Application Threat Modeling Example

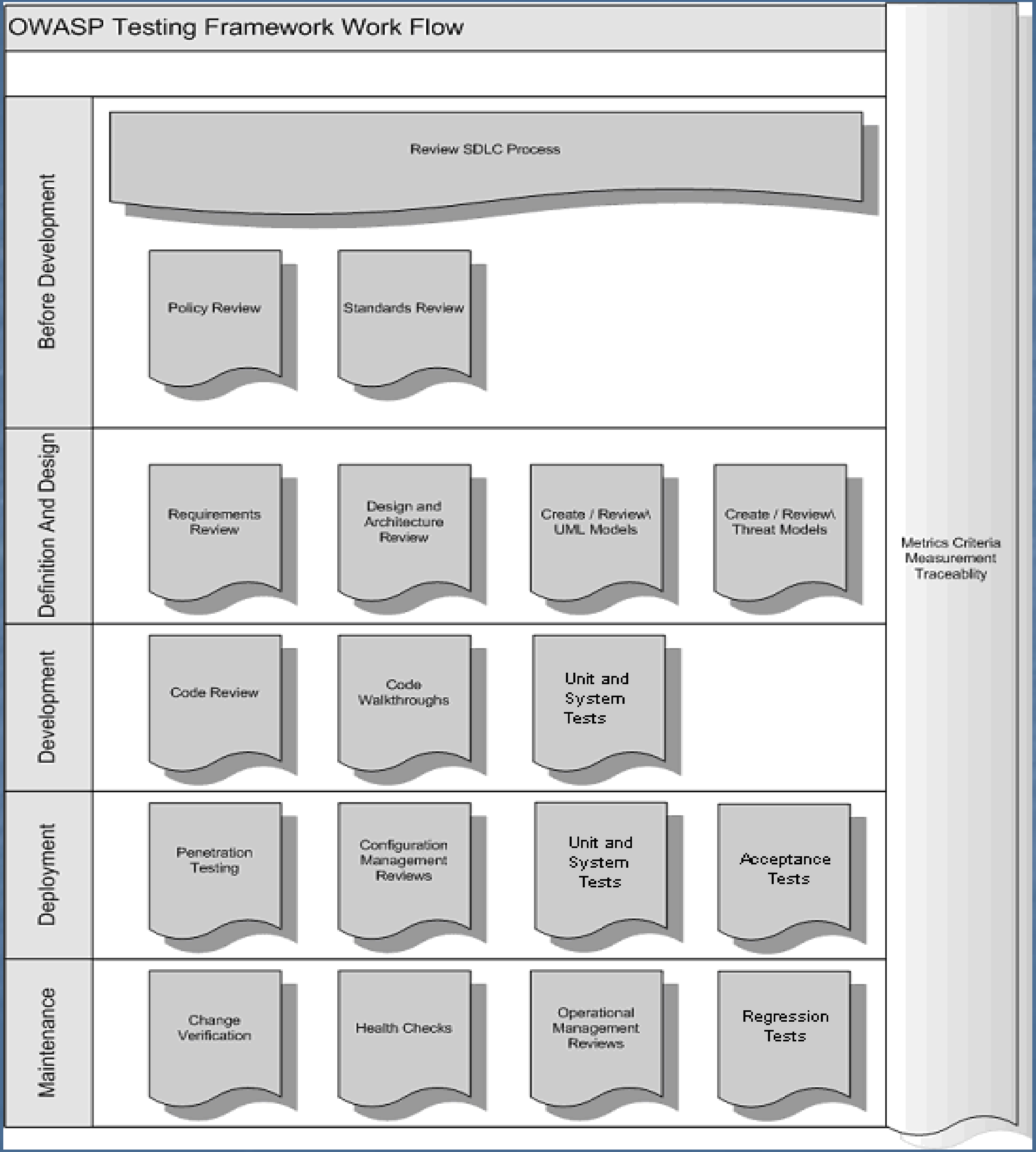
Τμήμα Πληροφορικής

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΙΡΑΙΩΣ

Threat Modeling Goals

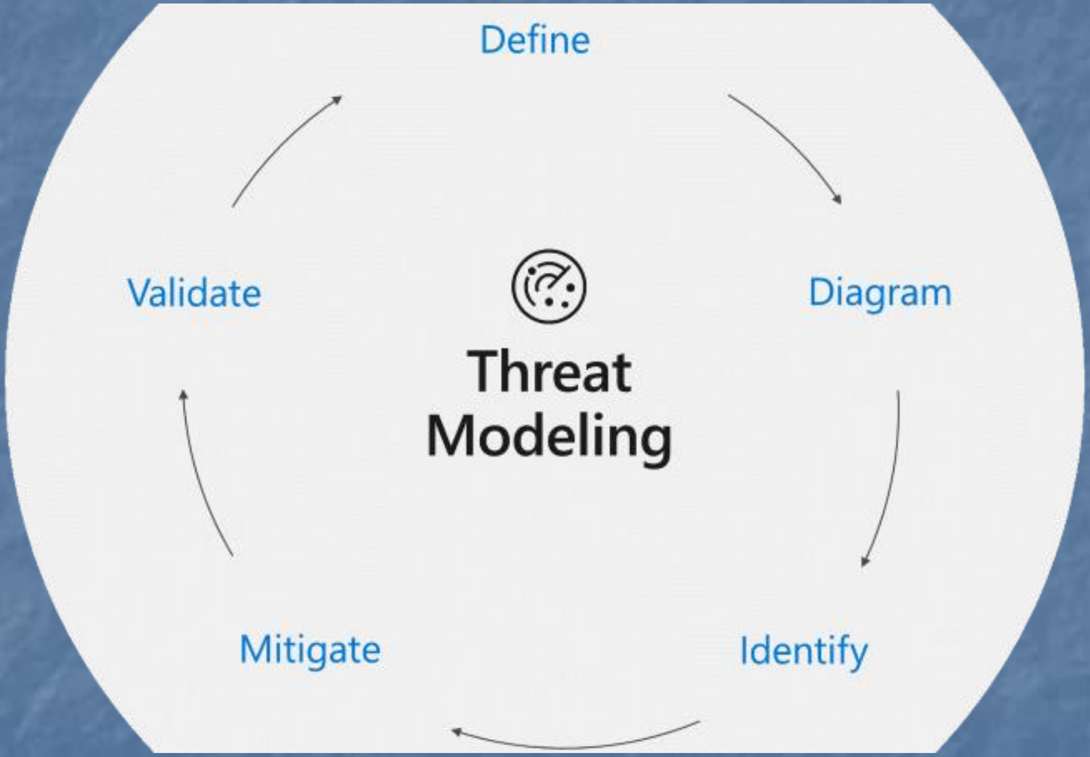
- To perform Application Threat Modeling use testing methodologies/techniques/frameworks/methods (e.g. OWASP testing framework) to identify, STRIDE methodology to Classify and DREAD methodology to rate, compare and prioritize risks, based on severity.

