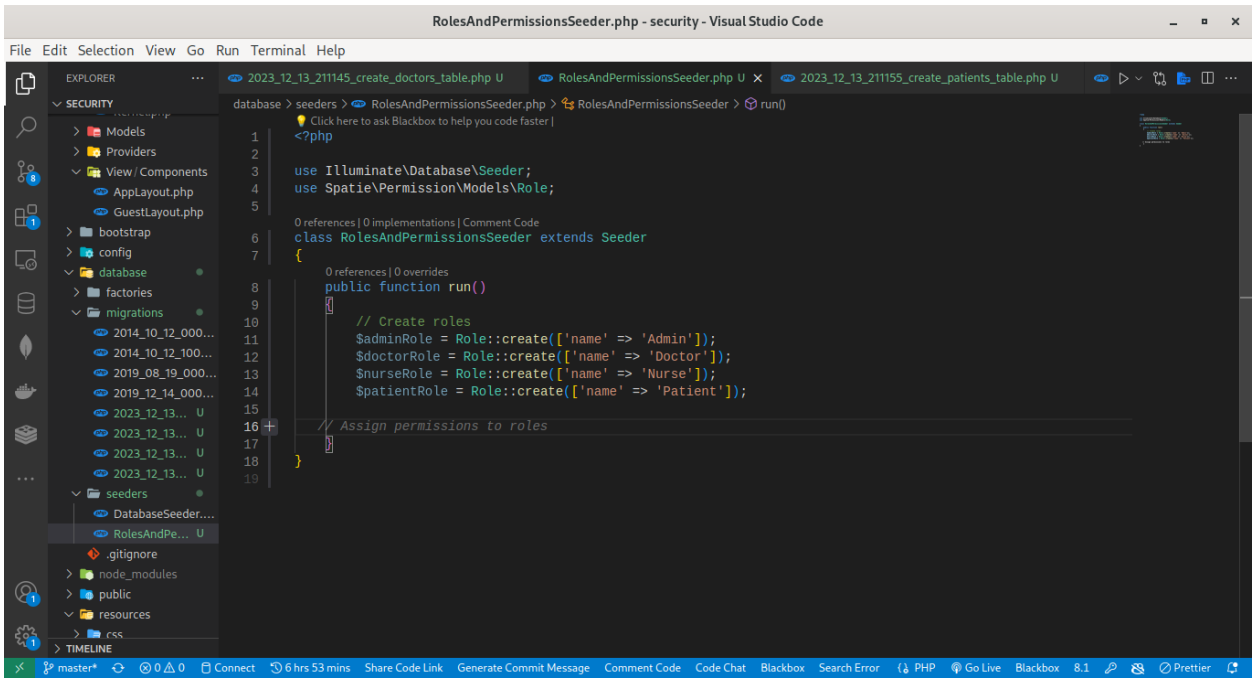


This is our web.php route file and this is where we inserted that all the written endpoints would need authentication in order to access it

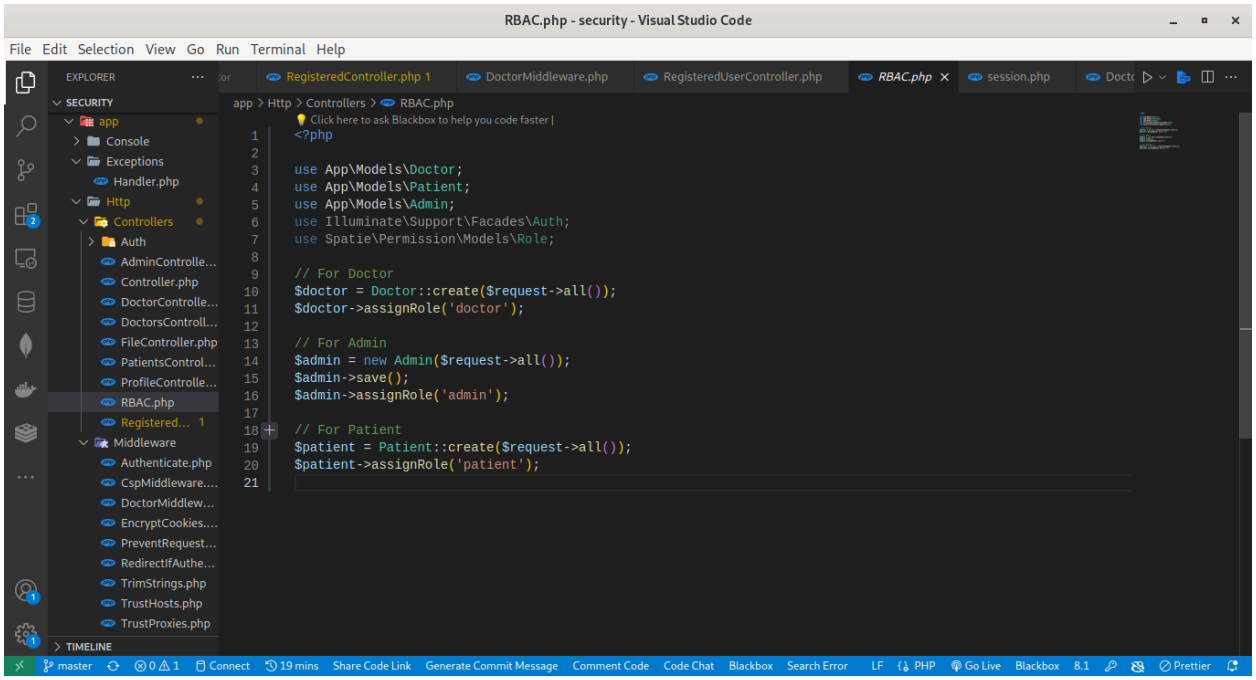


THIS IS the registration page where all authentication and validation are done on it and when the user clicks on register all data are sent to the database “users”

