Republic of Yemen
Ministry of Higher Education & Scientific Research
AL-Rasheed Private University
Computer Science & Information Technology

Secure Software Engineering

Lab04: Threat Modeling

Mohammed Alqmase

12/18/2024

SUBSYSTEM NAME: ***Administrative Tools Subsystem in a Judicial Management System***

GROUP NAMES:

1. *Mohammed Qasabah*
2. *Mazen Al-ammari*
3. *Mohanned Shaaf*
4. *Mohammed Al-howshabi*

Table of Contents

Threat Model

In this document, we will provide a threat modeling about [YOUR SUBSYSTEM].

1 Scope

In this section, we will…..

1.1 Information

Application Name	Judicial Management Administrative Tools
Application Version	1.0
Description	A subsystem designed for managing and administering judicial case information, user roles, and system settings.
Document Owner	Mohammed
Participants	1. Development Team 2. Security Team 3. System Administrators
Reviewer	Mohammed

1.2 Dependencies

ID	External Dependencies Description
1	**Database Management System (DBMS)**: The subsystem relies on a relational database for storing case data and user information.
2	**Authentication Service**: An external service responsible for user authentication, providing secure login capabilities.
3	**Logging Framework**: A library used for logging actions and errors within the application, ensuring that all activities are recorded.
4	**Email Notification Service**: An external service used to send alerts and notifications to users regarding system events and updates.

