Secure Web Tools

A secure web service that allows a registered user to login and upload a source code file to be statically analyzed. The user name and password need to conform to a set regular expression to be considered valid and prevent sql injections. Once the user logs in, there is an option to either view previously uploaded files or upload new files. While uploading, a file needs to have a valid name and extension that is checked using flask’s secure\_filename which returns a secure version of the filename to prevent malicious names and extensions and in effect stop malicious html files being uploaded to prevent XSS attacks. A limit is set based on the size of the file. Files larger than 10MB are rejected.

Once the file is uploaded it is encrypted using aes 256 with an initialization vector and a secret key and stored in a Mysql table on RDS. On click of the upload button, the service decrypts and statically analyses the file based on the file type. FindBugs for .class files, flawfinder for .cpp etc. The result of the analysis is written into a file and stored on the EC2 instance which abides by the least privilege principle having only read permissions. The contents of the file are displayed to the user. Each user can view files that he has uploaded and can choose to view the analysis result of each of his files.

A session timeout of 5 minutes is set after which the user is automatically logged out. Hence preventing session hijack attacks. A config file held all the configuration details hence separating concerns and storing configuration details securely. The number of failed login attempts is set to 3 to prevent password attacks.

An attempt was made to secure communications with the server with SSL using self-signed certificates but could not be implemented within the given time line.