Design Changes Based On Threat Assessment

The following design changes are proposed for a roguelike dungeon crawler game that implements procedural content generation in order to mitigate threats found using OWASP Threat Dragon:

Captcha acts as the first level of defence for the game given that it provides a Captcha test to any visitor it deems as a threat to game. A Captcha test efficiently removes bots that cannot read and supply a correct answer to the test.

The addition of a login system reduces the likelihood of manipulation by malware as a login system allows for proper validation of users' inputs and proper encoding of outputs.

Cryptographic Protocols such as salting are deployed to battle hackers who implements Trojan hacks. Salting prevents hackers who have gained access to one user’s hashed password from gaining access to other users with the same password thus reducing the cost of such an attack.

Source code files are protected by the addition of a firewall which adds a level of encryption for the game and prevent hackers from performing Local File Inclusion.

Source code can further be protected with the use of two-factor authentication which can block any suspicious sign-in attempts by requiring access to another authentication factor e.g., phone or email.

SQL Injection attacks on the dungeon database for the game can be avoided by the use of input validation and parametrized queries which include SQL prepared statements.