Software Development Life Cycle (SDLC) Testing Workflow



Microsoft Security Development Lifecycle (SDL)

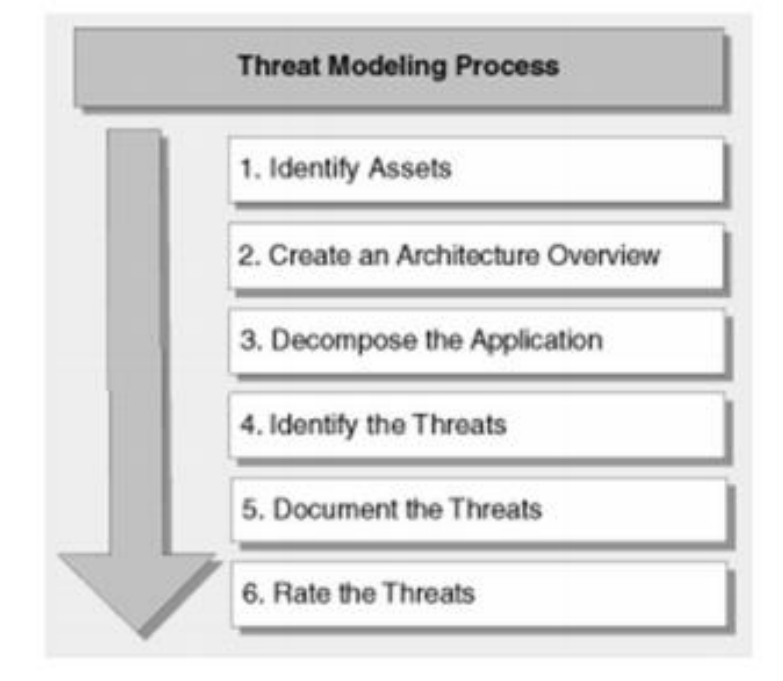
- Defining security requirements.
- Creating an application diagram.
- Identifying threats.
- Mitigating threats.
- Validating that threats have been mitigated.



Microsoft threat modeling tool

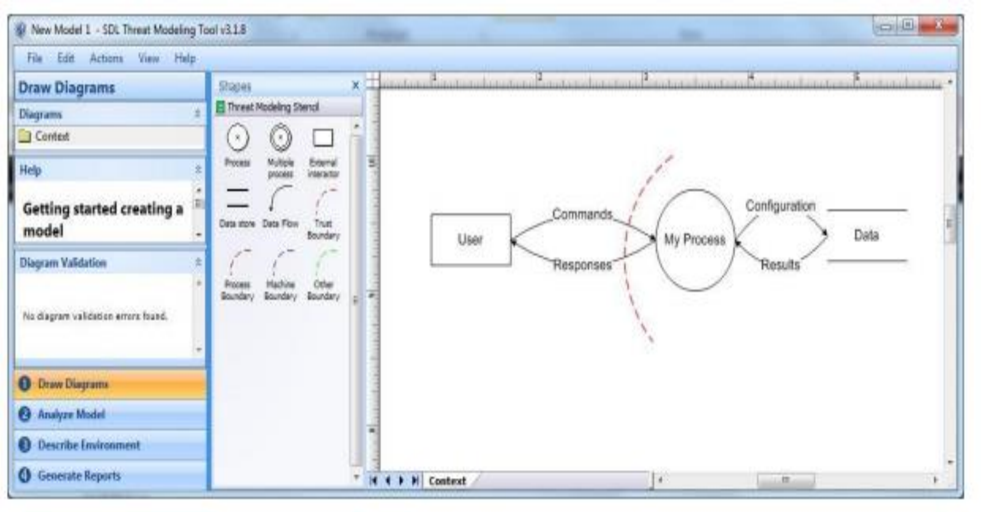
- STRIDE Model
- 1. Spoofing – attackers pretend to be someone or something they are not
- 2. Tampering – attackers change data in transit or in a data store
- 3. Repudiation – attackers perform actions that cannot be traced
- 4. Information disclosure – attackers gain access to data in transit or in data store that they shouldn’t have access to
- 5. Denial of service – attackers interrupt normal operation of the system
- 6. Elevation of privilege – attackers perform actions they are not authorized to perform

MICROSOFT THREAT MODELING PROCESS



Threat Modeling Process

1. Identify Assets
2. Create an Architecture Overview
3. Decompose the Application
4. Identify the Threats
5. Document the Threats
6. Rate the Threats



Getting started creating a model

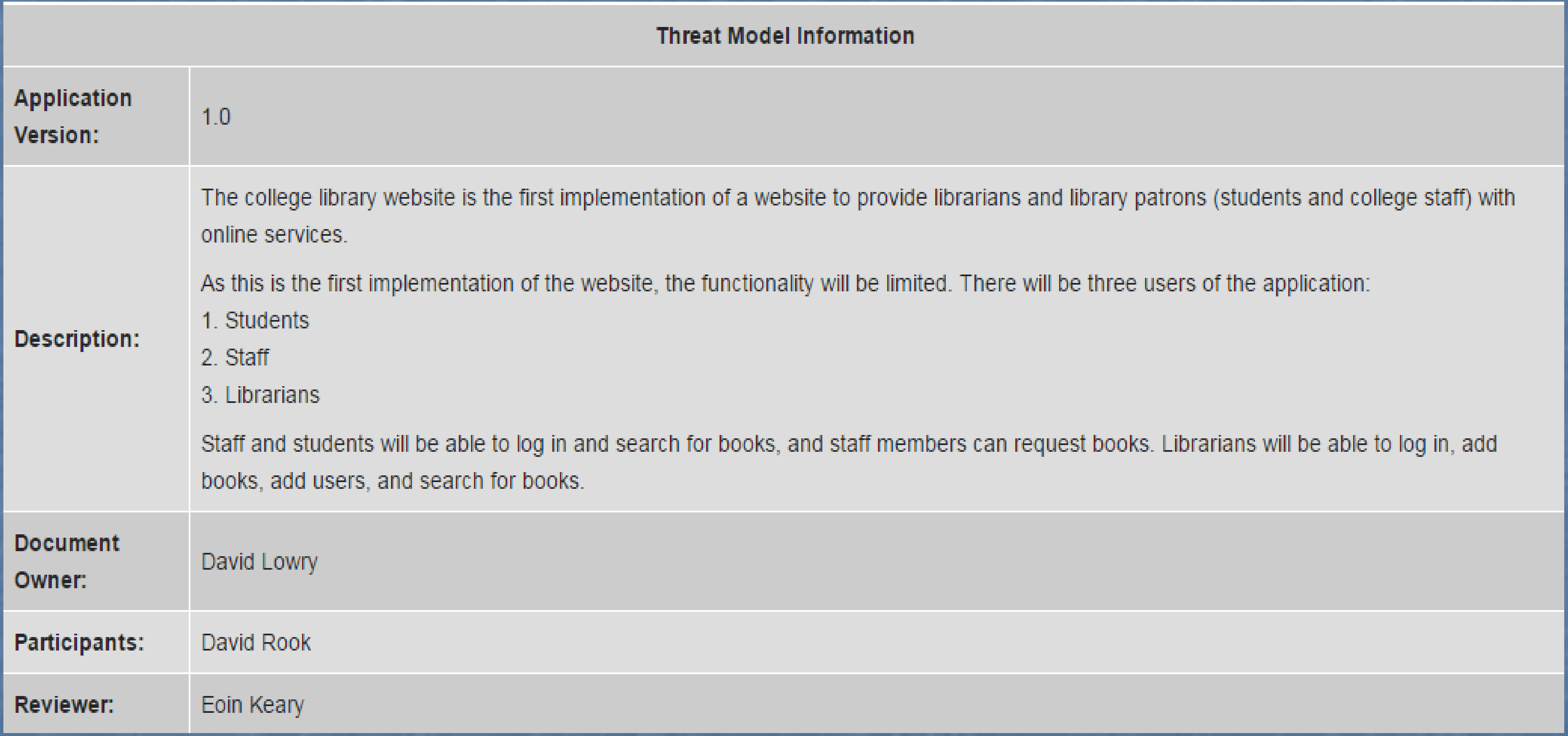
No diagram validation errors found.

