**Improper Access Control on the logs to Account Takeover**

During the analysis it was observed that Lumen PHP Framework was observed on the server by README.md file from directory bruteforcing.

Graphical user interface, text, email

Description automatically generated

Lumen Framework version was in running on the web server.

It was seen that the framework can be downloaded here: -

<https://github.com/laravel/lumen>

Upon reading about the server and going through the configuration it was observed that logs are generated in the specific directory of the server

Graphical user interface, text, application

Description automatically generated

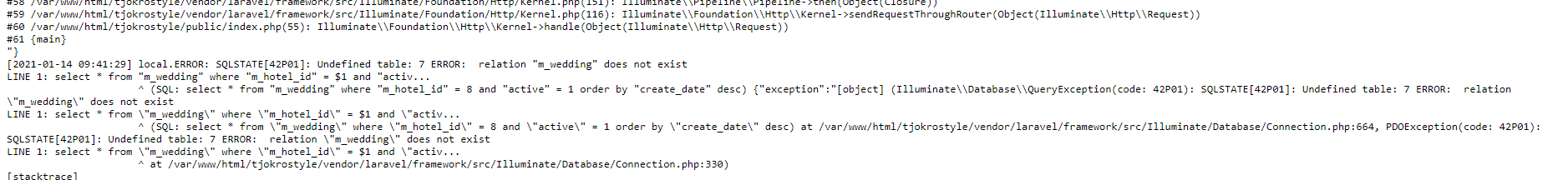
Upon digging deep it was observed that logs had a specific pattern for the file creation of logs in a format like below.

Graphical user interface, text, email

Description automatically generated

The Same was used on the application server to store the logs so I used recent dates to fetch the logs of the server.

It was observed that the logs were complete SQL commands in cleartext were observed on the server along with their succeed or failure result.



Graphical user interface, text, application

Description automatically generated

Using this it was observed that the logs had update user command where credentials were visible in cleartext along with the success message which lead to account and database takeover of the server.

Several can be found by adding google dork :- inurl:"/storage/logs/"