Arsh Abbas Naqvi

24/A02/028

EHAX WRITEUP SUBMISSION

MUSIC PAGES

1.Investigation Part

The index page shows that we can navigate to any page/file here, so it was a big enough hint for me, I came to conclusion that the retrieval of other files will be in the same way it does for webpages showing the music files, which are opened by the index.php file via query only

http://$ip:$port/index.php?view=<path>

Next step was the obvious finding robots.txt, didn't work so let's skip it

Other step was to check for LFI by going back by /../.. and finding etc/passwd, sadly this didn't work either(or I was an idiot)

2../git ??

Checking the git logs was the next step, the hint also pointed to it,

The .git folder contains all the information that is necessary for project in version control and all the information about commits, remote repository address, etc. All of them are present in this folder. It also contains a log that stores your commit history so that you can roll back to history.

The .git folder is present by default in every repo, it contains the following folders

- hooks/: This folder contains your client or server-side hook scripts
- **logs/**: It stores the records of all the changes you made. If you open the files you will find information about the log details, like what kind of changes you made, your name, email etc. (may contain flag)
- **logs/HEAD**: This stores the information about all the changes that have been made.(may contain flag)
- objects/: This folder stores all the content

3. Executing the final payload

Now we have the potential candidates to navigate to

After navigating to each of them we would come to the conclusion that the flag is located inside

http://$ip:$port/index.php?view=.git/logs/HEAD