DREAD model

- 1. Damage potential – Ranks the extent of damage that occurs if a vulnerability is exploited
- 2. Reproducibility – Ranks how often an attempt at exploiting a vulnerability really works
- 3. Exploitability – Assigns a number to the effort required to exploit the vulnerability. This also considers the preconditions such as whether the user must be authenticated
- 4. Affected users – A value characterizing the number of installed instances of the system that would be affected if an exploit became widely available
- 5. Discoverability – Measures the likelihood that, if unpatched, a vulnerability will be found by external security researchers, hackers, etc

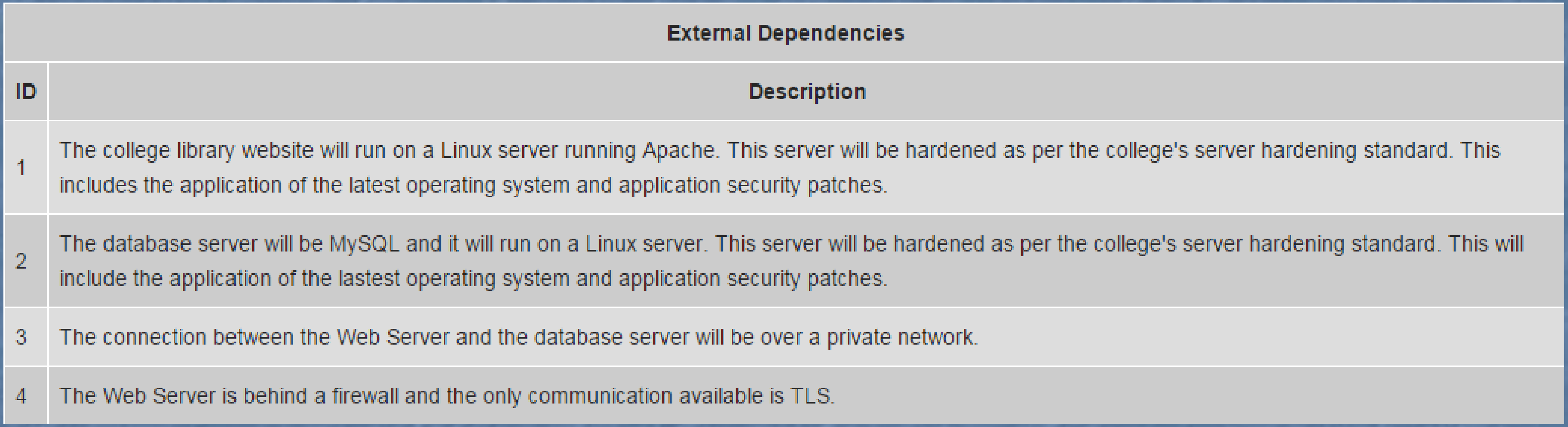
$$Risk\_DREAD = \frac{\text{Damage} + \text{Reproducibility} + \text{Exploitability} + \text{Affected Users} + \text{Discoverability}}{5}$$

Decompose the Application



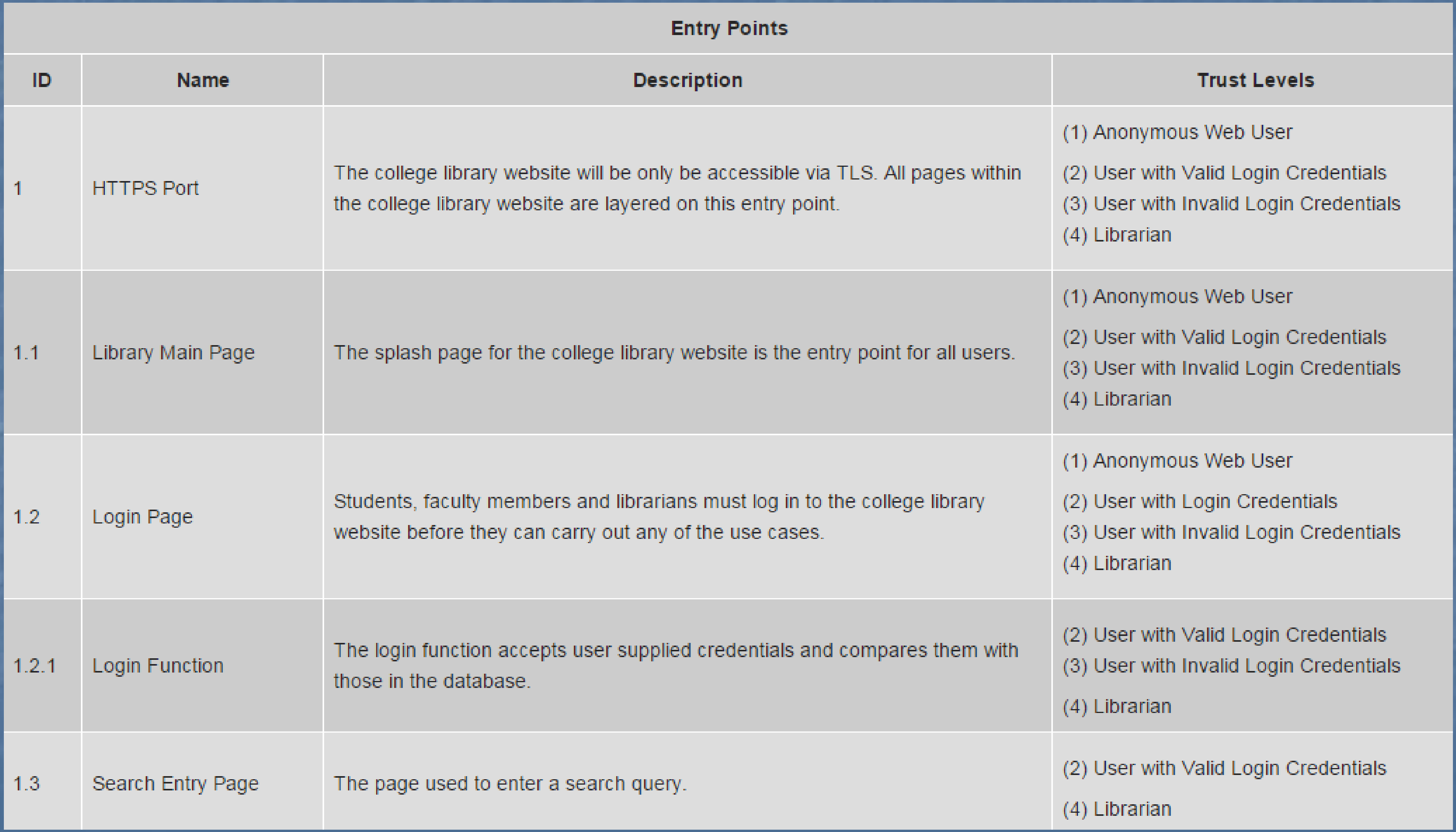
Threat Model Information	
Application Version:	1.0
Description:	The college library website is the first implementation of a website to provide librarians and library patrons (students and college staff) with online services. As this is the first implementation of the website, the functionality will be limited. There will be three users of the application: 1. Students 2. Staff 3. Librarians Staff and students will be able to log in and search for books, and staff members can request books. Librarians will be able to log in, add books, add users, and search for books.
Document Owner:	David Lowry
Participants:	David Rook
Reviewer:	Eoin Keary

