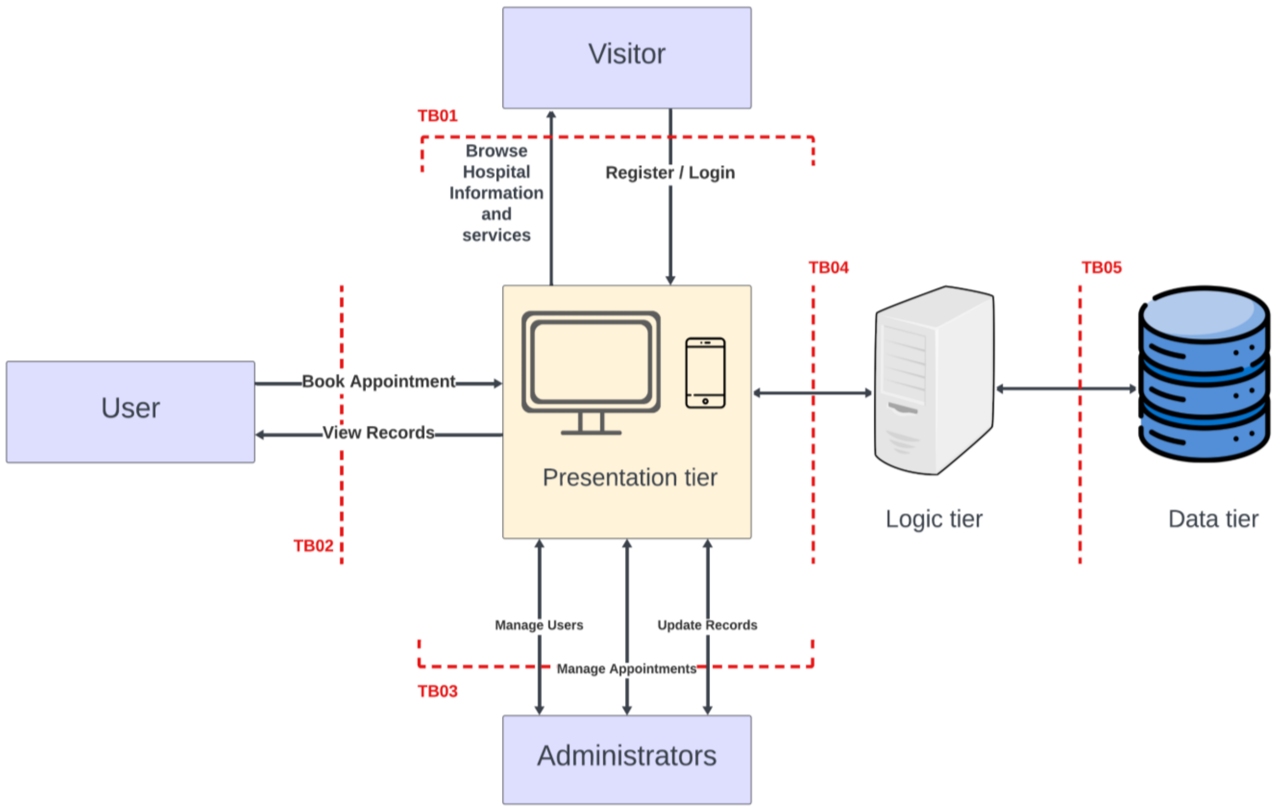
STRIDE Threat List		
Type	**Description**	**Security Control**
Spoofing	Threat action aimed at accessing and use of another user’s credentials, such as username and password.	Authentication
Tampering	Threat action intending to maliciously change or modify persistent data, such as records in a database, and the alteration of data in transit between two computers over an open network, such as the Internet.	Integrity
Repudiation	Threat action aimed at performing prohibited operations in a system that lacks the ability to trace the operations.	Non-Repudiation
Information disclosure	Threat action intending to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of service	Threat action attempting to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privilege	Threat action intending to gain privileged access to resources in order to gain unauthorized access to information or to compromise a system.	Authorization

Definition: Microsoft developed approach to quantitively assess and prioritize cyber threats

DREAD Threat List		
Category	Description	Ratings
Damage	The impact that a threat can cause	0: No damage 5: Information disclosure 8: Non-sensitive user data related to individuals or employer compromised 9: Non-sensitive administrative data compromised 10: Destruction of an information system; data or application unavailability
Reproducibility	How Easily the Attack can be Reproduced	0: Difficult or impossible 5: Complex 7.5: Easy 10: Very easy
Exploitability	How Easy it is to Launch the Attack	2.5: Advanced programming and networking skills 5: Available attack tools 9: Web application proxies 10: Web browser
Affected Users	How many users will be impacted	0: No users 2.5: Individual user 6: Few users 8: Administrative users 10: All users
Discoverability	How easily the Vulnerability can be found	0: Hard to discover the vulnerability 5: HTTP requests can uncover the vulnerability 8: Vulnerability found in the public domain 10: Vulnerability found in web address bar or form

Overall Threat Rating Categories	
Critical (40–50)	Critical vulnerability; address immediately.
High (25–39)	Severe vulnerability; consider for review and resolution soon.
Medium (11–24)	Moderate risk; review after addressing severe and critical risks.
Low (1–10)	Low risk to infrastructure and data.

