# Database Schema of

# Software Patch Management

# Web Application

**Sponsored by: Coupa Software**

*Team members:*

Amruta Gadgil

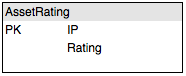
Fei Hao

Pramothini Dhandapany

*Faculty advisor:*

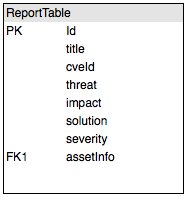
Patrick Tague ([tague@cmu.edu](mailto:tague@cmu.edu))

December 11, 2015

 Based on the goal and system design, the web application should have three tables in database to store data.

*Fig. 1 Database schema for assets and importance rating*

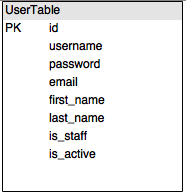
The first one is asset importance table (in Fig. 1), which uses IP as its prime key. Each asset will be identified by its IP, and will have an importance rating, which could be updated by system administrator.

 Assets will not be removed from database. When uploading a new Qualys scan report, new assets will be added into the table with default rating of 5, while old assets will not be deleted and their rating will be kept.

*Fig. 2 Database schema for vulnerabilities report*

The second one is the vulnerability report table (in Fig. 2), which uses ID as its prime key. Each vulnerabilities will be identified by its ID, and will have a series of information describing the severity, the title, the impact and the possible solution for this vulnerability. IP of the asset on which the vulnerability was detected cannot be used as primary key because there might be multiple vulnerabilities for one IP. For each vulnerability, it will fetch asset (IP) importance rating from AssetRating table.

When uploading a new Qualys scan report, new vulnerabilities of current report will be added into the table, while old vulnerabilities will be removed.



*Fig. 3 Database schema for user account*

The third one is the user account table (in Fig. 3), since the web application has authentication and privilege setting. Each user account will be identified by its ID, and will have a series of information like username, email, and password. The authentication and privilege of a user account is set by “is\_staff” and “is\_active” fields.