External Dependencies



External Dependencies	
ID	Description
1	The college library website will run on a Linux server running Apache. This server will be hardened as per the college's server hardening standard. This includes the application of the latest operating system and application security patches.
2	The database server will be MySQL and it will run on a Linux server. This server will be hardened as per the college's server hardening standard. This will include the application of the lastest operating system and application security patches.
3	The connection between the Web Server and the database server will be over a private network.
4	The Web Server is behind a firewall and the only communication available is TLS.

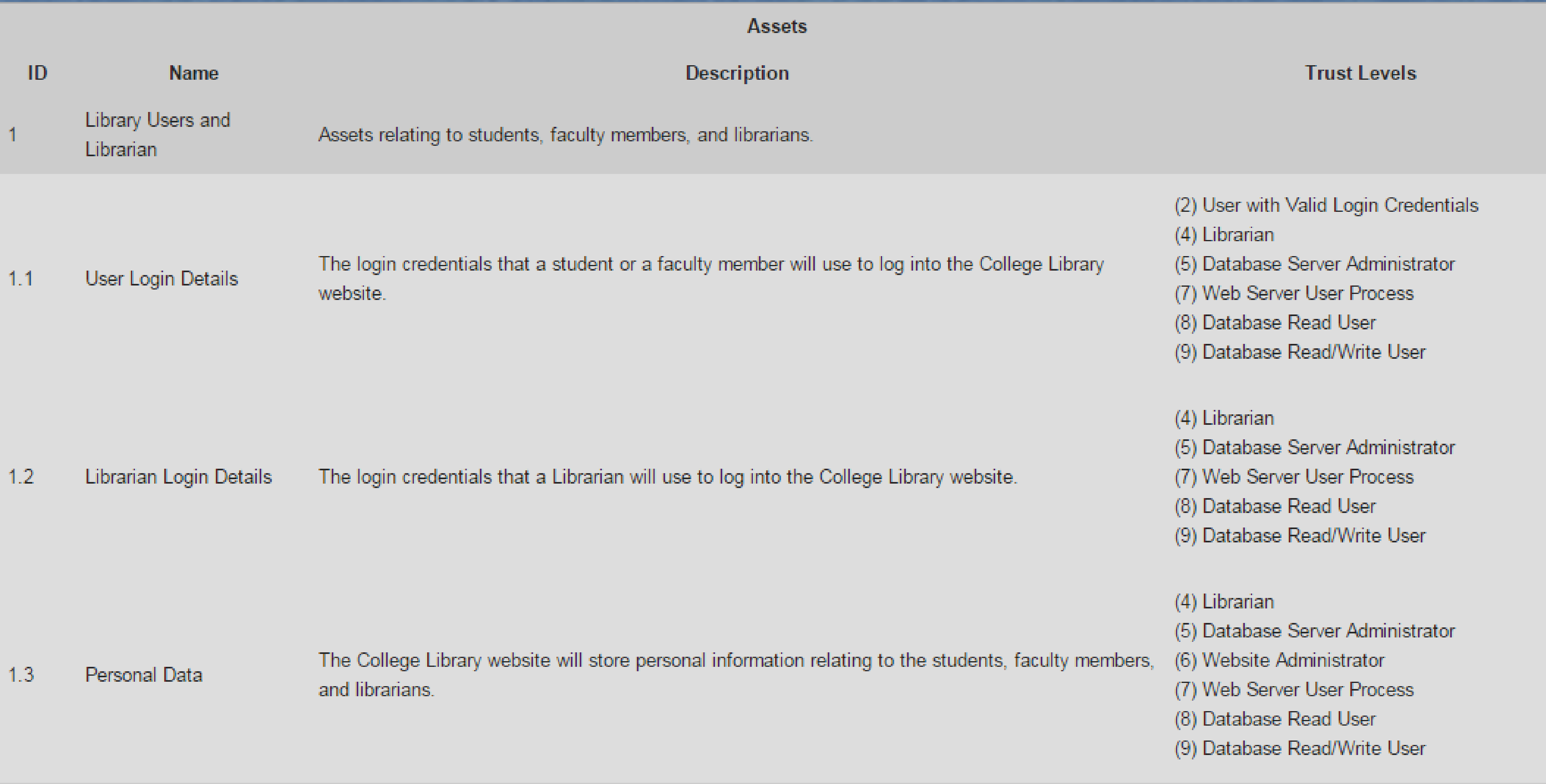
Entry Points



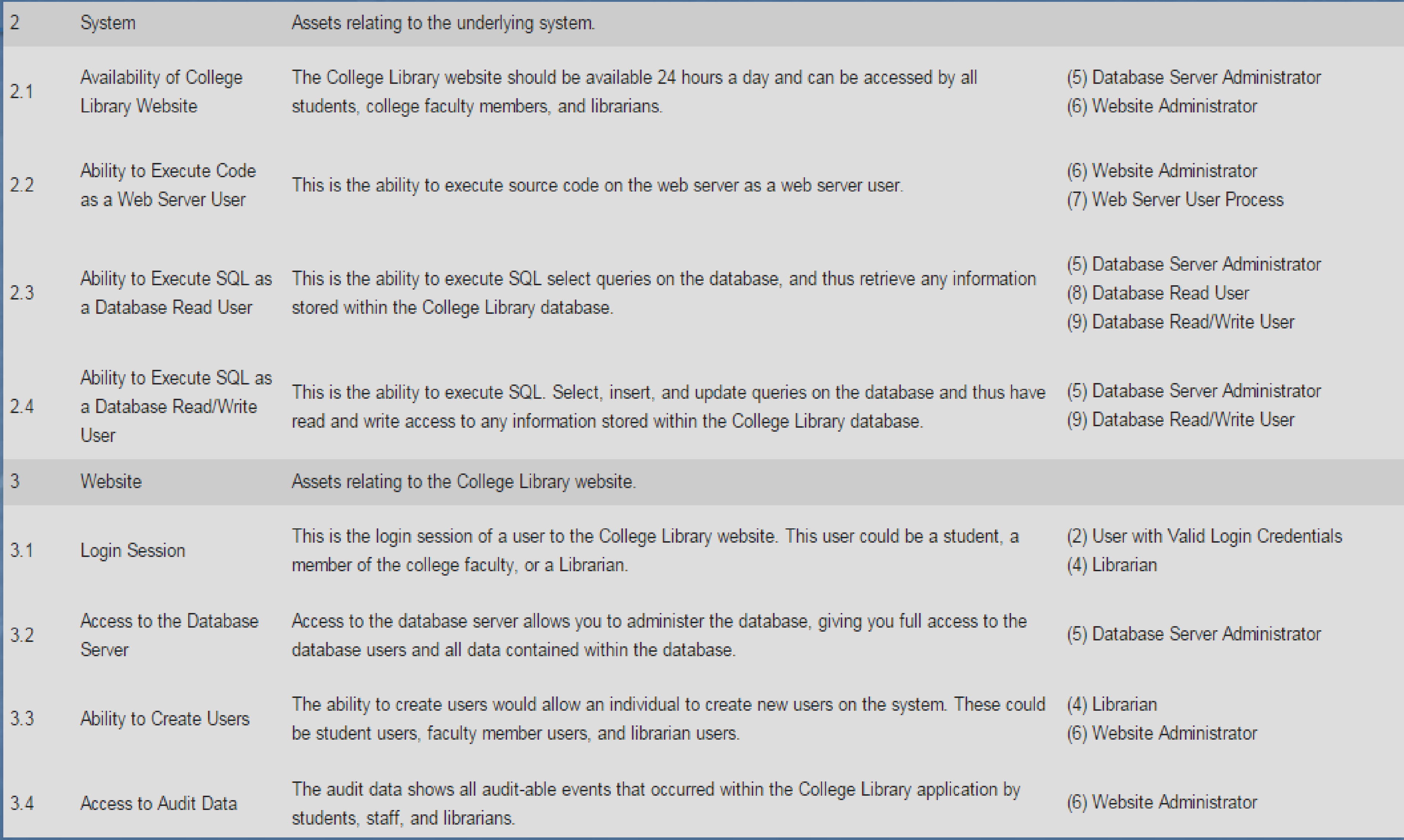
Entry Points

ID	Name	Description	Trust Levels
1	HTTPS Port	The college library website will be only be accessible via TLS. All pages within the college library website are layered on this entry point.	(1) Anonymous Web User (2) User with Valid Login Credentials (3) User with Invalid Login Credentials (4) Librarian
1.1	Library Main Page	The splash page for the college library website is the entry point for all users.	(1) Anonymous Web User (2) User with Valid Login Credentials (3) User with Invalid Login Credentials (4) Librarian
1.2	Login Page	Students, faculty members and librarians must log in to the college library website before they can carry out any of the use cases.	(1) Anonymous Web User (2) User with Login Credentials (3) User with Invalid Login Credentials (4) Librarian
1.2.1	Login Function	The login function accepts user supplied credentials and compares them with those in the database.	(2) User with Valid Login Credentials (3) User with Invalid Login Credentials (4) Librarian
1.3	Search Entry Page	The page used to enter a search query.	(2) User with Valid Login Credentials (4) Librarian