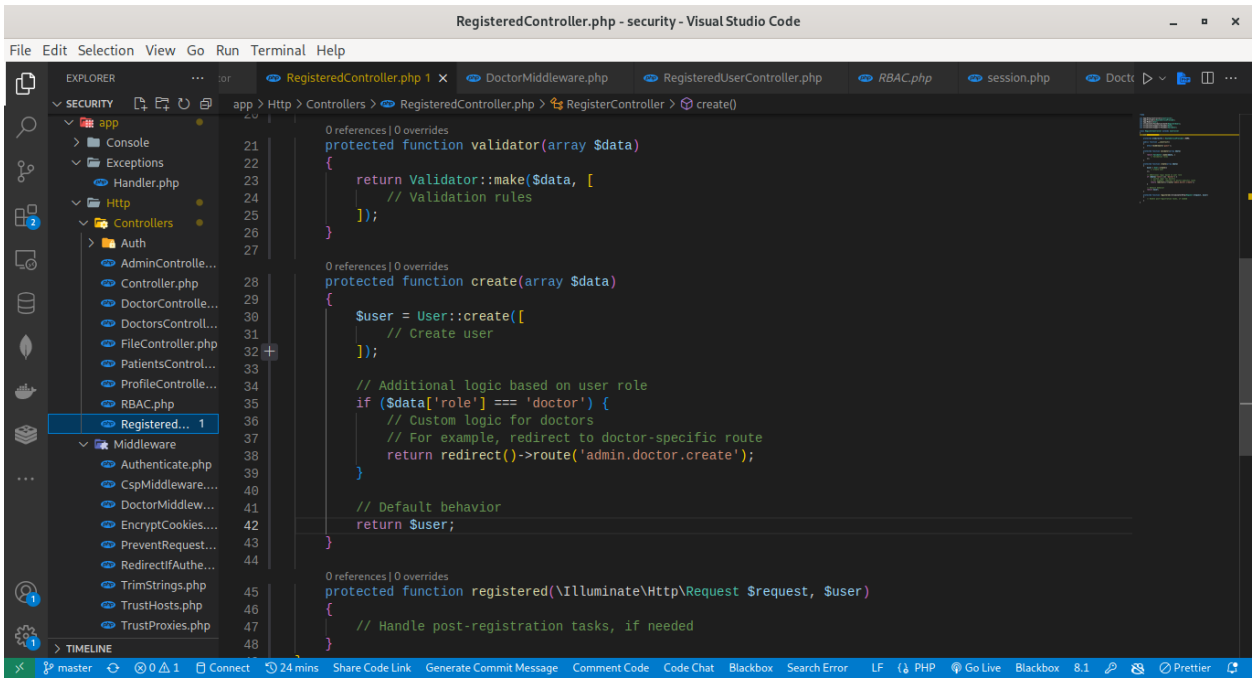
2 - ACCESS CONTROL



Create a database seed to defines roles

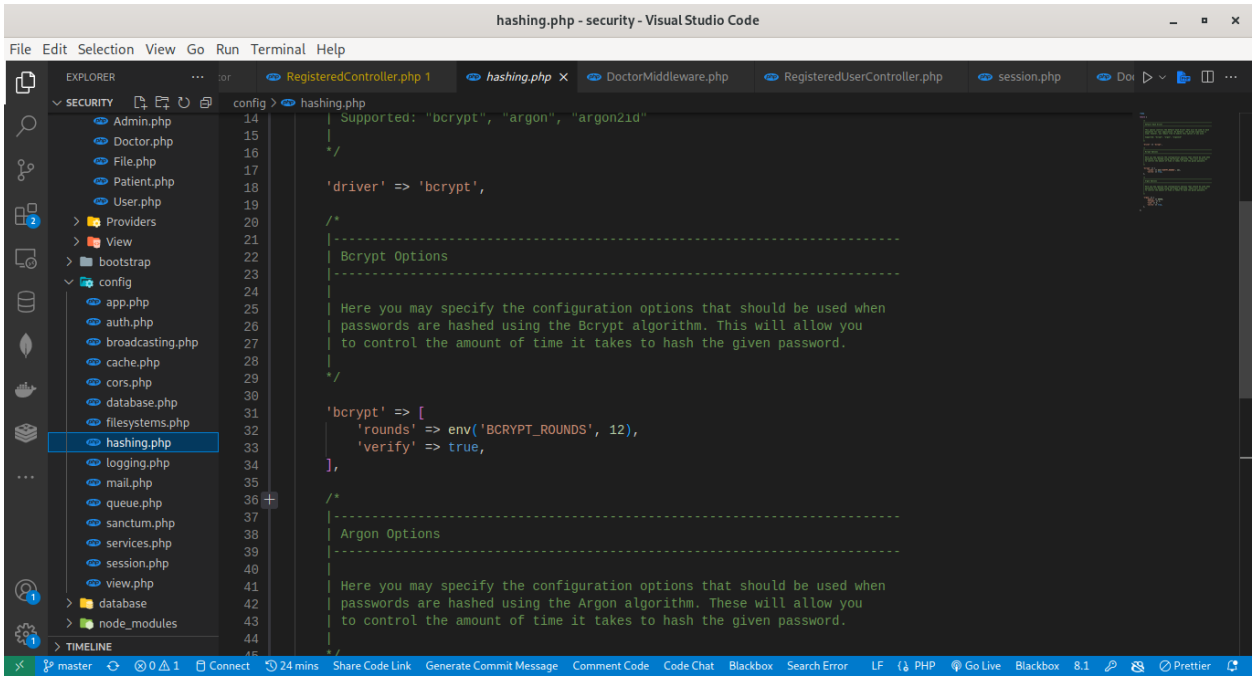


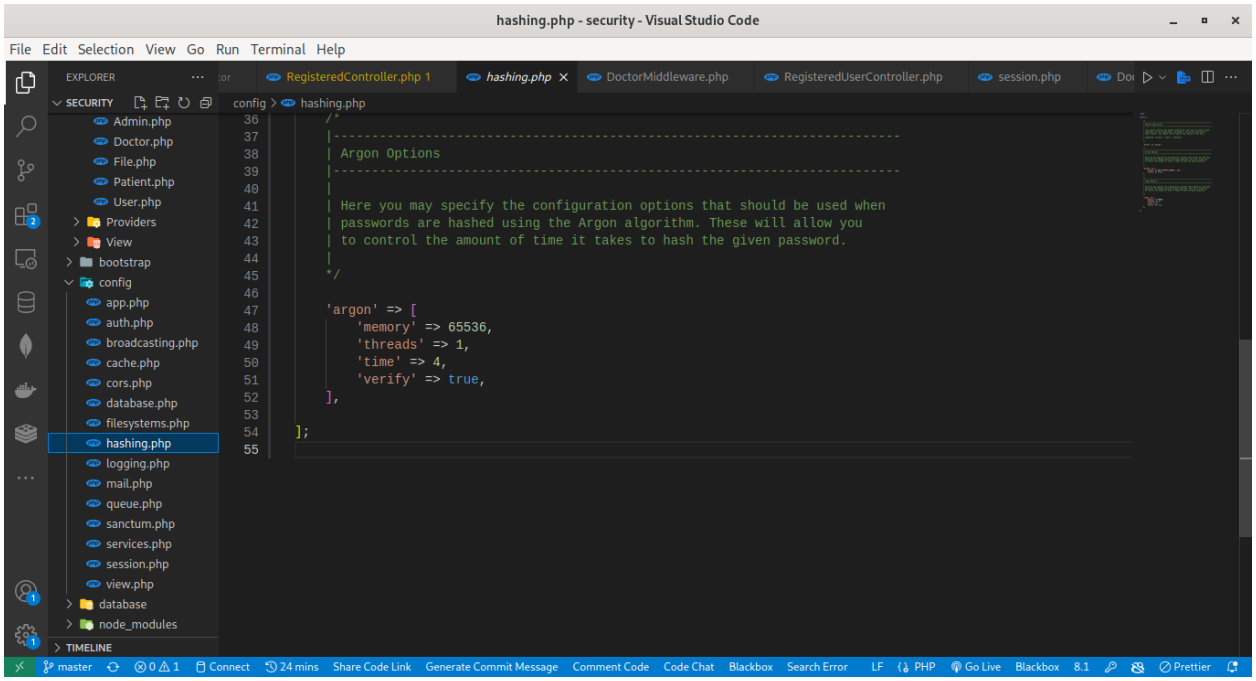
This files assigns roles for each user



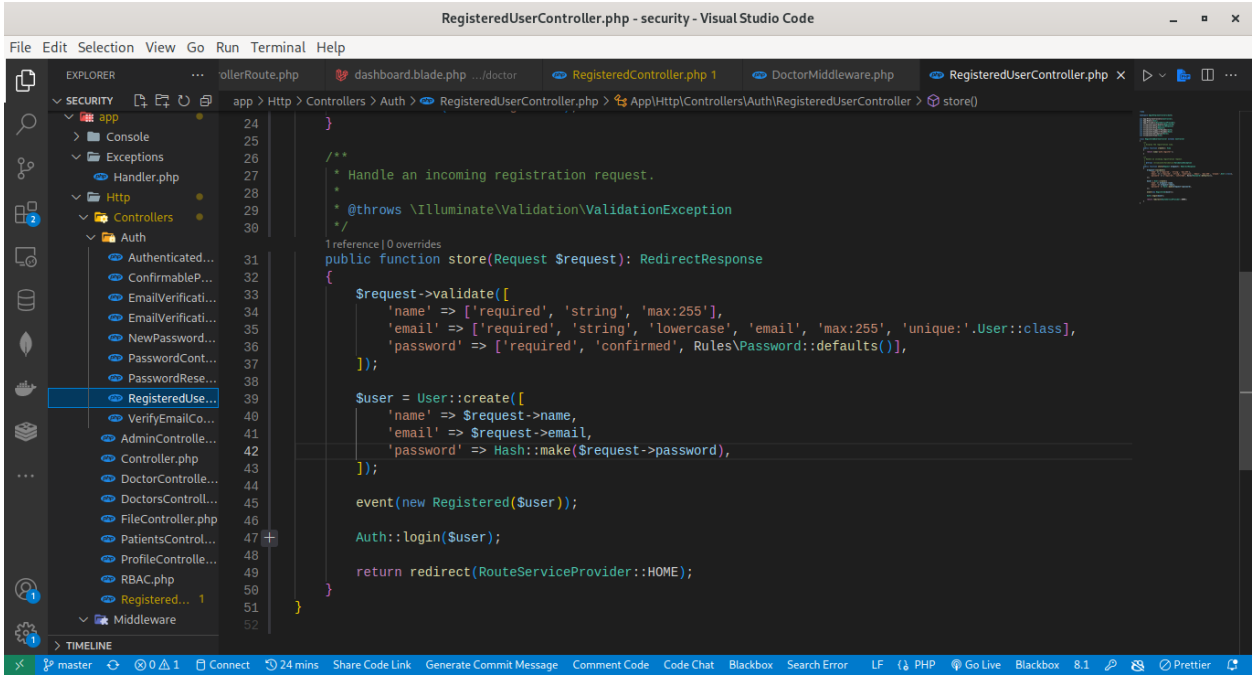
This file secures the route for a page if the user is a doctor (role = doctor)

3 - Data Encryption:



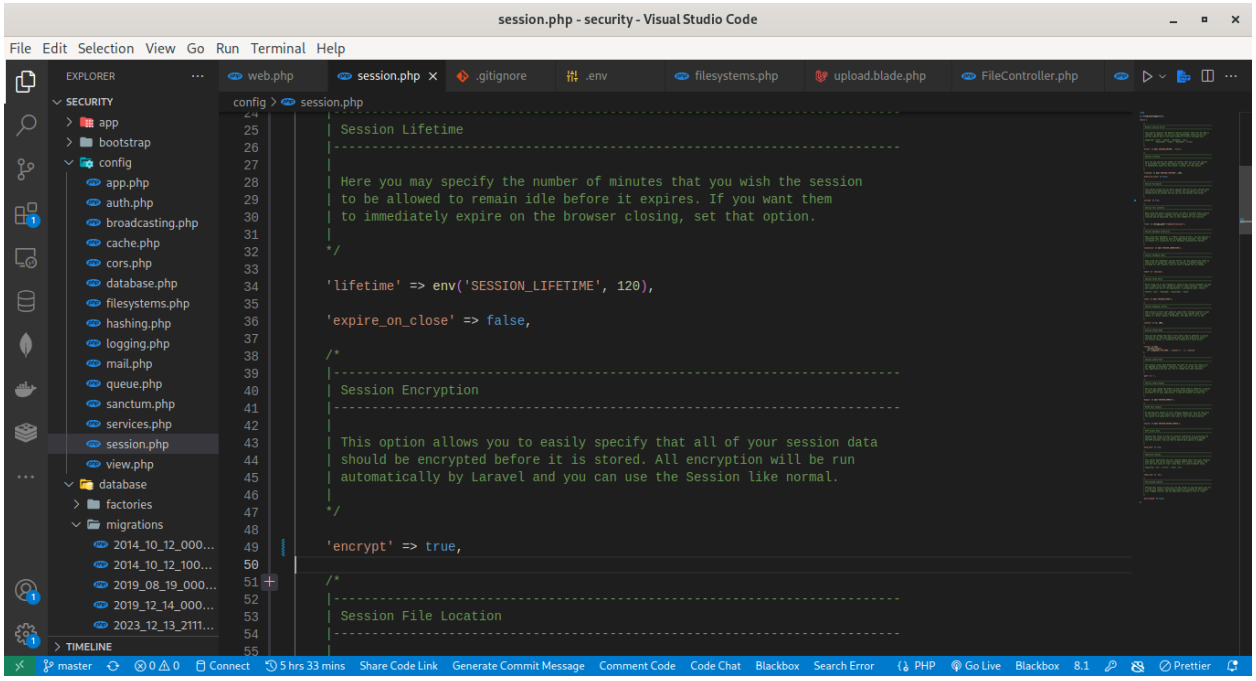


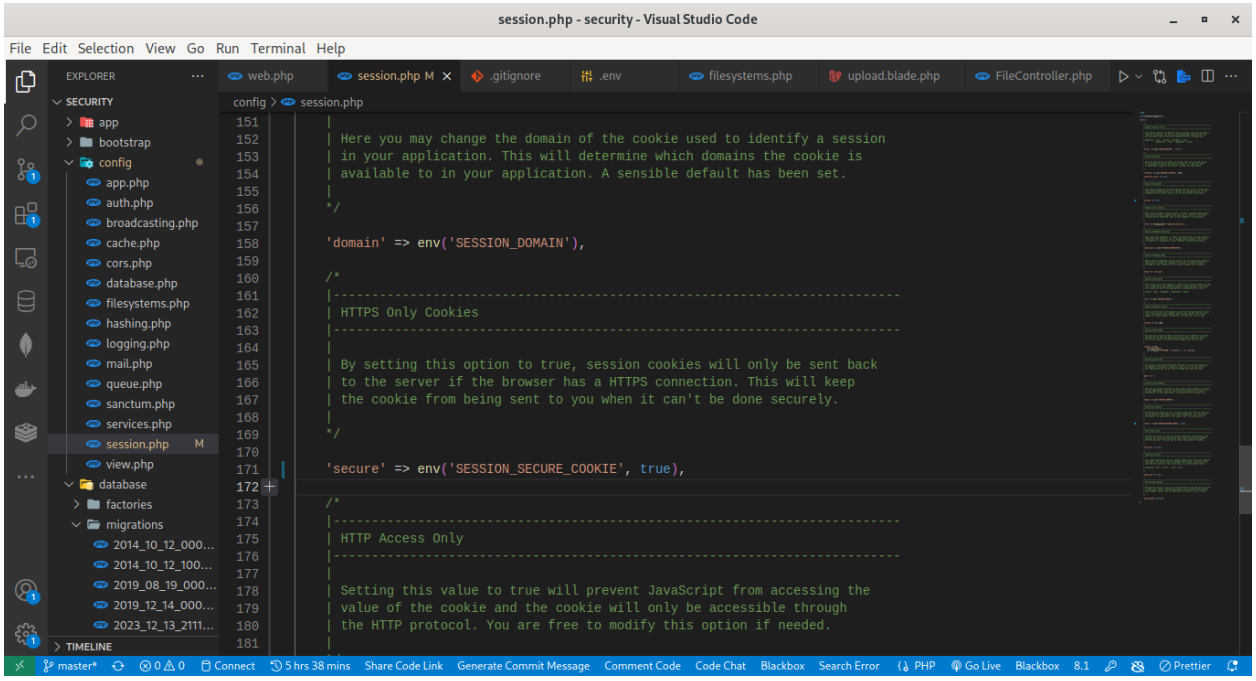
In the config file in the hash file , we found two drivers .. argon and bcrypt (both of these are hashing algorithms to hash passwords)



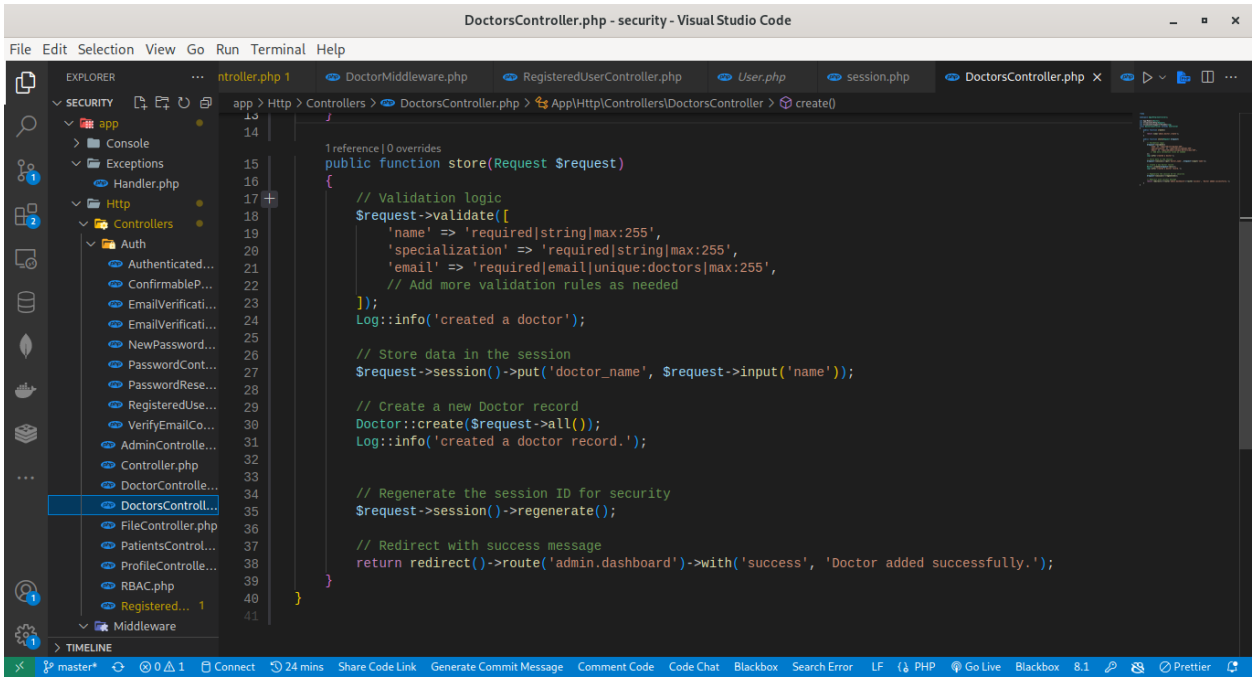
This is how we hashed the password in the user registration controller

4 - Session Management:





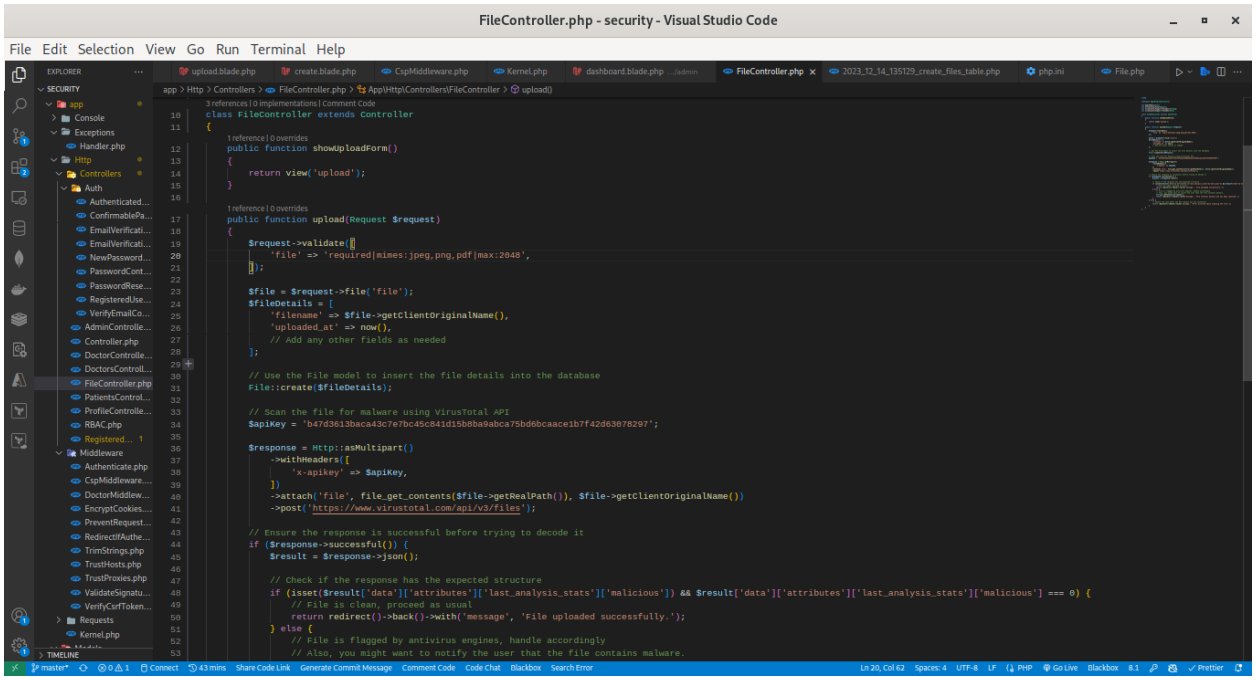
Here is the session config file where we handle all session timeout and session configurations and session token security



Here in the doctor controller i am storing my data in a session and then i am regenerating the session id for security purposes (this is one of the main use cases of sessions)

6. File Upload Security:

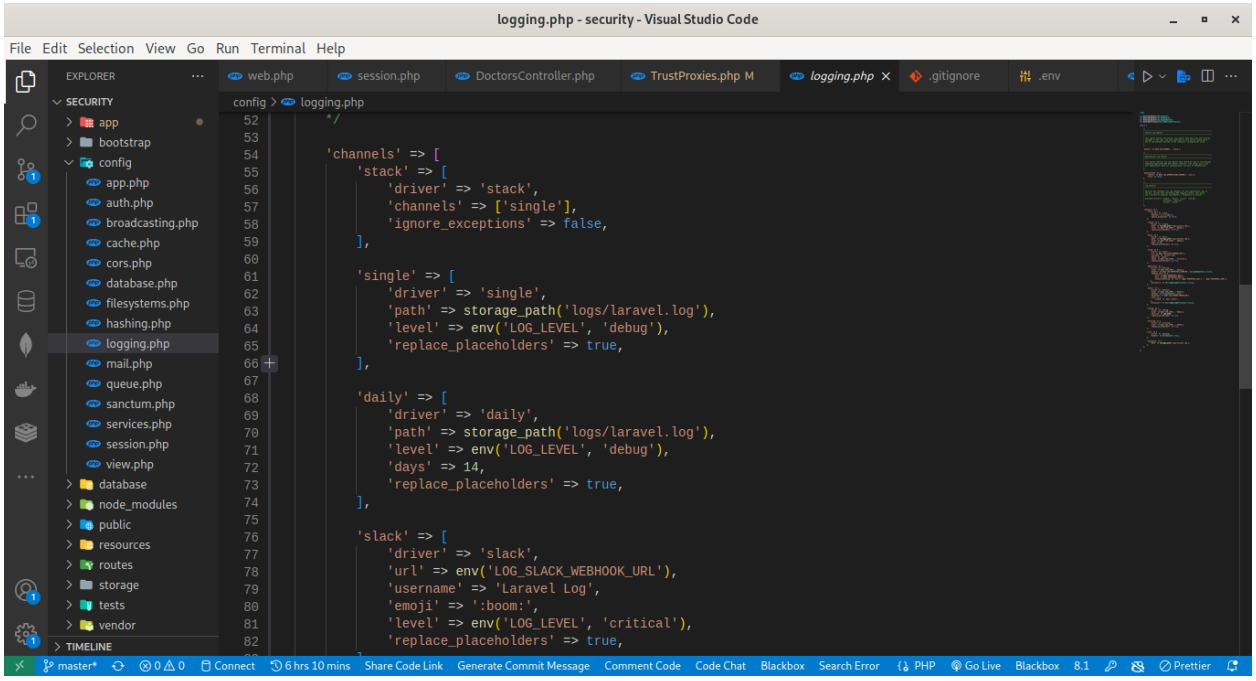
This is the upload page where you can add files into the pgsql db