1.3 Entry Points

ID	Name	Description	Trust levels
1	**Web Interface**	The primary interface for user interaction with the system.	Medium (User-initiated actions)
2	**API Endpoints**	RESTful APIs for programmatic access to system functionalities.	Medium (Requires authentication)

3	**Database Connection**	Connection established by the application to interact with the database.	High (Internal system access)
4	**File Upload Interface**	Allows users to upload documents related to cases.	Low (Potential for malicious file uploads)

1.4 Exit Points

ID	Name	Description	Trust levels
1	**Data Export Functionality**	Allows users to export case data in various formats (e.g., CSV, PDF).	Medium (Authorized users only)
2	**Email Notifications**	Automated emails sent to users regarding updates and alerts.	Medium (Sensitive information shared)
3	**Audit Logs**	Logs that can be accessed by administrators for review.	High (Sensitive internal data)
4	**User Interface Feedback**	Feedback messages displayed to users after actions (e.g., success/error messages).	Low (General information)

1.5 Assets

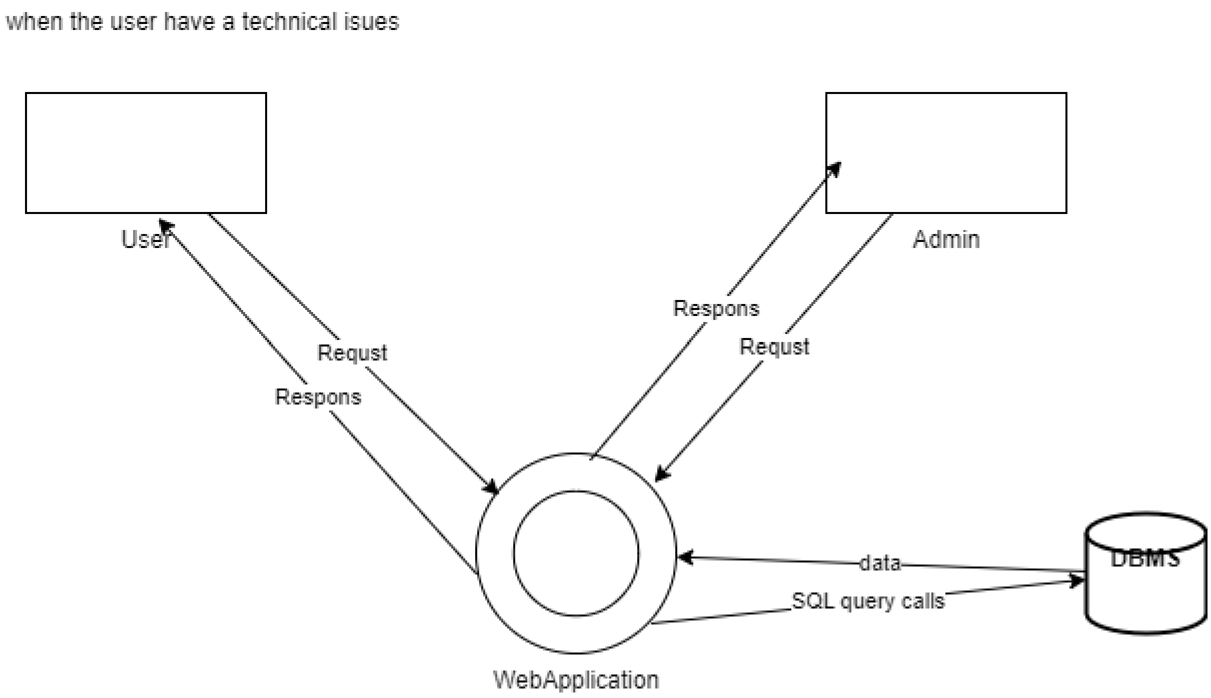
ID	Name	Description	Trust levels
1	**User Data**	Personal and sensitive information of users (e.g., names, emails).	High (Confidential)
2	**Case Information**	Detailed records of judicial cases, including sensitive details.	High (Confidential)
3	**System Configuration**	Settings and configurations that dictate system behavior.	High (Critical for operation)