Assets

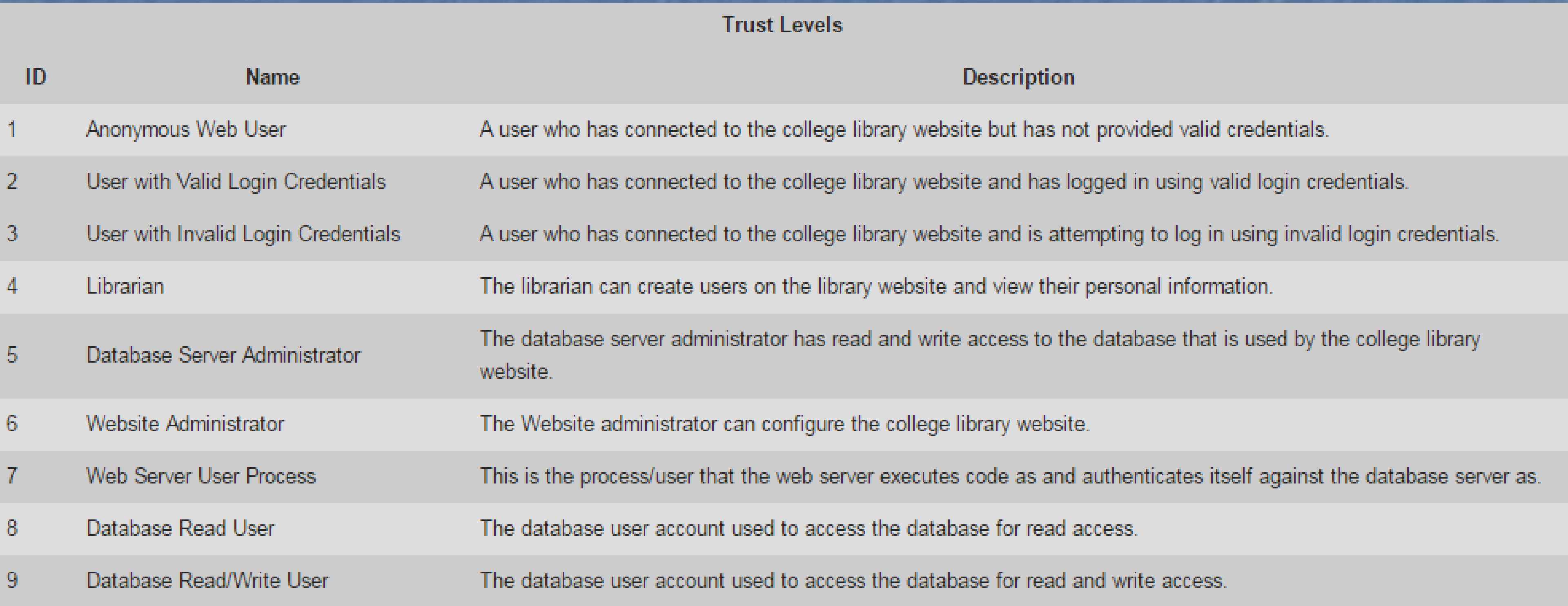


Assets			
ID	Name	Description	Trust Levels
1	Library Users and Librarian	Assets relating to students, faculty members, and librarians.	
1.1	User Login Details	The login credentials that a student or a faculty member will use to log into the College Library website.	(2) User with Valid Login Credentials (4) Librarian (5) Database Server Administrator (7) Web Server User Process (8) Database Read User (9) Database Read/Write User
1.2	Librarian Login Details	The login credentials that a Librarian will use to log into the College Library website.	(4) Librarian (5) Database Server Administrator (7) Web Server User Process (8) Database Read User (9) Database Read/Write User
1.3	Personal Data	The College Library website will store personal information relating to the students, faculty members, and librarians.	(4) Librarian (5) Database Server Administrator (6) Website Administrator (7) Web Server User Process (8) Database Read User (9) Database Read/Write User



2	System	Assets relating to the underlying system.	
2.1	Availability of College Library Website	The College Library website should be available 24 hours a day and can be accessed by all students, college faculty members, and librarians.	(5) Database Server Administrator (6) Website Administrator
2.2	Ability to Execute Code as a Web Server User	This is the ability to execute source code on the web server as a web server user.	(6) Website Administrator (7) Web Server User Process
2.3	Ability to Execute SQL as a Database Read User	This is the ability to execute SQL select queries on the database, and thus retrieve any information stored within the College Library database.	(5) Database Server Administrator (8) Database Read User (9) Database Read/Write User
2.4	Ability to Execute SQL as a Database Read/Write User	This is the ability to execute SQL. Select, insert, and update queries on the database and thus have read and write access to any information stored within the College Library database.	(5) Database Server Administrator (9) Database Read/Write User
3	Website	Assets relating to the College Library website.	
3.1	Login Session	This is the login session of a user to the College Library website. This user could be a student, a member of the college faculty, or a Librarian.	(2) User with Valid Login Credentials (4) Librarian
3.2	Access to the Database Server	Access to the database server allows you to administer the database, giving you full access to the database users and all data contained within the database.	(5) Database Server Administrator
3.3	Ability to Create Users	The ability to create users would allow an individual to create new users on the system. These could be student users, faculty member users, and librarian users.	(4) Librarian (6) Website Administrator
3.4	Access to Audit Data	The audit data shows all audit-able events that occurred within the College Library application by students, staff, and librarians.	(6) Website Administrator

