Introduction

An SQL injection vulnerability in a web application should be discussed with a third party. Therefore, the web server access log file and the customer database have to be shared as a basis for this discussion. Such sensitive data must be anonymized before sending it to a third party.

In the resources section you will find a zip file containing the following files:

- access.log: the web server access log with the attack patterns
- customerdata.db: the database with customer data
- checksums.sha256: SHA-256 checksums for any binary files required for this task
- encrypt_cc.py: a copy from the application's source code for your reference

Goal & Tasks

- Describe and justify in a short report which data from the files access.log and customerdata.db must be masked, pseudo-anonymized or anonymized.
- Mask, pseudo-anonymize and anonymize all relevant data in the files access.log and customerdata.db by using suitable methods or tools. Be careful not to destroy the actual attack patterns or timeline.
- Describe in the report how the anonymization was done.

Submission

ZIP file with the following contents:

- PDF report with all information as required in the section goal above.
- The anonymized access.log and customerdata.db files
- Any scripts / programs you wrote for this task as separate source files