***Subsystem Name: Prosecutors office***

***Group Names:***

1. ***Laila Al-shibami***
2. ***Fatima Hassan***
3. ***Nabeel Khalid***

**Table of Contents**

[1 Scope 3](#_Toc185363366)

[1.1 Information 3](#_Toc185363367)

[1.2 Dependencies 3](#_Toc185363368)

[1.3 Entry Points 3](#_Toc185363369)

[1.4 Exit Points 3](#_Toc185363370)

[1.5 Assets 3](#_Toc185363371)

[1.6 Trust Levels 3](#_Toc185363372)

[1.7 Data Flow Diagrams 3](#_Toc185363373)

[2 Break 4](#_Toc185363374)

[2.1 STRIDE Framework 4](#_Toc185363375)

[2.2 Threat Analysis 4](#_Toc185363376)

[2.2.1 Attack Trees 4](#_Toc185363377)

[2.2.2 Misuse Cases 4](#_Toc185363378)

[2.2.3 Threat Description Table 4](#_Toc185363379)

[2.3 Ranking 4](#_Toc185363380)

[2.3.1 Delphi Ranking 4](#_Toc185363381)

[2.3.2 Average Ranking 4](#_Toc185363382)

[2.3.3 Probability x Impact (P x I) Ranking 4](#_Toc185363383)

[3 Fix 5](#_Toc185363384)

[4 Verify 6](#_Toc185363385)

[4.1 Review Documentation 6](#_Toc185363386)

[4.2 Test cases 6](#_Toc185363387)

[4.3 Validation 6](#_Toc185363388)

1. **Scope**

The purpose of this threat modeling document is to analyze and mitigate potential vulnerabilities in the Prosecutor's Case Management System. This system manages sensitive legal case files, evidence, and associated documents, ensuring their security and integrity.

1. **Information**

* **Application Name:** Prosecutor's Case Management System
* **Application Version:** 1.0
* **Description:** A secure digital platform for storing, managing, and retrieving sensitive legal data.
* **Document Owner:** Mohammed Alqmase
* **Participants:** Security analysts, IT personnel, and system users.
* **Reviewer:** Security lead or external consultant

1. **Dependencies**

|  |  |  |
| --- | --- | --- |
| ID | External Dependency | Description |
| 1 | Database Server | MySQL or PostgreSQL for storing case data. |
| 2 | Authentication Service | OAuth 2.0 for secure user login and role management. |
| 3 | Backup and Restore System | Regular backups to external storage. |
| 4 | Network Security Infrastructure | Firewalls and intrusion detection systems. |

1. **Entry Points**

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Trust Level |
| 1 | Web Portal | User login for prosecutors and staff. | High |
| 2 | API Endpoint | Case data submission via integration. | Medium |
| 3 | Mobile Access | Access through secure mobile apps. | Medium |
| 4 | Admin Console | Administrative configuration and logs. | High |

1. **Exit Points**

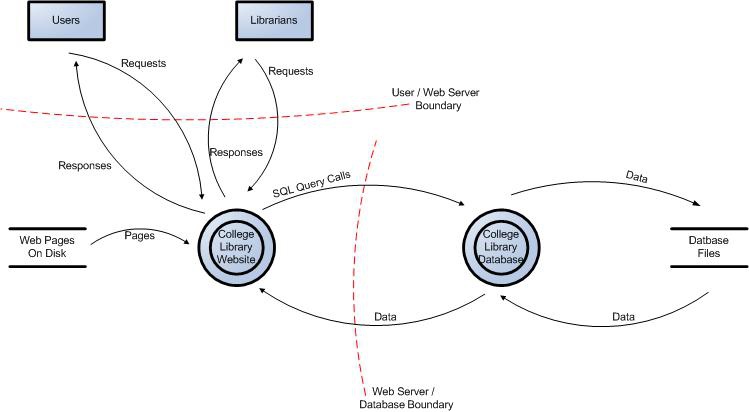
|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Trust Level |
| 1 | File Download | Retrieval of case files by users. | High |
| 2 | Reporting API | Exporting reports for analysis. | Medium |
| 3 | Backup System | Data sent to external backup servers. | Medium |
| 4 | Alerts | Email notifications for updates. | Low |

1. **Assets**

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Trust Level |
| 1 | Case Files | Sensitive legal case documents. | High |
| 2 | User Credentials | Usernames and hashed passwords. | High |
| 3 | Audit Logs | Logs of all system activities. | Medium |
| 4 | Configurations | System and security settings. | High |