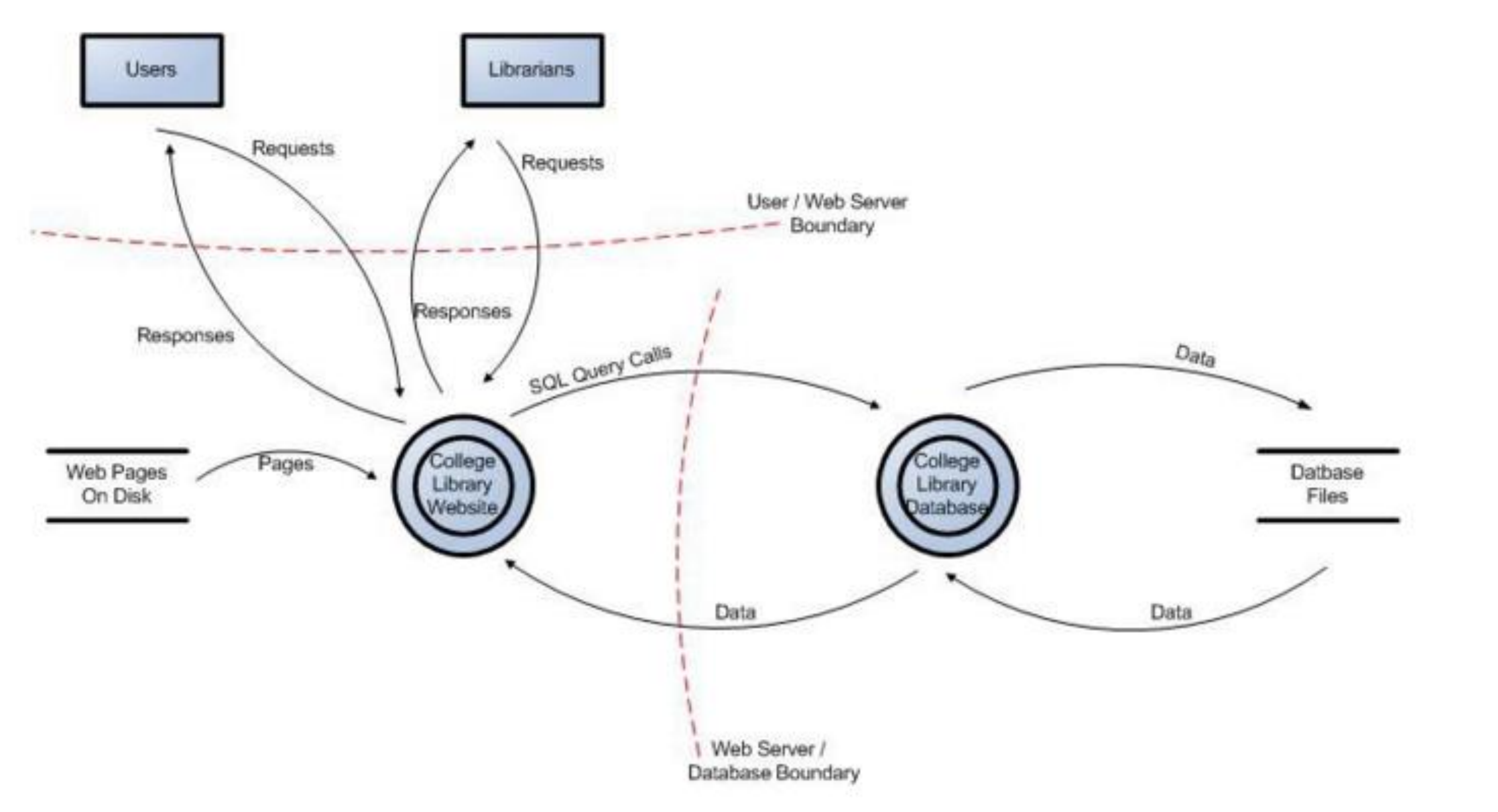
Trust Levels



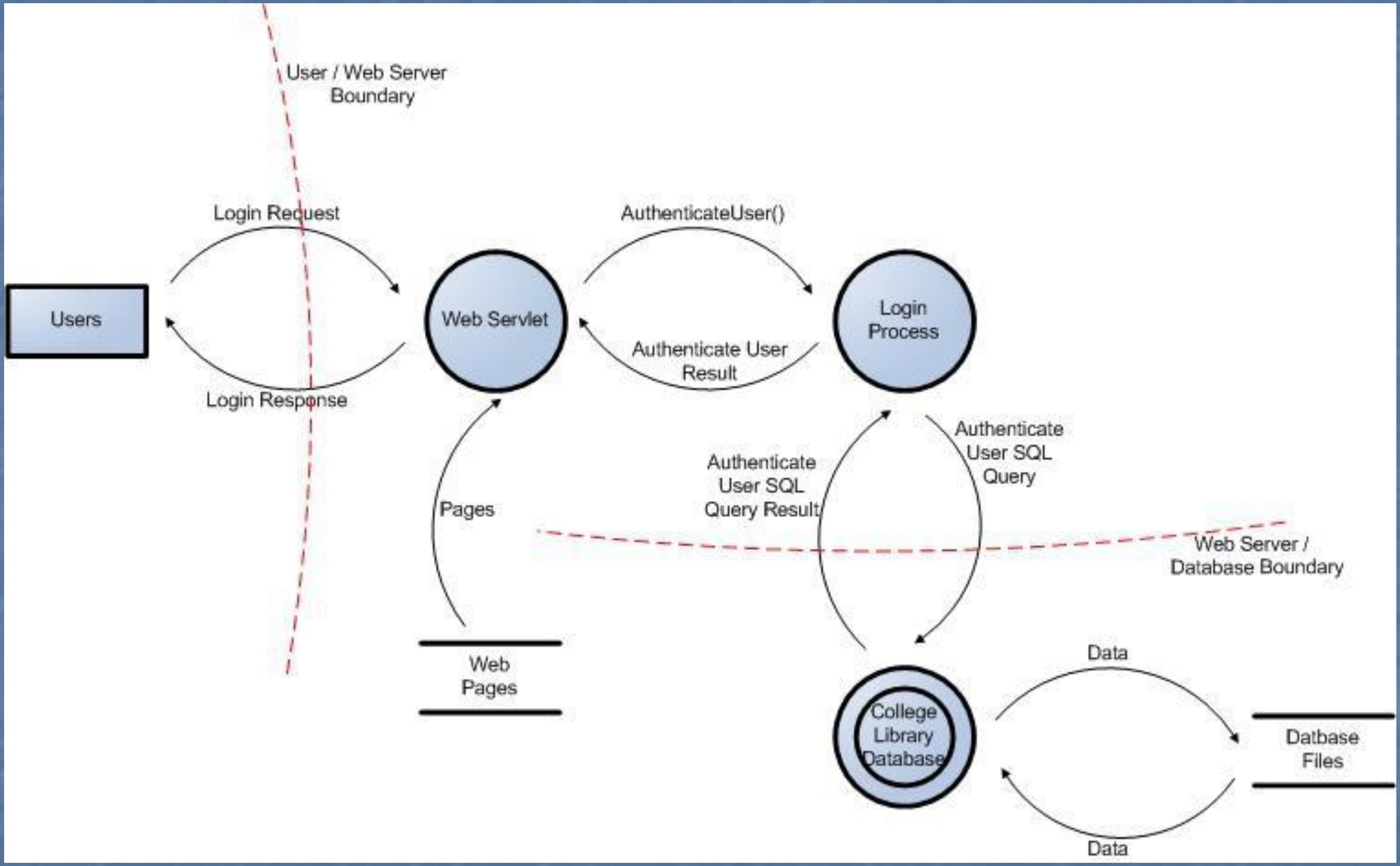
Trust Levels

ID	Name	Description
1	Anonymous Web User	A user who has connected to the college library website but has not provided valid credentials.
2	User with Valid Login Credentials	A user who has connected to the college library website and has logged in using valid login credentials.
3	User with Invalid Login Credentials	A user who has connected to the college library website and is attempting to log in using invalid login credentials.
4	Librarian	The librarian can create users on the library website and view their personal information.
