|  |  |  |
| --- | --- | --- |
| Use Case Name: Security Enhancement | ID: | Importance: |

|  |  |
| --- | --- |
| Primary Actor: Security Administrators | Use Case Type: Non-functional |

|  |
| --- |
| Stakeholders: Security Administrators, Developers, Users |
| Brief Description: The online Texas Hold'em poker game is operational and actively used by players. The security administrator aims to proactively enhance the overall security of the game. |
| Trigger: The Security Administrator reviews the current security measures and assesses the overall security posture of the game. Type: **External** / Temporal |
| Relationships: |
| Normal Flow of Events:  The administrator conducts a comprehensive risk assessment to identify potential security gaps and areas that may need improvement. This assessment includes a review of:   * **User Authentication**: Evaluating the strength of user authentication mechanisms, including password policies and multi-factor authentication options. * **Data Encryption**: Assessing data encryption protocols for protecting sensitive player information, including financial transactions. * **Access Control**: Reviewing and tightening access control policies to restrict access to sensitive system components. * **Server Security**: Evaluating server security, including the hosting environment, to ensure servers are well-protected from physical and digital threats. * **Security Awareness**: Reviewing the presence of security awareness and training programs for both players and internal staff.   The administrator develops a set of general security enhancements based on the findings of the risk assessment. These enhancements may include:   * **Implementing Stronger Encryption**: Upgrading data encryption to higher standards to better protect player data. * **User Account Security**: Introducing additional security features, such as security questions, to enhance user account security. * **Regular Security Audits**: Scheduling regular security audits and penetration testing to proactively identify and address vulnerabilities. * **Access Control Improvements**: Implementing more granular access control to ensure that only authorized personnel have access to sensitive parts of the system. * **Incident Response Plan**: Developing or enhancing an incident response plan to effectively address security incidents if they occur. |
| Subflows: |
| Alternate Flows: |