1. **Trust Levels**

|  |  |  |
| --- | --- | --- |
| ID | Name | Description |
| 1 | High | Authorized personnel with admin access. |
| 2 | Medium | Regular users with specific access rights. |
| 3 | Low | External systems with limited access. |

****

**STRIDE Framework**

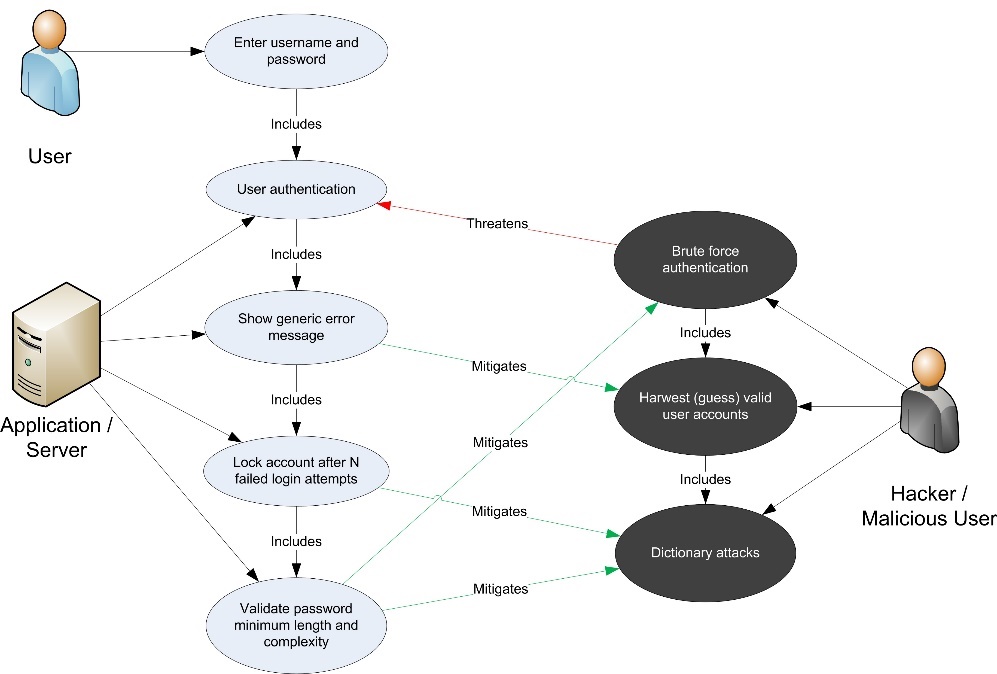
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID |  |  | Threat Type | Threat Description | Security Control |
| 1 |  |  | Spoofing | Impersonation of legitimate users. | Multi-factor authentication. |
| 2 |  |  | Tampering | Unauthorized modification of case files. | File integrity monitoring. |
| 3 |  |  | Repudiation | Denying actions taken within the system. | Comprehensive audit logs. |
| 4 |  |  | Information Disclosure | Unauthorized access to sensitive data. | Data encryption and access control. |
| 5 |  |  | Denial of Service | Overloading the system to cause unavailability. | Rate limiting and load balancing. |
| 6 |  |  | Elevation of Privileges | Unauthorized access to admin functionalities. | Role-based access control. |

**Threat Analysis**

* **Attack Trees**

Detail the possible attack paths for each identified threat.

* **Misuse Cases**



Example misuse cases to identify vulnerabilities:

* An insider leaks case information.
* A hacker modifies case data for malicious purposes.
* **Threat Description Table**

|  |  |  |
| --- | --- | --- |
| Threat ID | Threat Description | Threat Type |
| 1 | Unauthorized user access. | Spoofing |
| 2 | Data modification by attackers. | Tampering |
| 3 | Leakage of sensitive information. | Information Disclosure |
| 4 | Service outage due to attack. | Denial of Service |

1. **Rankings**

* **Delphi Ranking**

Assign threat rankings using consensus.

* **Average Ranking**

Calculate the average ranks from team inputs.

* **Probability x Impact Ranking**

Evaluate risk scores based on threat probability and impact severity.

1. **Fix**

|  |  |  |
| --- | --- | --- |
| Threat ID | Threat Description | Mitigation Measures |
| T#001 | Spoofing threats | Implement strong authentication mechanisms. |
| T#002 | Tampering with case files | Use digital signatures to verify data. |
| T#003 | Information disclosure | Encrypt all sensitive data in transit and at rest. |

1. **Verify**
2. **Review Documentation:** Ensure all identified threats and mitigations are thoroughly documented.
3. **Test Cases:** Create scenarios to test the effectiveness of controls.
4. **Validation:** Verify the implemented safeguards against real-world attack simulations.