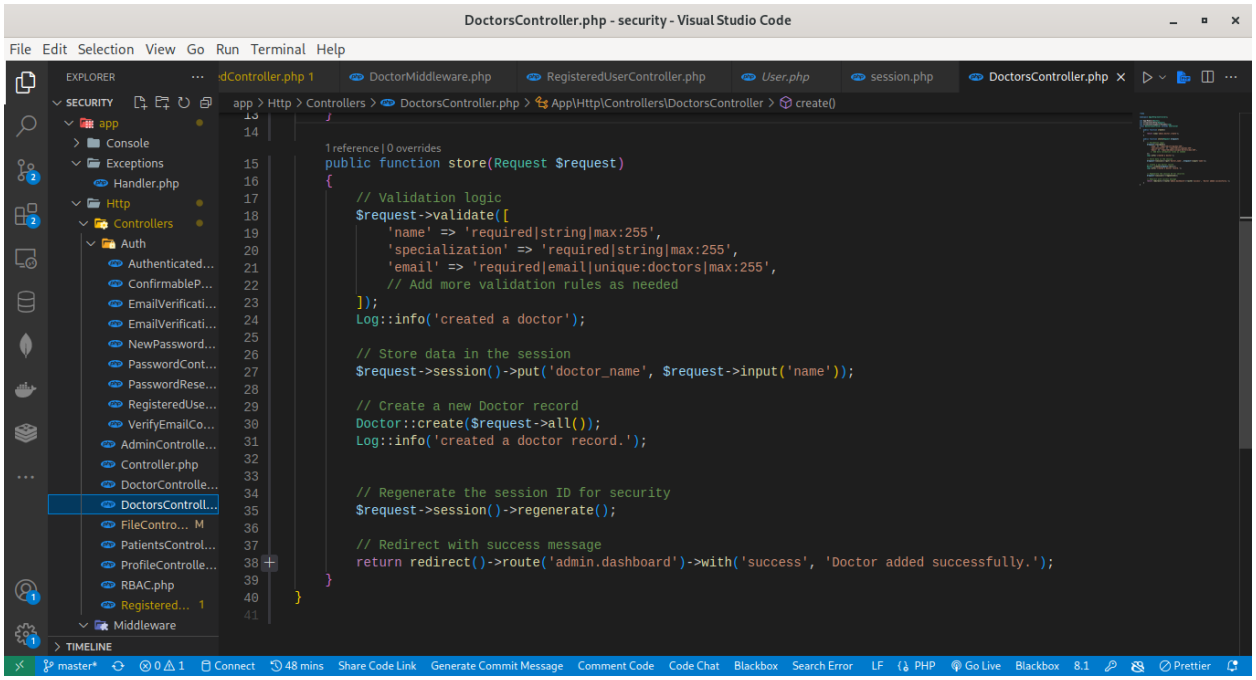
This is the fileupload controller that takes a file as input and sends it into the db
And what files could be passed to it

We also inserted a third party library that tests with all the malware file testing the file uploaded and response if there is malware or not

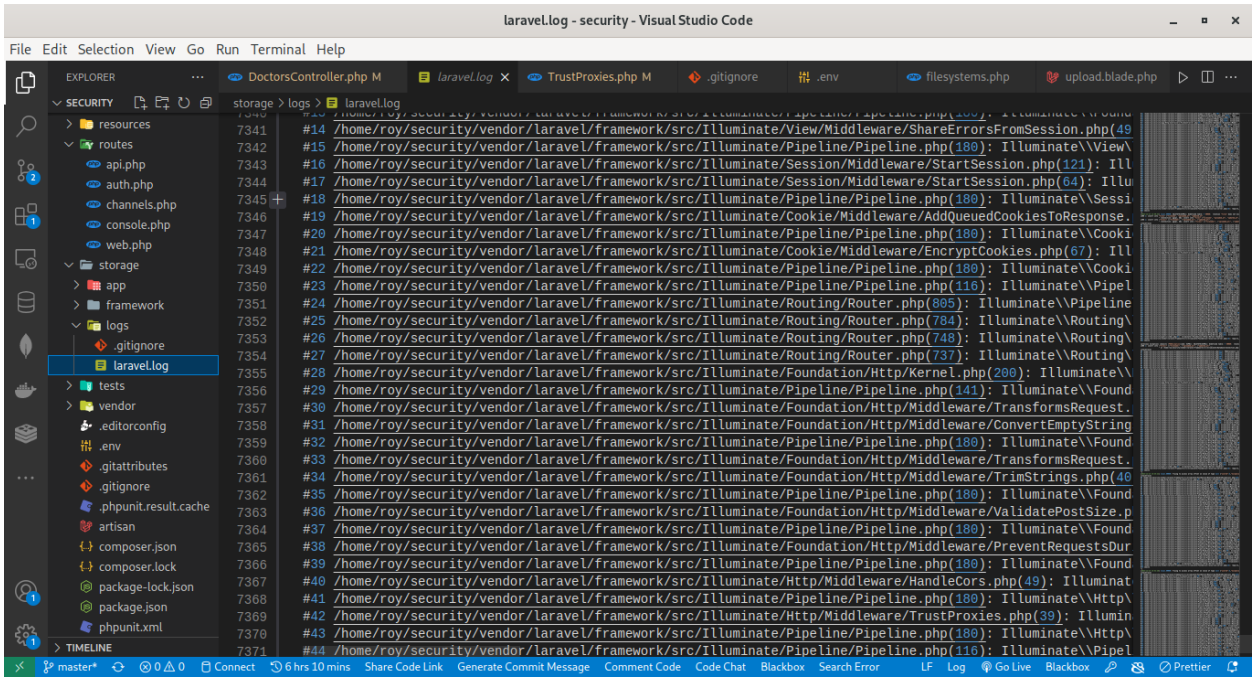
6 - Error handling and logging



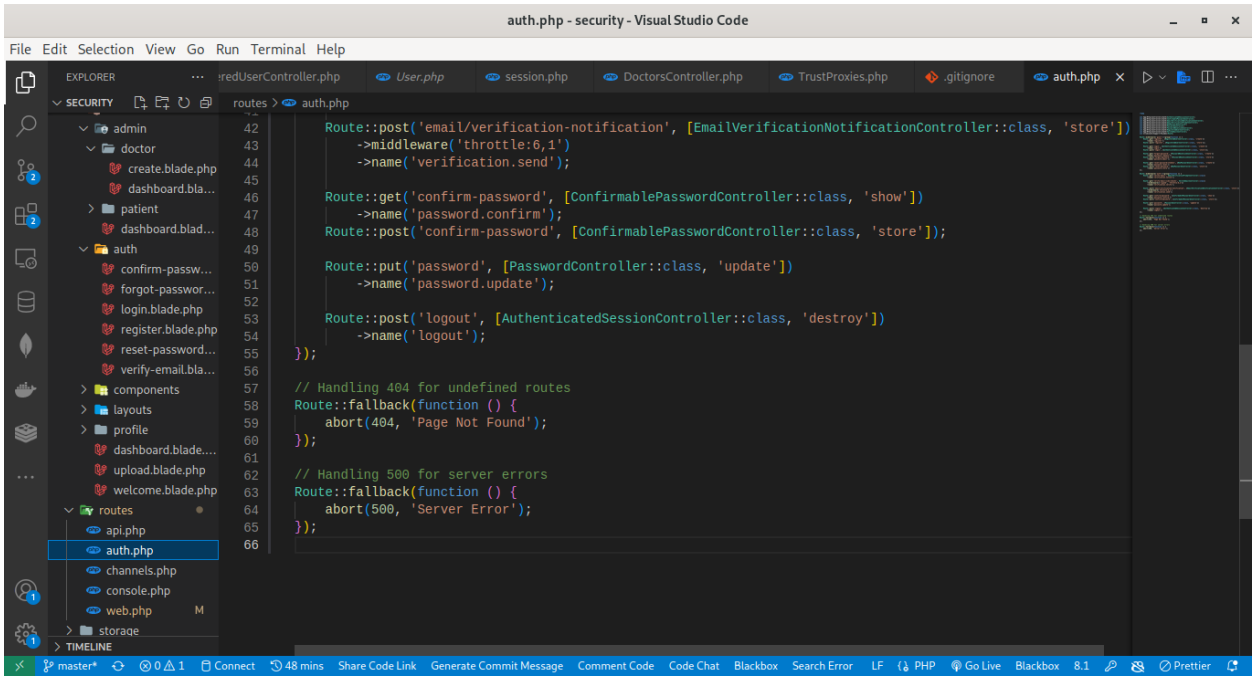
This is the config of the logging file where it is divided into channels



This is the doctor controller and here we can see where we used log::info to send it into the logs of the app