4	**Audit Trails**	Historical logs of user actions and system changes.	Medium (Sensitive but necessary for accountability)

1.6 Trust Levels

ID	Name	Description
1	**High**	Data or access that is critical and must be highly protected (e.g., user data, case information).
2	**Medium**	Data or access that is important but not critical; requires protection (e.g., logs, notifications).
3	**Low**	General information that is publicly accessible or less sensitive (e.g., feedback messages).
4	**Internal**	Access limited to internal system processes or users only.

1.7 Data Flow Diagrams


when the user have a technical isues
User
Admin
Requst
Respons
Respons
Requst
WebApplication
data
SQL query calls
DBMS

2 Break

In this section, we will…..

2.1 STRIDE Framework

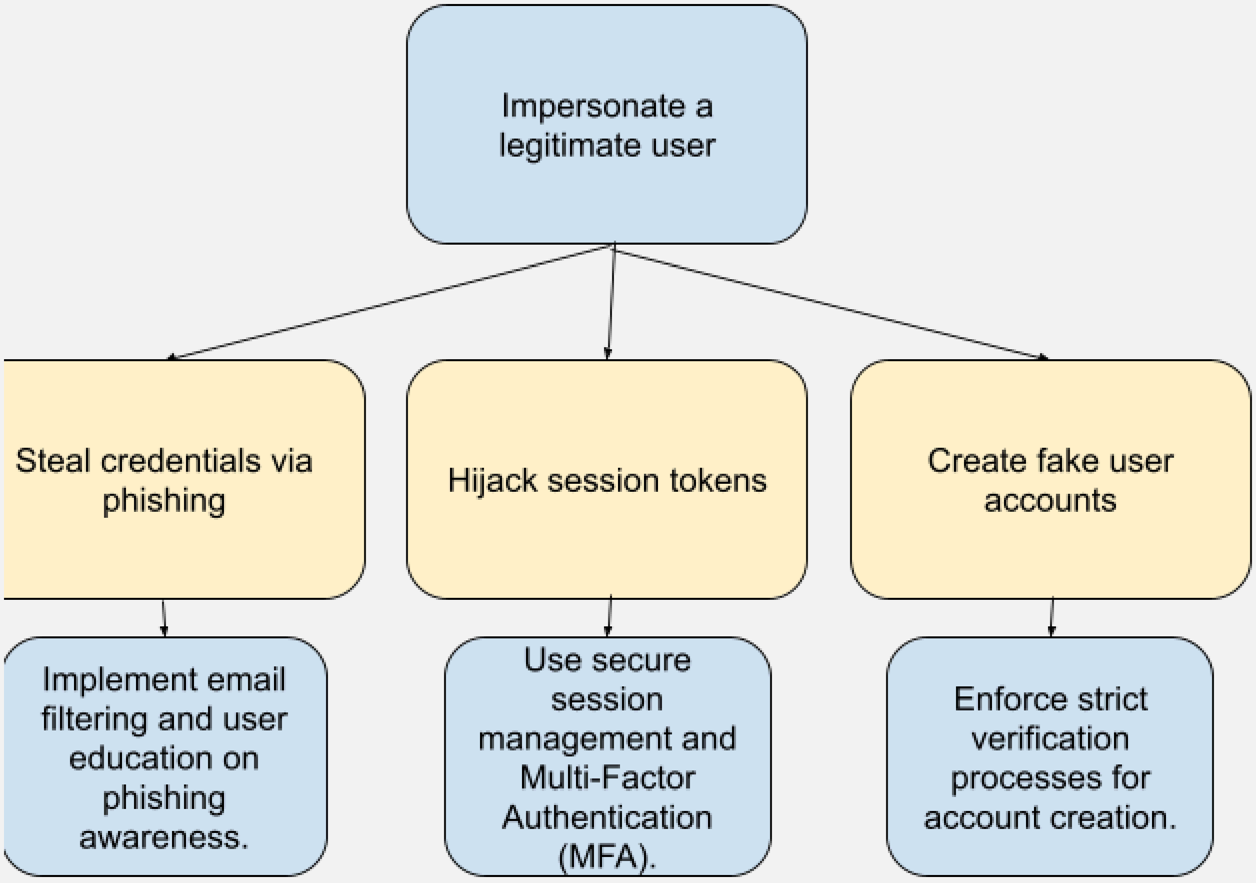
ID	Threats types	threats Description	Security control types
1	Spoofing	1. Attacker may be able to hijack a session token to take over an authenticated session. 2. Attacker may be able to create fake accounts to bypass user verification.	Authentication
2	Tampering	1. Attacker may be able to upload malicious files to compromise the system. 2. Attacker may be able to change system configurations to introduce vulnerabilities.	Integrity
3	Repudiation	1. Attacker may be able to dispute notifications due to poor record-keeping. 2. Attacker may be able to alter logs to erase evidence of unauthorized actions.	Non- Repudiation
4	Information Disclosure	1. Attacker may be able to access unsecured API endpoints exposing sensitive information. 2. Attacker may be able to intercept unencrypted data transmitted over the network.	Confidentiality
5	Denial of Service	1. Attacker may be able to launch a DDoS attack to overwhelm the application and disrupt access. 2. Attacker may be able to exploit vulnerabilities to exhaust server resources.	Availability
6	Elevation of Privileges	1. Attacker may be able to gain excessive permissions due to misconfigurations.	Authorization

