# Source Code Patterns of SQL Injection Vulnerabilities

Looking into the OWASP Top Ten shows that the same vulnerability categories are occurring all the time. One of the top categories is still. A lot of research has been done on SQL injection. To discover the reason why the same vulnerabilities are occurring, we investigated the source code from open source projects. For the source code, similar methods and operations are grouped up and are called source code patterns. Our work shows which source code patterns occur in real life projects, to provide a data set that can be compared to existing vulnerability data sets like SAMATE SARD Another aspect will be using this data set to provide exercises for software developers to learn or improve their software security skills. Training developers with a data set based on existing vulnerabilities helps developers to identify vulnerabilities beyond artificial samples. The first question to be answered is: How such source code patterns look like? The next question is, are there any special cases that are not typical for SQL injection vulnerabilities? Real source code samples are investigated to get answers to these questions.

The presentation will split up into …

The first part describe how the source code samples are received. How the crawler works and how these source code samples are mined. An overview of the results will be presented.
The second part describes the reviewing process. What important parts were looked for and how everything was reviewed. The different categories which were created based on the review results are presented. Some code snippets will be shown as examples.
The last part of the presentation will provide an comparision to related work. Additionally the future work for Insecurity Refactoring will be described.