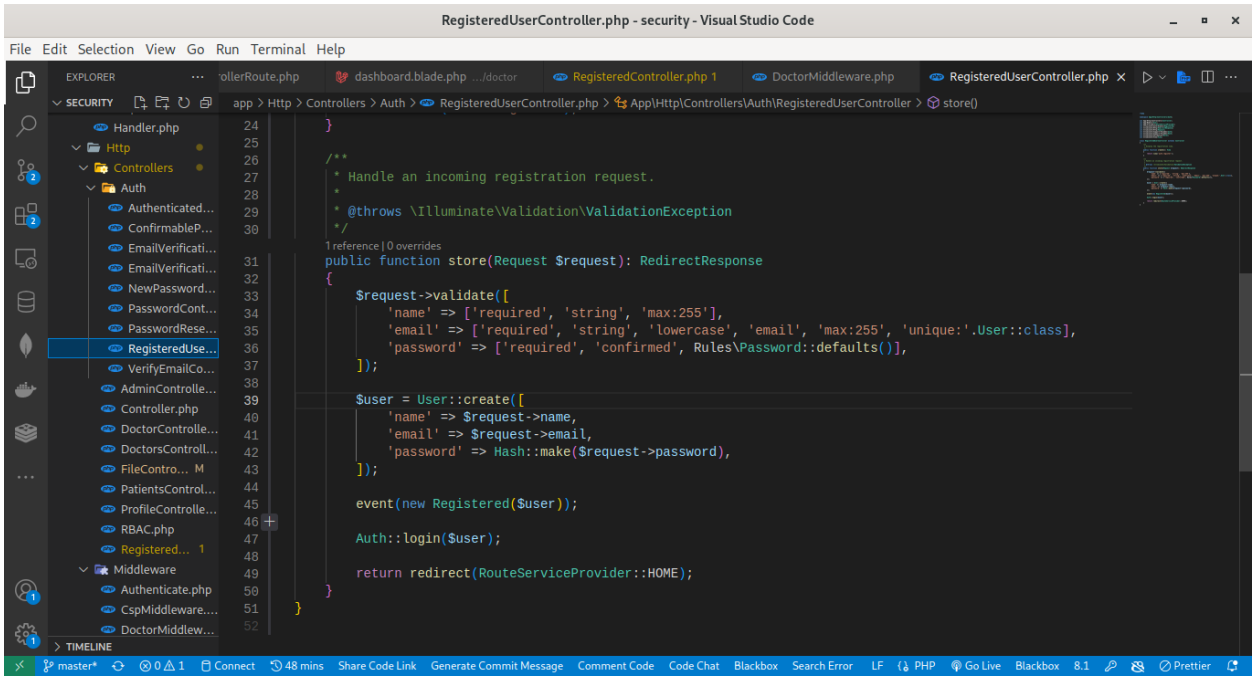


Here are the logs of the app

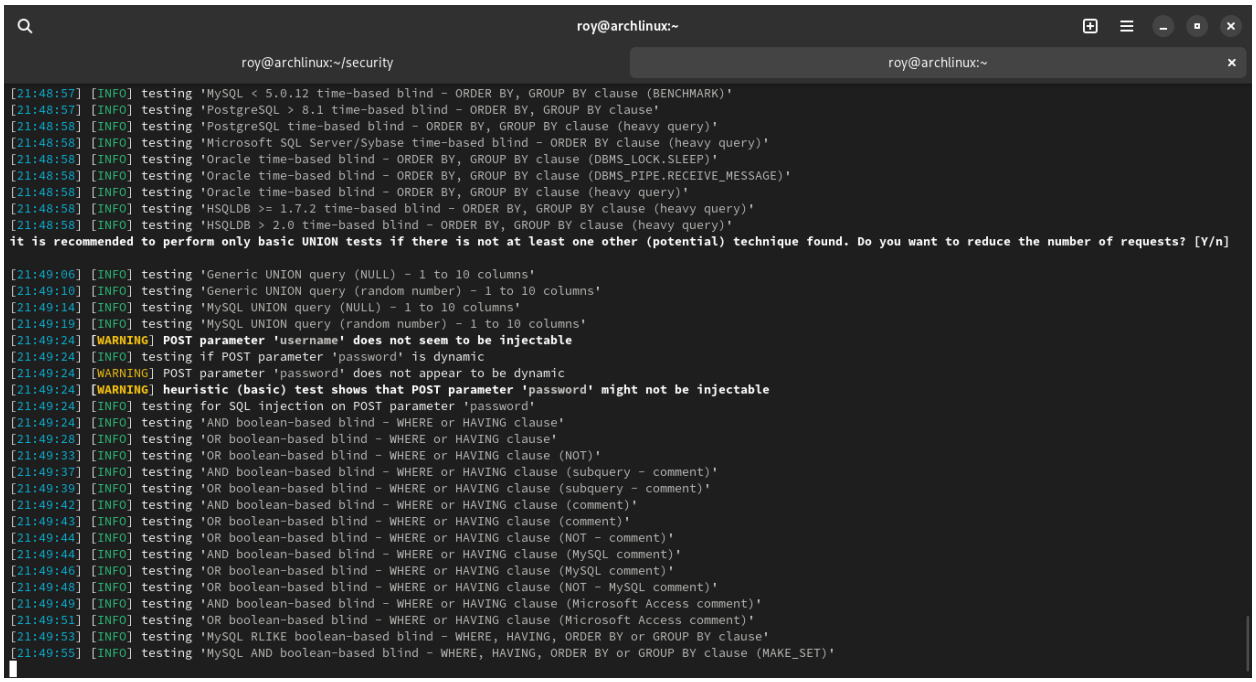


Here is the auth.php , and this is where we handles the errors that we might get come into .. code status ; 404 , 500

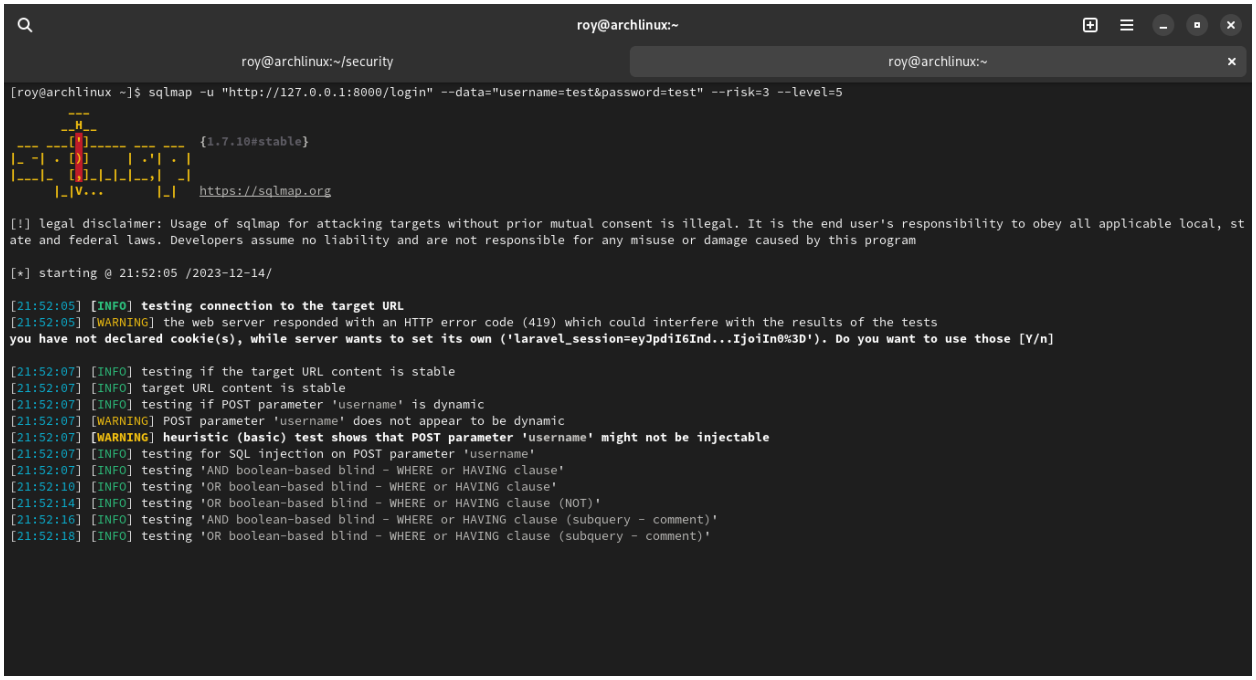
7 - **sql injection prevention and penetration testing**



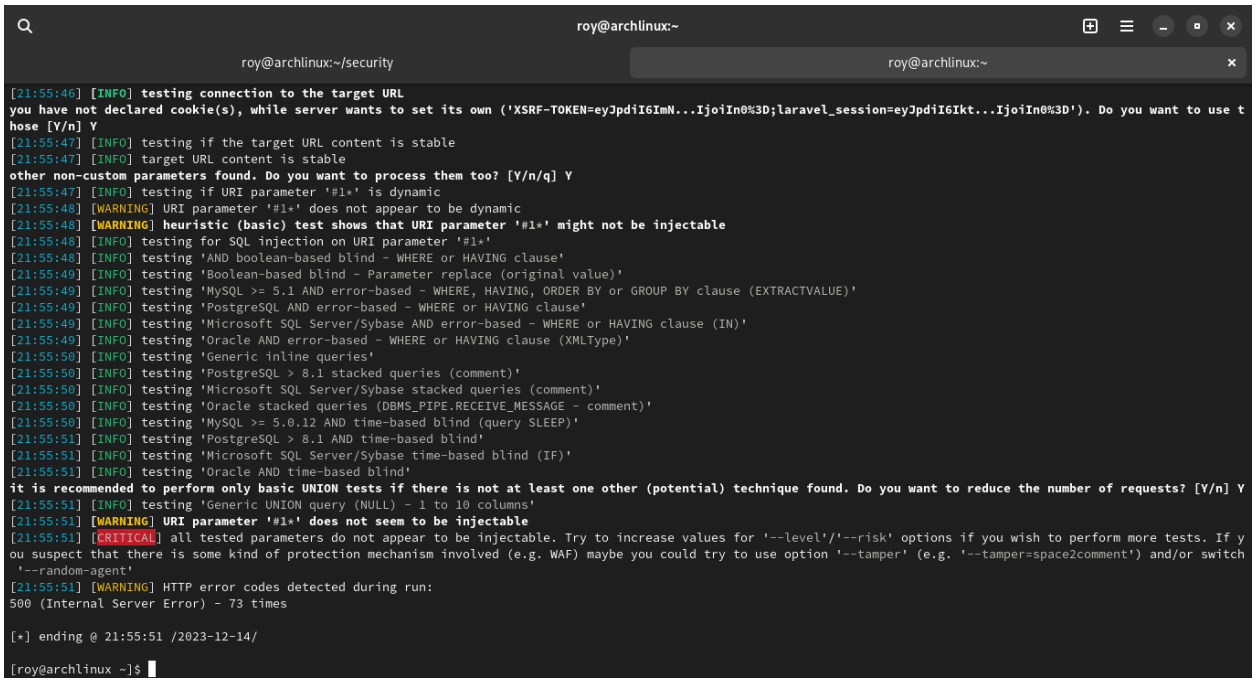
Here we inserted eloquent orm and validation to prevent all sql injection hacks



