Suite 4

Information source Lists

The account are stored in a mySql database which is checked and maintained by the server. If the connection is not made correctly there could be potentially severe performance issiues.

Users need to see who is connected to the system, what games are active, and they need to access to their account setting.

- Test Item 4.1 Information Pipeline ( high level of risk)

That the information flow follows specification

- Login: client->server->database->server->client

- Chat/gaming client -> server-> client(s)

- Private Message client->server->client

- Test Item 4.2 Checks and Balances (medium High level of risk).

- User account verification must take place during logon.

- Password authentication must take place during logon

- Test Item 4.3 Security and Fault – tolerance(error checking/ program stability) Information display (“Low level of risk”)

- Displays:

- Server not available

- Incorrect account information

- connection lost

Risk analysis:

The ranching is based on a security level that each test has and the overall security impact that it has to the application. Flaws in the pipeline could create a theft of identity with a intrusion in the clients computer.

Risk analysis

4.1 “ High level of risk “

- The information flow does not follow requirements

- Risk of injecting html tags or scripts in the chat-box .

- possibility in stealing conversation chat information.

- All storing procedure is not done in the MySql instead it uses an intermediate stage in the

Back-end part.

4.2 ”Medium High level of Risk”

- The application does not require always a logon procedure after a first logon and browser is

closed or connection is lost.

- Password authentication does not follow Html type password there for it is visible to the

Screen.

- The recover password /username does not work properly

4.3 “Low level of Risk”

- The application does not display the statuses .