|  |  |  |
| --- | --- | --- |
| RAZDA Co. | | |
| **Filename: [security\_alerts.py]** | | |
| **Summary***:*  This file monitors security-related events such as failed login attempts, account lockouts, and unlocks in the Razda Market system. It helps prevent unauthorized access by enforcing lockout policies after multiple failed login attempts and generates security alerts for suspicious activity. | | |
| ***Processes*** | | |
| * **Failed Login Monitoring** | **Continuously monitors failed login attempts and tracks users with repeated failures. Triggers alerts if attempts exceed a threshold.** | |
| * **Account Lockout Management** | **Locks accounts that exceed the failed login threshold, adding the user to a lockout list and triggering a high-severity alert.** | |
| * **Automatic Account Unlock** | **Periodically checks and unlocks user accounts after the lockout duration has passed, restoring access to locked-out users.** | |
| * **Security Alert Logging** | **Logs all security alerts, such as lockouts and errors, for review by administrators and audit purposes.** | |
| * **Generate Security Report** | **Generates a report of security events within a specified date range, allowing administrators to analyze security incidents over time.** | |
| * **Display Recent Alerts** | **Shows the most recent security alerts from the log file, enabling quick review of recent security incidents.** | |
| **Files it Gets Information From:** | | **Files it Sends too:** |
| * **Environment Variables** (dotenv): For DB credentials, failed login threshold, and lockout duration. | * **Log File** (security\_alerts.log): Logs details of security alerts and account lockouts. | |
| * **Database** (razda\_market\_db): Retrieves failed login attempts from login\_attempts table. | * **Alert Manager**: Sends security alerts to alert\_manager for processing and admin notifications. | |
| * **Alert Manager** (alert\_manager): Manages alerts based on security events in the system. | * **Database** (razda\_market\_db): Updates account status for locked and unlocked users as needed. | |
| **Expected input into file:** | | **Expected output from file:** |
| **Security Configuration**: Failed login threshold and lockout duration define the rules for account lockouts.  **Login Attempt Data**: Retrieves login attempt records from the login\_attempts table for monitoring | | **Alerts**: Sends alerts to alert\_manager when thresholds are exceeded.  **Security Log**: Logs all monitored events, including lockouts, unlocks, and other security issues. |
| **Things that need to be taking place:** | | |
| |  | | --- | | **● Continuous Monitoring: Regularly checks for failed login attempts to prevent unauthorized access.** |  |  | | --- | | **● Alert Triggering: Sends security alerts to alert\_manager if a user exceeds failed login attempts, enabling rapid response.** |  |  | | --- | | **● Automatic Lockout Enforcement: Locks out accounts that exceed the failed login threshold, enforcing Razda Market's security policy.** |  |  | | --- | | **● Automatic Account Unlocks: Periodically unlocks accounts after the lockout duration expires, restoring access for legitimate users.** |  |  | | --- | | **● Logging and Auditing: Maintains logs of all security events, supporting audits and accountability for security-related actions.** |  |  | | --- | | **● Configurable Thresholds: Uses environment variables for customizable lockout duration and failed login limits, adapting to varying security needs.** |  |  | | --- | | **● Security Reporting: Allows generation of security event reports, providing insight into security trends and helping with incident response planning.** |  |  | | --- | |  | | | |
| Edit log (update each time you make changes to doc or file). | | |
| Contribution to the entire Project:  The **security\_alerts.py** file plays a vital role in securing the Razda Market platform by detecting suspicious login behavior and enforcing account lockouts. This file’s robust alerting, lockout management, and reporting capabilities help prevent unauthorized access, ensuring account security and protecting user data. Its integration with alert manager ensures that administrators are promptly notified of potential security breaches. | | |
| * Oliver Smith (Razda Admin) Nov 8, 2024: Configured to monitor failed logins, manage account lockouts, trigger alerts, and generate security reports. | | |