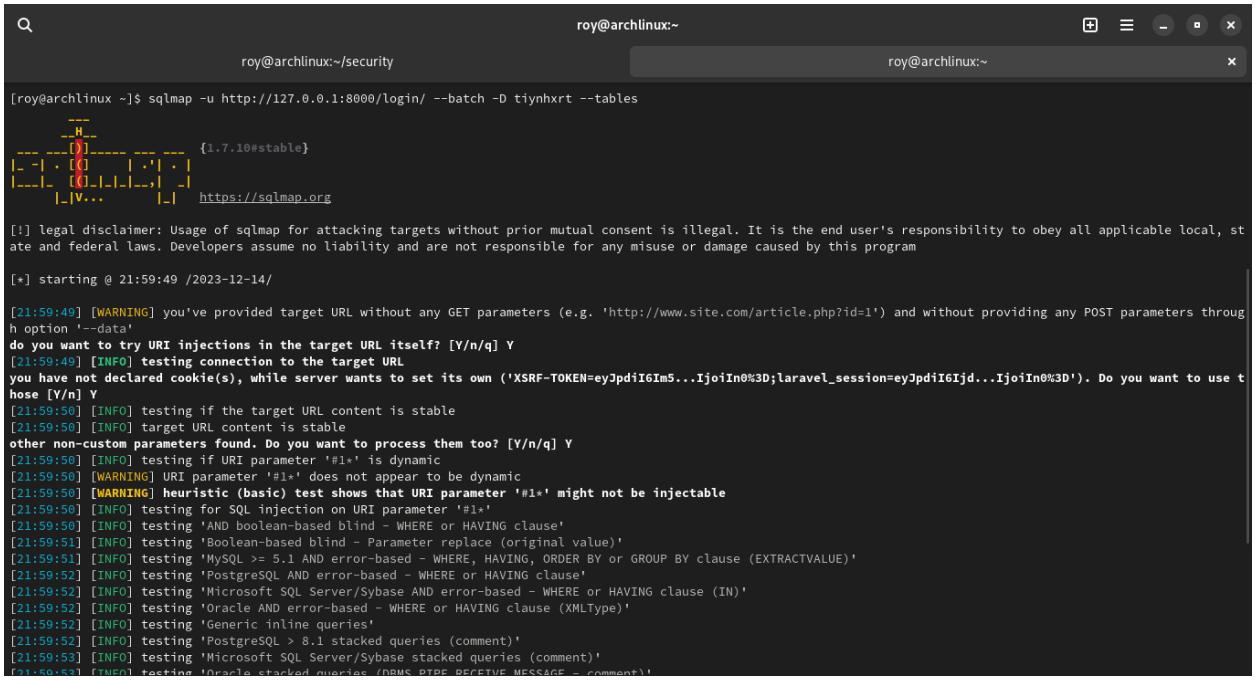
Testing our app using sqlmap , a tool made for testing sql injection



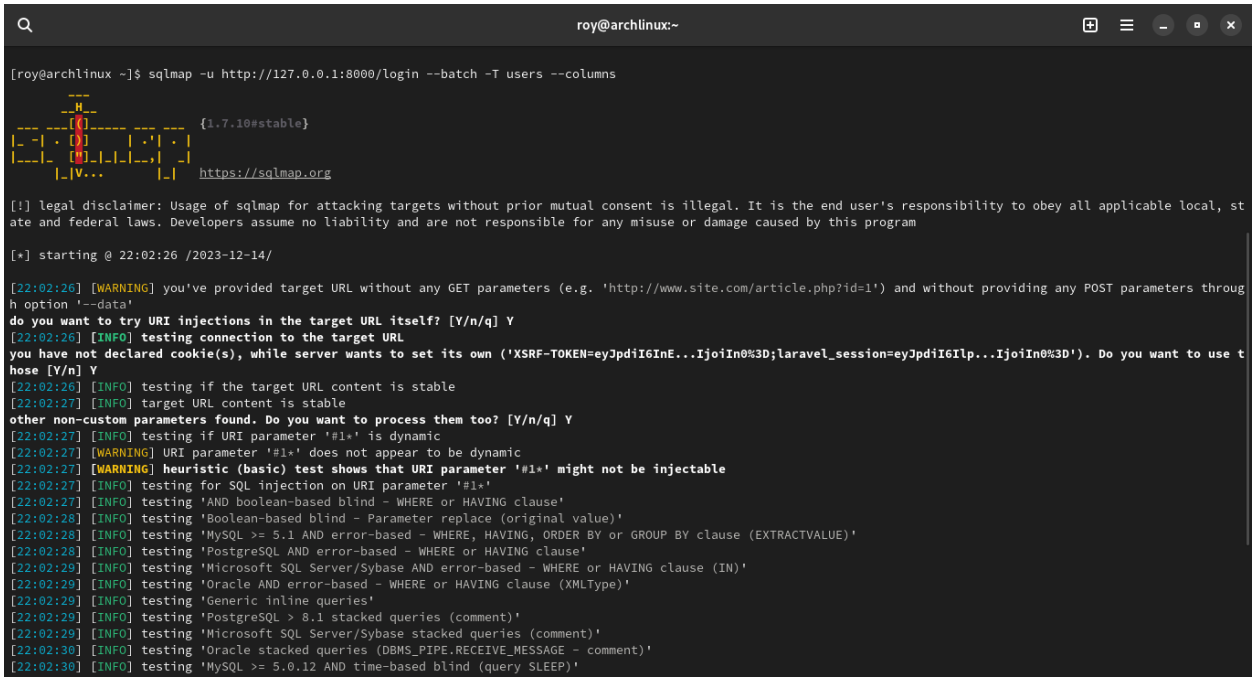
Here we gived him username = test & password = test