Data Flow Diagram - Level 0



TB01	External Visitors	
	Strengths	**Weaknesses**
Spoofing	TLS/SSL Certificate that encrypt all communications between Clients and the Server	HSTS misconfigured on Web Server Use of weak or deprecated Encryption Algorithms /Ciphers
Tampering	Input validation applied on the all inputs	Not using SQL Parameterized Queries
Repudiation		
Information disclosure		Error messages not handled
Denial of service		
Elevation of privilege		

TB03	Administrators	
	Strengths	**Weaknesses**
Spoofing	Proper Authentication (Username & Password) Password Complexity Applied	No 2FA default/common passwords not checked Session token cookies missed (httpOnly and Secure) flags
Tampering	Input Validation is applied	Not using SQL Parameterized Queries
Repudiation	Proper logging of user actions	
Information disclosure	Path traversal is handled	Error messages not handled
Denial of service	Account Lockout policy applied	No Captcha to prevent anti-automation File upload size is not handled
Elevation of privilege	user session token never sent in the URLs Proper Access Control	Session token cookies missed (httpOnly and Secure) flags

Threat	Damage	Reproducibility	Exploitability	Affected Users	Descoverability	Threat Score	Threat Severity	Recommendations	Status
Lack of Input Validation: Increased risk of injection attacks and malicious input exploitation.	8	10	9	8	10	45	Critical	Implement strict input validation across all inputs. Use whitelisting approaches and sanitize inputs.	Closed
Absence of Two-Factor Authentication for Admins: Elevated risk of unauthorized admin access if credentials are compromised.	9	5	9	8	10	41	Critical	Implement MFA for all admin accounts to enhance security.	Open
Session Tokens Sent in URLs: Increased risk of session hijacking through exposed tokens in browser history or logs.	8	7.5	5	8	10	38.5	High	Avoid sending session tokens in URLs; use HTTP headers or cookies instead.	Closed
Insufficient Password Complexity: Increased likelihood of brute-force attacks due to easily guessable passwords.	8	5	5	8	10	36	High	Enforce password complexity requirements and educate users on creating strong passwords.	Open
Failure to Use SQL Parameterized Queries: Susceptibility to SQL injection attacks, leading to data breaches.	9	5	9	8	5	36	High	Always use parameterized queries or prepared statements to prevent SQL injection attacks.	Open
Path Traversal Vulnerabilities: Risk of unauthorized access to restricted directories and files on the server.	8	5	5	8	10	36	High	Validate and sanitize file paths, and restrict access to sensitive directories.	Closed
No Account Lockout Policy: Increased risk of account takeover through repeated login attempts without restrictions.	8	5	5	8	10	36	High	Implement an account lockout policy after a specified number of failed login attempts.	Closed
Poor Access Control Mechanisms: Unauthorized access to sensitive resources due to inadequate permissions and restrictions.	9	7.5	5	8	5	34.5	High	Implement role-based access control (RBAC) and regularly review permissions.	Closed
Absence of CAPTCHA: Vulnerability to automated attacks and bots due to lack of anti-automation measures.	5	7.5	5	6	10	33.5	High	Implement CAPTCHA on forms to prevent automated submissions.	Open
Weak or Deprecated Encryption Algorithms: Vulnerability to data interception and decryption, compromising sensitive information.	9	5	5	8	5	32	High	Update encryption standards to use strong, current algorithms. Regularly audit encryption protocols.	open
HSTS Misconfiguration: Potential exposure to man-in-the-middle attacks due to improper HSTS settings.	8	5	5	8	5	31	High	Ensure proper HSTS configuration and enable it for all subdomains. Regularly test for correctUpdate encryption standards to use strong, current algorithms. Regularly audit encryption protocols. implementation	open
Unmanaged Error Messages: Exposure of sensitive system information through detailed error responses, aiding attackers.	5	5	5	6	10	31	High	Standardize error messages to avoid revealing sensitive information. Log detailed errors internally.	Open
Default/Common Passwords Not Checked: Vulnerability to unauthorized accounts due to the use of predictable passwords.	8	5	5	8	5	31	High	Implement checks against common password lists during registration and password changes.	Open
Missing Session Token Cookie Flags: Exposure to session hijacking attacks due to lack of security attributes on cookies.	8	5	5	8	5	31	High	Set `httpOnly` and `Secure` flags on cookies to protect session tokens from theft.	Open
Inadequate Logging of User Actions: Difficulty in detecting and responding to suspicious activities due to poor audit trails.	5	5	5	2.5	5	22.5	Medium	Implement comprehensive logging of user actions and establish alerts for suspicious activities.	Closed