5	Database Server Administrator	The database server administrator has read and write access to the database that is used by the college library website.
6	Website Administrator	The Website administrator can configure the college library website.
7	Web Server User Process	This is the process/user that the web server executes code as and authenticates itself against the database server as.
8	Database Read User	The database user account used to access the database for read access.
9	Database Read/Write User	The database user account used to access the database for read and write access.

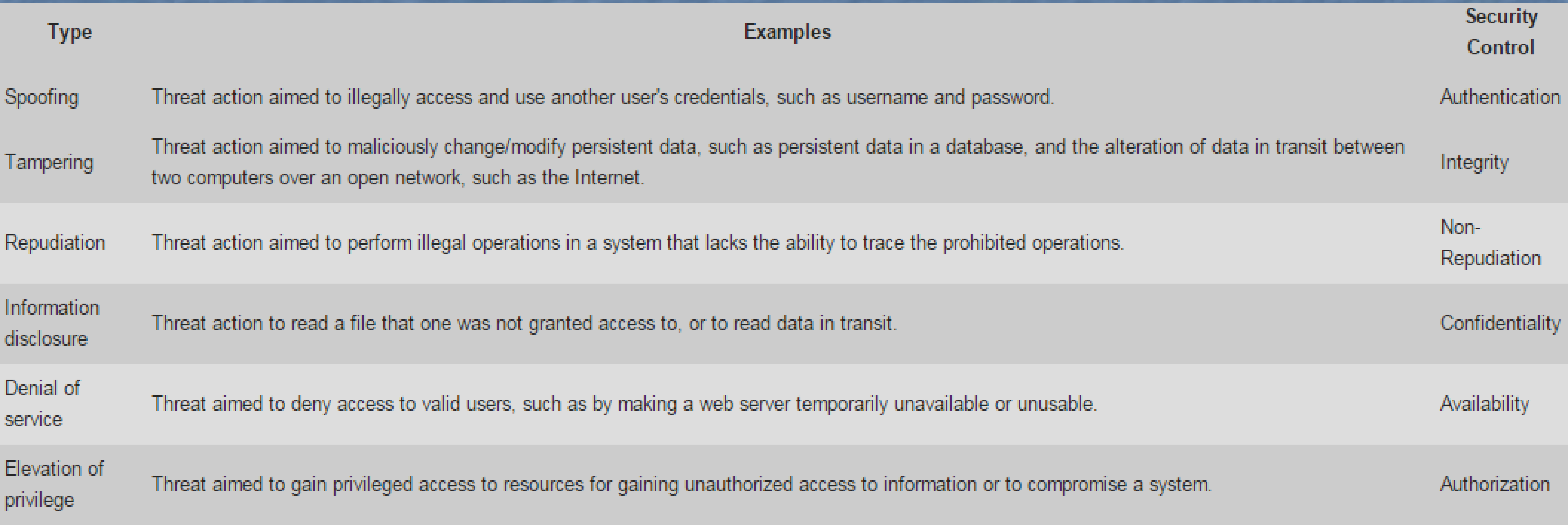
Data Flow Diagram for the College Library Website



