For example, when we look at sql enjection vulnerabilities:

1) Bad and good http request coming from sql\_bad\_demotestfire\_all.log and good.log file respectively(these files was created by using burpsuite with payloads from different github repositories for bad log and burpsuite web crawling option used for good log)(folder: 1\_making\_dataset\_and\_ml\_model\_comparing /2-sql/)

2) We converted these files into csv files.( by using sql\_bad\_demotestfire\_all.py which includes some parts of code from github repositories debasishm89/burpy.)

3) After 1st and 2nd steps, we obtained the data for machine learning process.

4) By using python we wrote code for mitmproxy in order to work on real-time protection (virtual environment was created) (folder: ml\_env3)

- firstly waf\_sql\_cmd.py must be run

- waf\_sql\_cmd.py is related to waf\_sql\_kod.py

All the above steps were done for other types of vulnerability.And machine learning performance was calculated for all vulnerabilities.

The files obtained in real time for all vulnerabilities were combined into a single csv file and the performance of machine learning was measured.(webserver\_log\_files/0\_all/ confusion\_matrix.jpg)