MID REVIEW

ISP-2020 Hyper-Pace

H.V.I.S Alex   Y.D.M Kahatagahawatta

Hyper-Pace project summarization for the Mid Review

This is a web based CTF which is targeted to the general audience of the information security sector especially beginner level enthusiasts.

So until now, we have created the environment for the challenges to be hosted. The environment will be a series of web pages where the user can make themselves an account to access certain challenges. Up to now we included three challenges which are : SQL injection challenge for the login form , picture steganographic challenge and the cryptography challenge

SQL injection challenge walkthrough

First the user will have to check whether a particular page is vulnerable to SQL injection attacks.

Second the user will figure out what the vulnerable query and try to make a remote executable query.

Third, the user will have to access the database and get the flag that is in the database.

Picture Steganographic Challenge

The user will have to find the right image out of all the steganographic images that have been included. The user will have to download the image and decrypt it and get the flag.

Cryptographic Challenge

The user will have to access the challenge through the crypto tab. The text will be encrypted and the key to it must be found by solving the riddle provided at the bottom of the page. By decrypting the passage the player will be able to get a clue of a hidden url. Upon accessing the hidden url the user will be directed to page where he will have to find the hidden flag.

Future plans

We hope of implementing these challenges in the near future:

- Reverse engineering challenge for a selected executable file.
- Pdf meta-data analysis challenge.
- Audio steganography challenge.

There are also some other challenges that are to be implemented