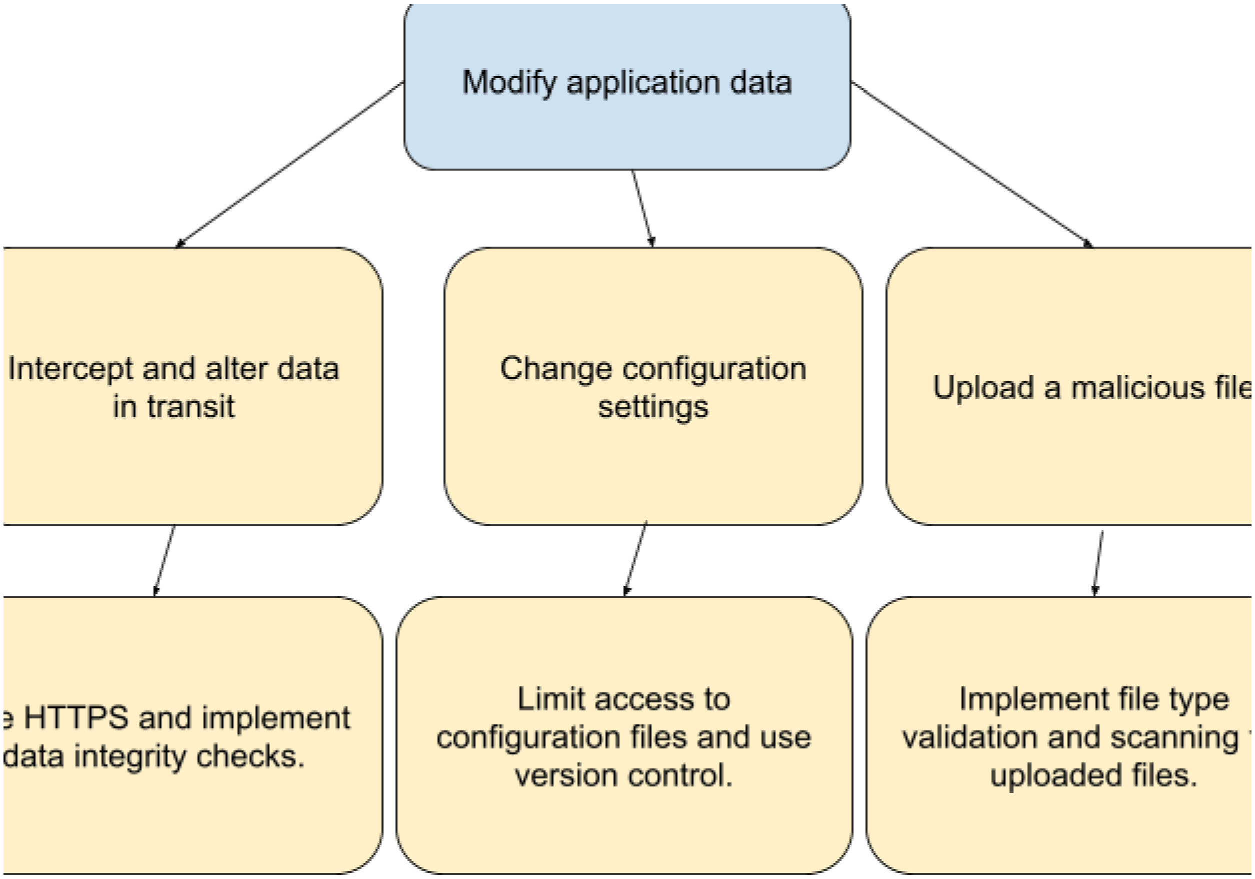
		2. Attacker may be able to misuse legitimate access to obtain confidential information.	

