



Loki

A ML-platform about adversarial attacks



3 people

Project Description

Is your nightmare called adversarial attack? Come face it here, and develop a web platform allowing to observe the influence of a selected attack on a dataset.

Skills

Python



Machine Learning



HTML



(*)[The skill scale is from 0 (Fundamental Awareness) to 6 (Expert).]

Level 1

You may now pursue to the level 1 of the project.

- * **Web platform**
Design the architecture of your web platform to make sure everything is running online easily. Don't start from scratch!
- * **Role**
Add the possibility to be a simple member or a administrator, with a special access.
- * **Upload a picture**
Implement a webpage to upload a picture or a dataset.
- * **Display and store results**
Add a feature to display precise results on the effectiveness of the selected previous attack. Don't forget to set up a way to store it, linking it to your own account.
- * **Database**
Implement a database for your need.
- * **Basic unit tests**
Implement simple unit tests to be sure that everyone can create an account, upload a picture, obtain result, etc.



Loki

A ML-platform about adversarial attacks



3 people

Project Description

Is your nightmare called adversarial attack? Come face it here, and develop a web platform allowing to observe the influence of a selected attack on a dataset.

Skills

Python



Machine Learning



HTML



(*)[The skill scale is from 0 (Fundamental Awareness) to 6 (Expert).]

Level 2

Level 1 must be unlocked to read this section

- * **Developer Documentation** Required for lvl 2 validation
Document your project (not necessarily only in the source code) so that a newcomers developer could understand and contribute to the code.
- * **Release** Required for lvl 2 validation
Produce a release as a source archive or git tag. The release files should have up-to-date README and INSTALL files and more generally allow anyone to deploy the application.
- ** **Attack in action**
Implement at least one typical attack to discover the result of your job.
- *** **Boost your tests**
Study the paper that you can find here: <https://arxiv.org/pdf/1608.04644.pdf>. Collect the same classifier and datasets to check that you obtain a very close result when you compare it to this article.