After finishing the testing it gives us that no parameters could be injectable

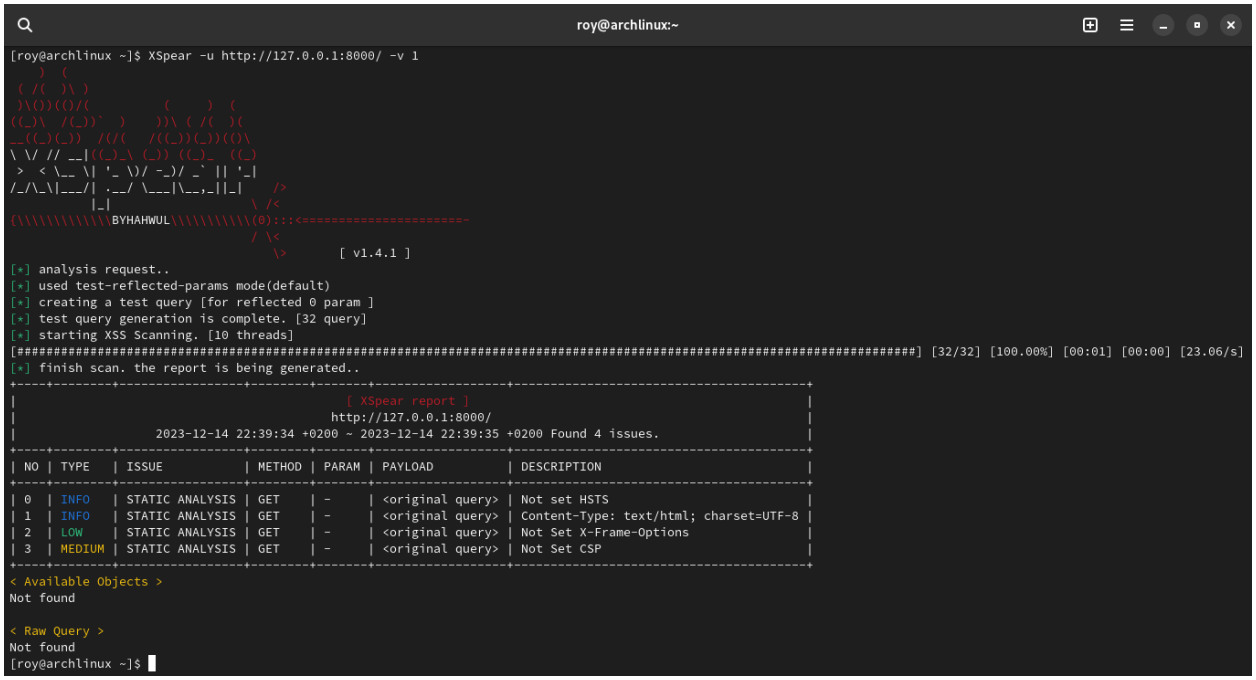


Here trying to get tables from the databse using this query



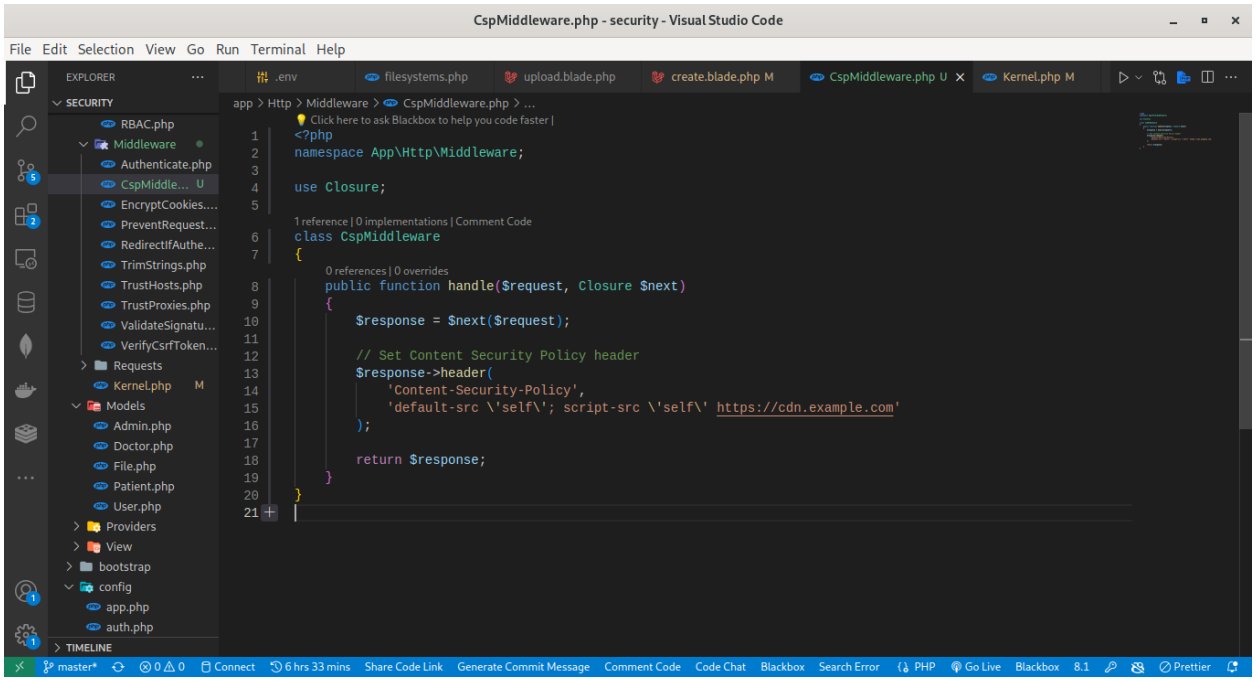
Here trying to get users from the database users table

(none of these test was successfully and this means that our sql injection prevention was totally accepted)

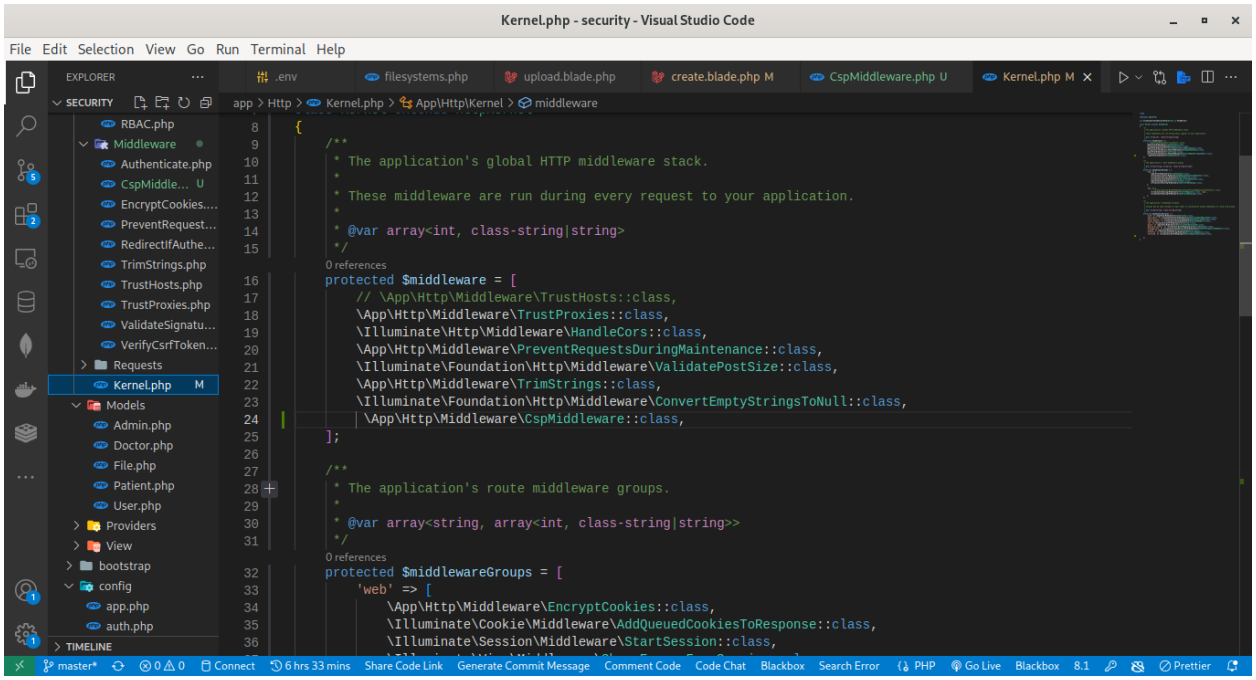


Installing another tool called XSpear that scans you the whole project and gives you a whole report about all warnings and security vulnerabilities

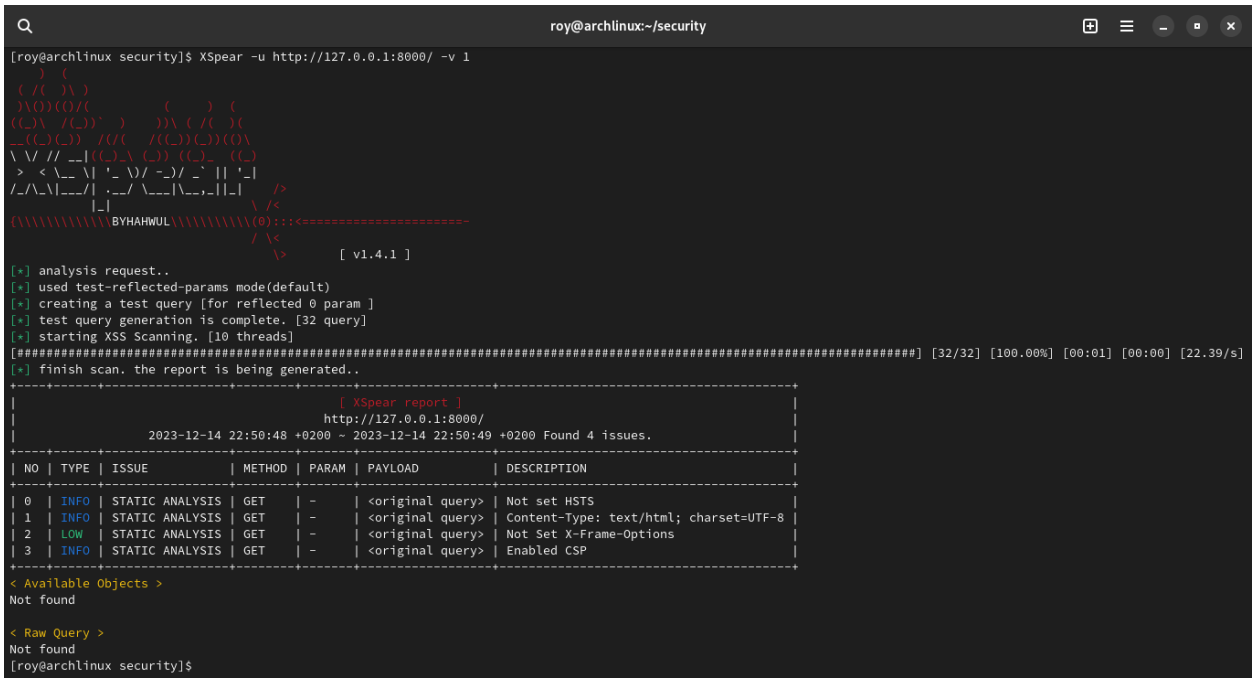
.. in this report we found out that we didn't setups CSP and that is a medium warning we have