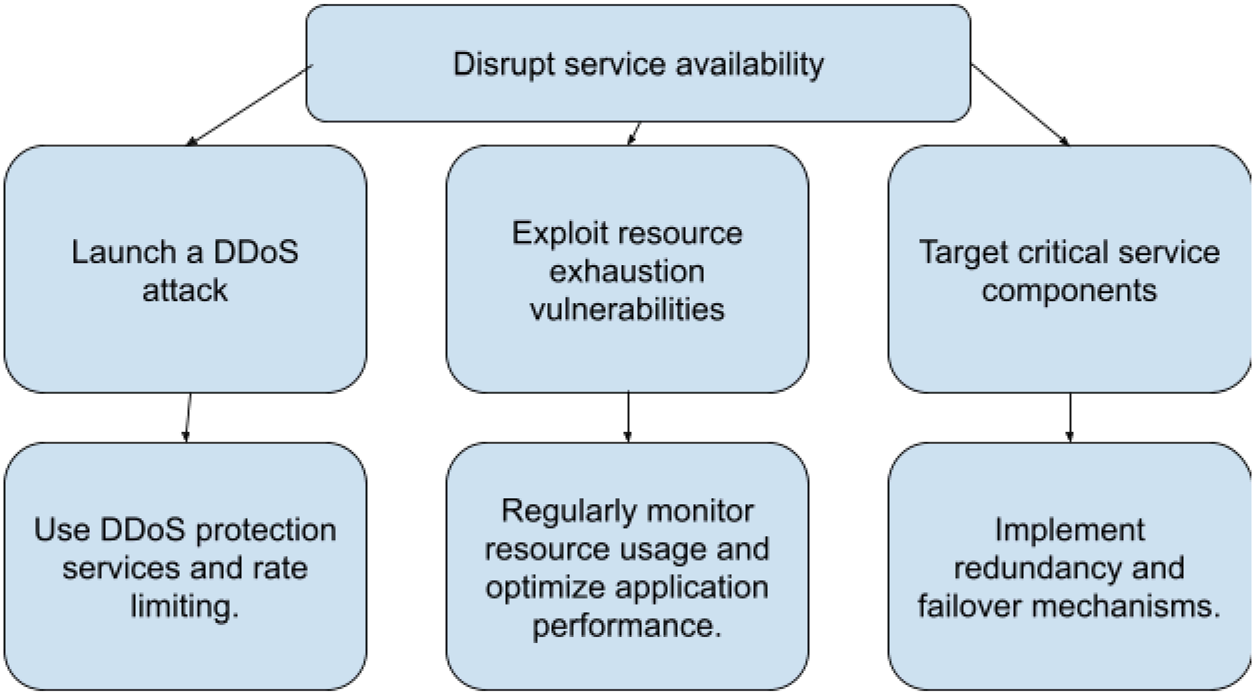
2.2 Threat Analysis

In this section, we will…..

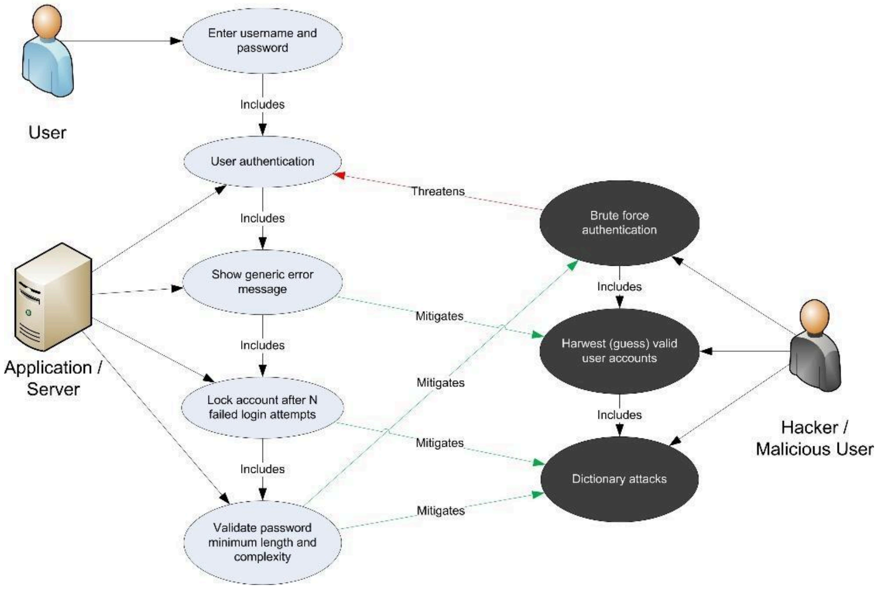
1.1.1 Attack Trees


Impersonate a legitimate user
Steal credentials via phishing
Hijack session tokens
Create fake user accounts
Implement email filtering and user education on phishing awareness.
Use secure session management and Multi-Factor Authentication (MFA).
Enforce strict verification processes for account creation.


Modify application data
Intercept and alter data in transit
Change configuration settings
Upload a malicious file
e HTTPS and implement data integrity checks.
Limit access to configuration files and use version control.
Implement file type validation and scanning uploaded files.


Disrupt service availability
Launch a DDoS attack
Exploit resource exhaustion vulnerabilities
Target critical service components
Use DDoS protection services and rate limiting.
Regularly monitor resource usage and optimize application performance.
Implement redundancy and failover mechanisms.

