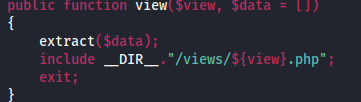
Since HTB was nice to provide the backend source code, let’s review it, below are some interesting findings, in the TimeModel.php, we can see that the command to get the date is likely vulnerable to command injection based on how the format is directly used in the command execution (which after running the web app once you would notice that it takes in a “format” parameter)



Second interesting find might be the /views/index.php

 -> this is later proved to be useless since it does not interact with the server in anyway

Lets try injecting my own commands to execute **‘;$(cat /flag)’’**, url encoded would be **%27;$(cat%20/flag)%27'** -> Nothing returned, hmm let’s try something simpler



Lets just do a single quote follow by a pipe so that we can chain the commands of formatting and our cat command

**'|cat /flag'** or url encoded would be **%27|cat%20/flag%27** -> viola that is the case