Here we created a middleware to implement the CSP

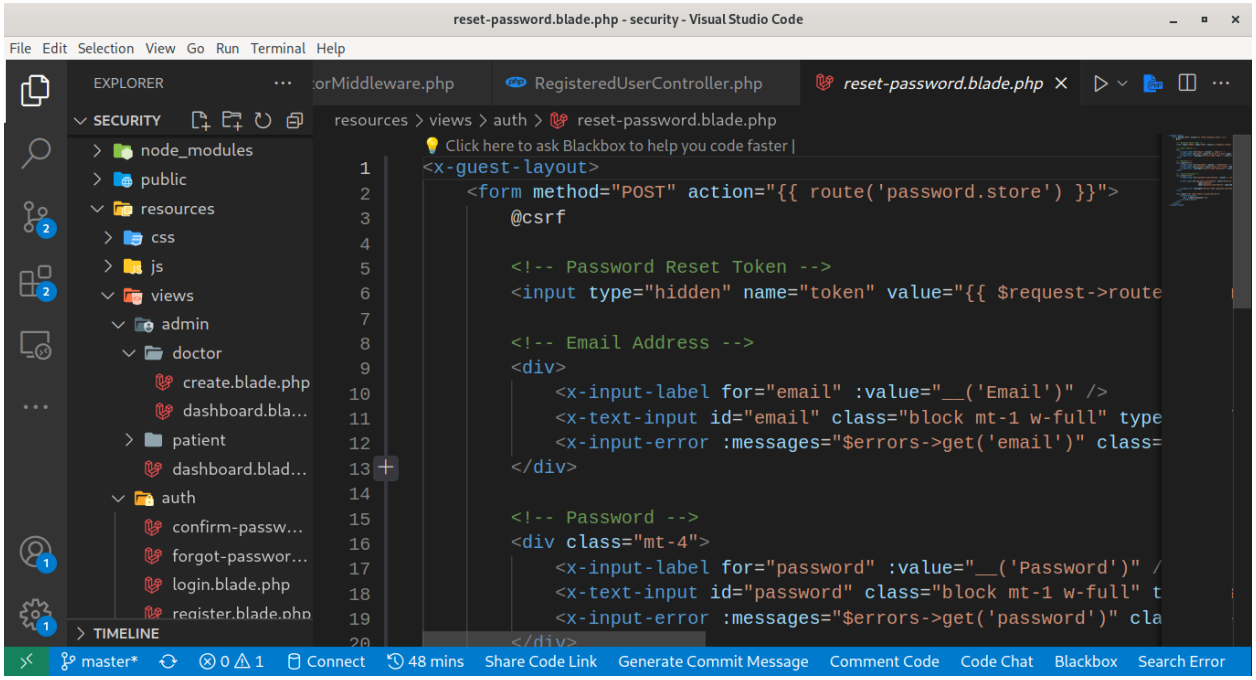


We added the middleware into the kernel.php

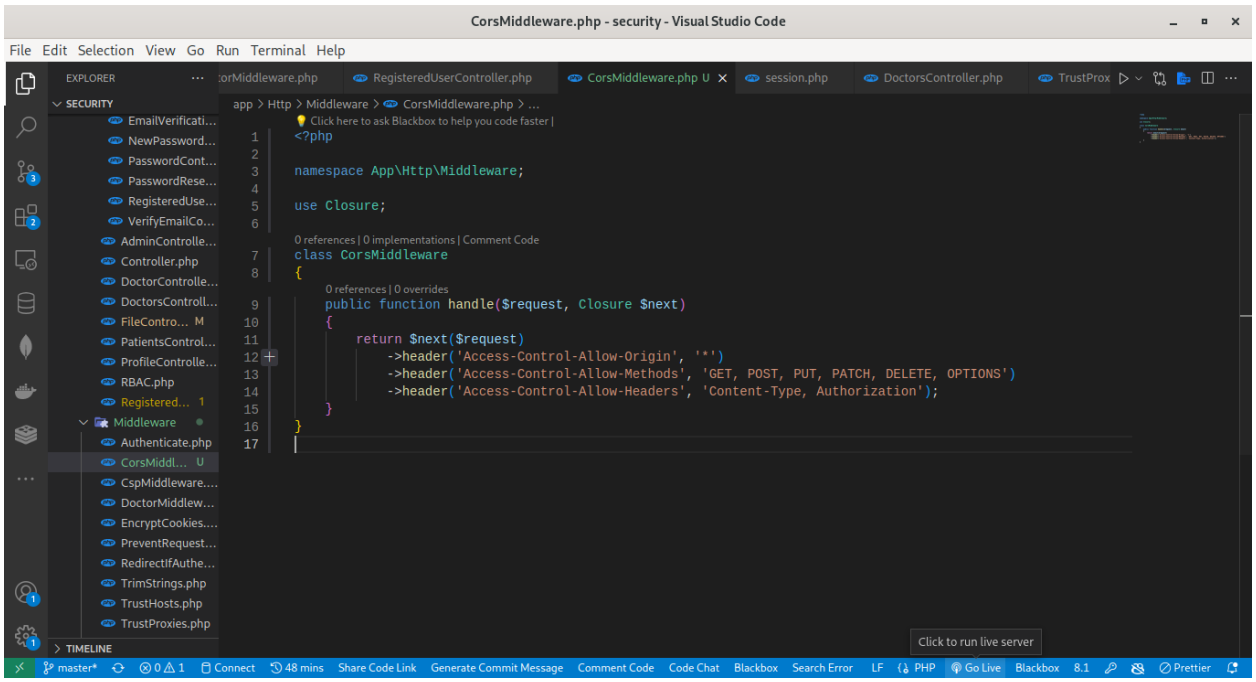


Rerunning the XSpear testing tool and found out that no critical warning are found and that we fixed the CSP vulnerability

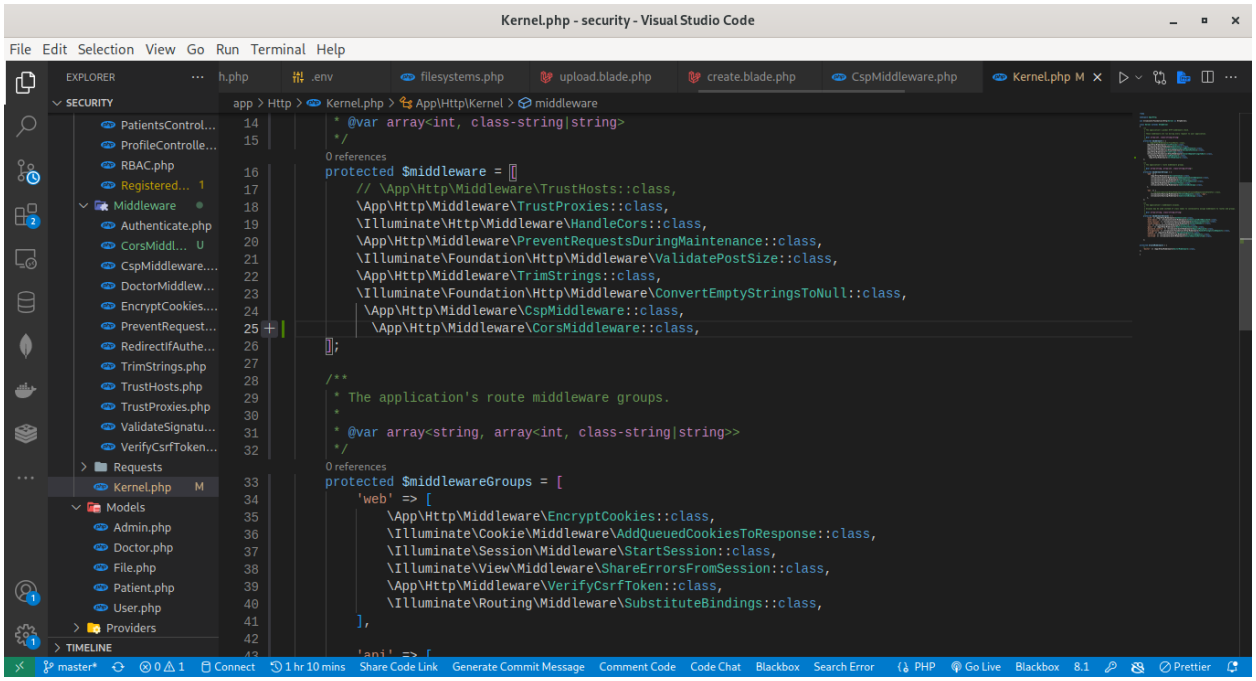
Additional setups :



In every form it is necessary to implement the CSRF to prevent all csrf attacks

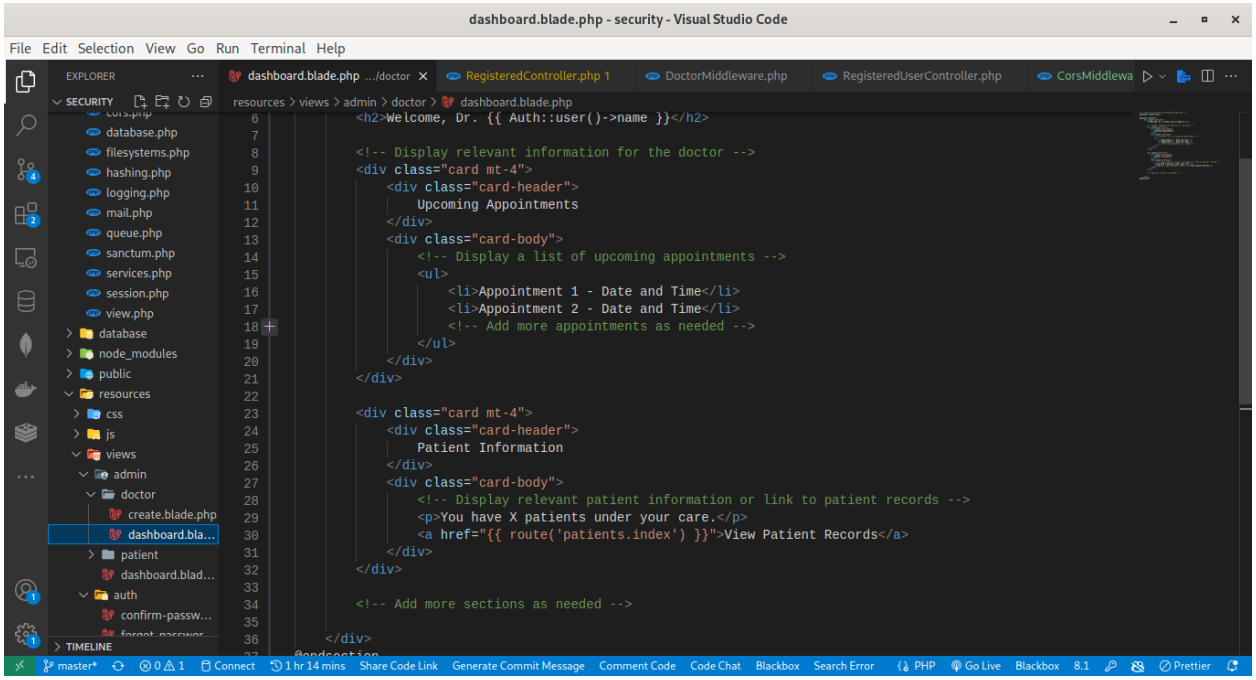


Creating a new middleware to enable CORS on laravel



Added the cors middleware into the kernel provider

And this how we implemented cors in laravel



Writing {{ }} is automatic escaping and that's to prevent XSS attacks also we can use {!! !!} for output that should not be escaped.

Final Review

- This project helped us a lot with understanding the security implementations in web apps
- This project helped us with knowing how to test our app and prevent it from all vulnerabilities using many tools and logics
- This projects helped us learn laravel as a new backend framework
- This is our github project : SecurityProject , we would be happy for any contribution

This project was created in 13/12/2023 and submitted in 15/12/2023