1.1.2 Misuse Cases


User
Enter username and password
Includes
User authentication
Includes
Show generic error message
Includes
Lock account after N failed login attempts
Includes
Validate password minimum length and complexity
Application / Server
Threatens
Brute force authentication
Includes
Harwest (guess) valid user accounts
Includes
Dictionary attacks
Mitigates
Mitigates
Mitigates
Mitigates
Hacker / Malicious User

1.1.3 Threat Description Table

Threat ID	Threat Description	Threats Types

1	Attacker may hijack a session token to take over an authenticated session.	Spoofing
2	Attacker may create fake accounts to bypass user verification.	Spoofing
3	Attacker may upload malicious files to compromise the system.	Tampering
4	Attacker may change system configurations to introduce vulnerabilities.	Tampering
5	Attacker may access unsecured API endpoints exposing sensitive information.	Information Disclosure
6	Attacker may launch a DDoS attack to overwhelm the application and disrupt access.	Denial of Service
7	Attacker may exploit vulnerabilities to exhaust server resources.	Denial of Service

2.3 Ranking

In this section, we will…..

1.1.4 Delphi Ranking

Threat ID	Threat Title	Member 1 Rank	Member 2 Rank	Member 3 Rank	Average Rank	Final Consensus Rank	Comments
1	Session Hijacking	2	3	1l	2.0	2	Critical concern
2	Fake Account Creation	3	2	2	2.33	2	Needs monitoring
3	Malicious File Upload	1	2	2	1.67	2	High impact threat
4	Configuration Tampering	3	3	2	2.67	3	Requires quick action
5	Unsecured API Access	2	1	2	1.67	2	Immediate attention needed
6	DDoS Attack	3	2	3	2.67	3	Consider mitigation strategies
7	Resource Exhaustion	2	3	3	2.67	3	Need for monitoring

1.1.5 Average Ranking

Threat ID	Threat Title	D	R	E	A	Average Rank	Risk Levels
1	Session Hijacking	3	3	2	1	2.25	High
2	Fake Account Creation	2	3	2	2	2.25	Medium
3	Malicious File Upload	1	2	3	1	1.75	High
4	Configuration Tampering	3	2	3	3	2.75	Medium
5	Unsecured API Access	1	2	1	1	1.25	High
6	DDoS Attack	4	3	2	3	3.00	Medium
7	Resource Exhaustion	3	2	4	3	3.00	Medium

1.1.6 Probability x Impact (P x I) Ranking

Threat ID	Threat Title	P Probability	I Impact	Risk Score P x I	Rank
1	Session Hijacking	4	5	20	1
2	Fake Account Creation	3	4	12	3
3	Malicious File Upload	5	5	25	1
4	Configuration Tampering	3	3	9	4
5	Unsecured API Access	4	4	16	2
6	DDoS Attack	3	3	9	4
7	Resource Exhaustion	2	4	8	5

3 Fix

In this section, we will…..

Threat ID	T#001
Threat Description	Session hijacking involves an attacker taking over an active session to gain unauthorized access.
Threat targets	User accounts and session tokens.
Attack techniques	Session fixation, credential theft, or cookie theft.
Security Impact	Compromised user data and unauthorized actions on behalf of the user.
Risk	High - potential for significant data breaches and loss of user trust.
Safeguard controls to implement	Implement multi-factor authentication (MFA), use secure cookie attributes, and regularly review session management practices.

Threat ID	T#002
Threat Description	Fake account creation involves unauthorized users creating accounts to exploit system vulnerabilities.
Threat targets	User registration processes and account management.
Attack techniques	Social engineering, automated bots, or phishing.
Security Impact	Erosion of trust in the system and potential data leaks.

Risk	Medium - could lead to fraud and misuse of resources.
Safeguard controls to implement	Implement CAPTCHA, email verification, and monitor for suspicious registration patterns.

Threat ID	T#003
Threat Description	Malicious file upload refers to the process of uploading harmful files to the system.
Threat targets	File upload functionalities and storage systems.
Attack techniques	Exploiting file type restrictions or using executable files.
Security Impact	System compromise and potential data loss or corruption.
Risk	High - can lead to severe security incidents.
Safeguard controls to implement	validate file types, implement file size limits, and scan uploads for malware.

4 Verify

In this section, we will…..

4.1 Review Documentation

Search and complete this at home

4.2 Test cases

Search and complete this at home

4.3 Validation

Search and complete this at home