User Login Data Flow Diagram for the College Library Website

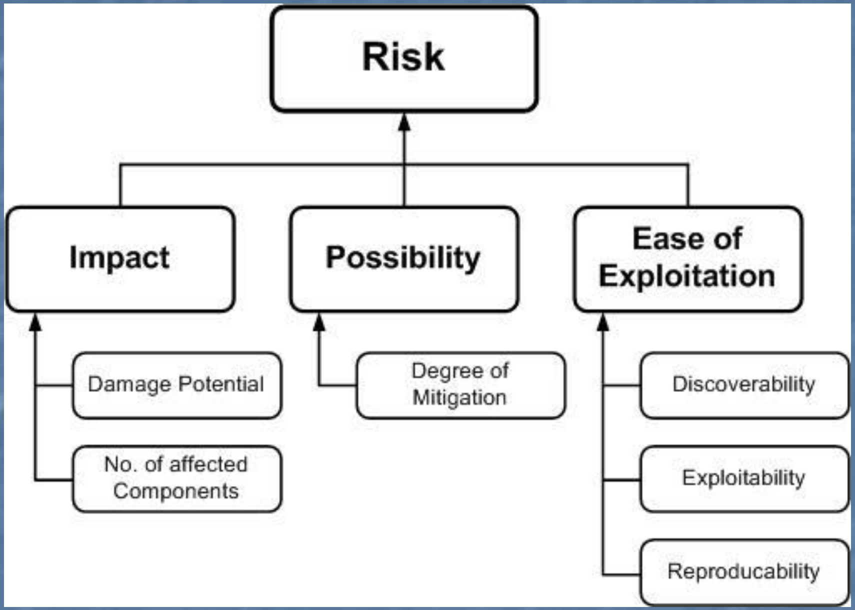


STRIDE Threat List



Type	Examples	Security Control
Spoofing	Threat action aimed to illegally access and use another user's credentials, such as username and password.	Authentication
Tampering	Threat action aimed to maliciously change/modify persistent data, such as persistent data 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 to perform illegal operations in a system that lacks the ability to trace the prohibited operations.	Non-Repudiation
Information disclosure	Threat action to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of service	Threat aimed to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privilege	Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system.	Authorization

Ranking of Threats



1. **Damage potential:** Threat to reputation as well as financial and legal liability:8
2. **Reproducibility:** Fully reproducible:10
3. **Exploitability:** Require to be on the same subnet or have compromised a router:7
4. **Affected users:** Affects all users:10
5. **Discoverability:** Can be found out easily:10

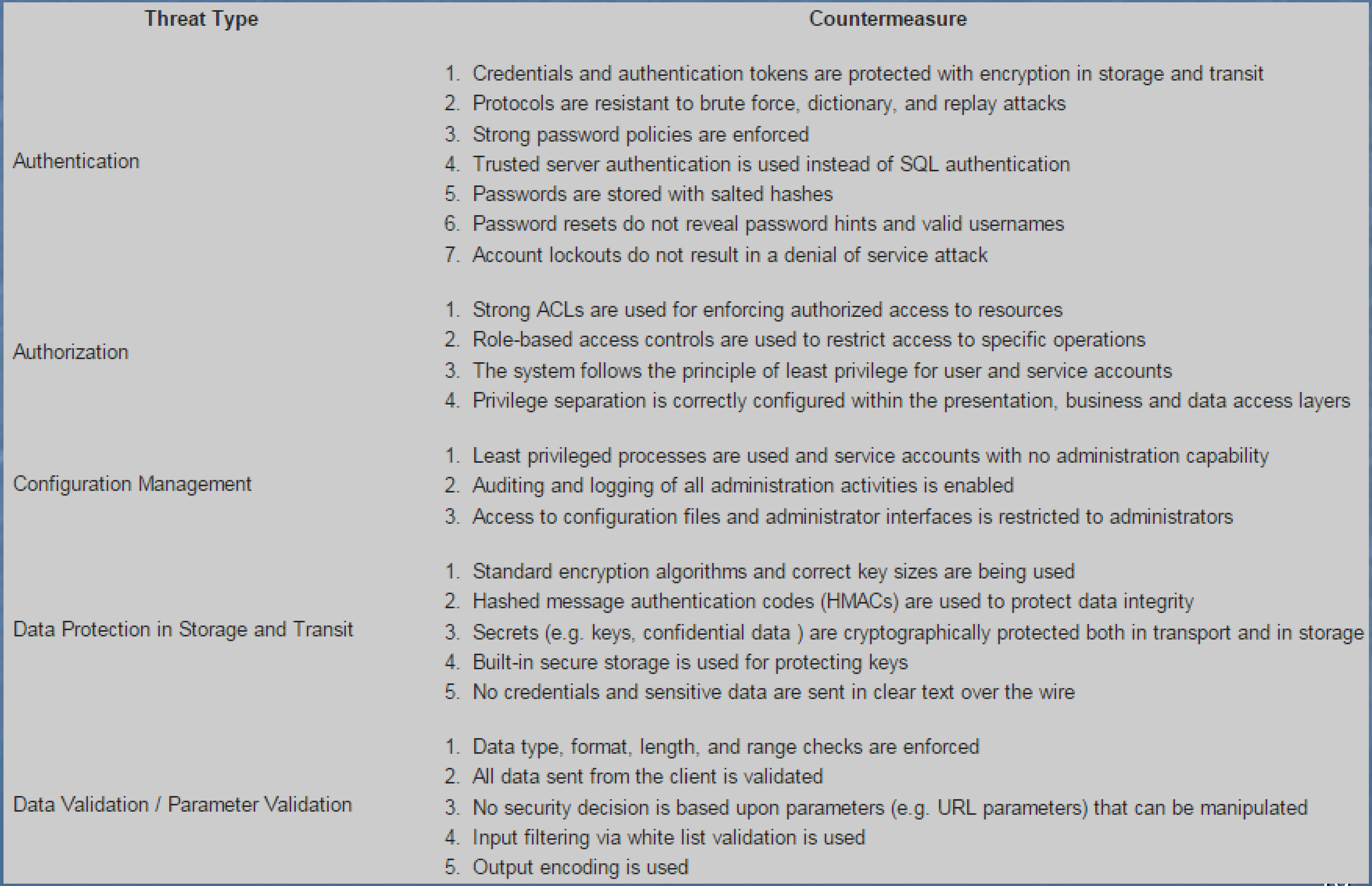
Overall DREAD score: (8+10+7+10+10) / 5 = 9

In this case having 9 on a 10 point scale is certainly a high risk threat

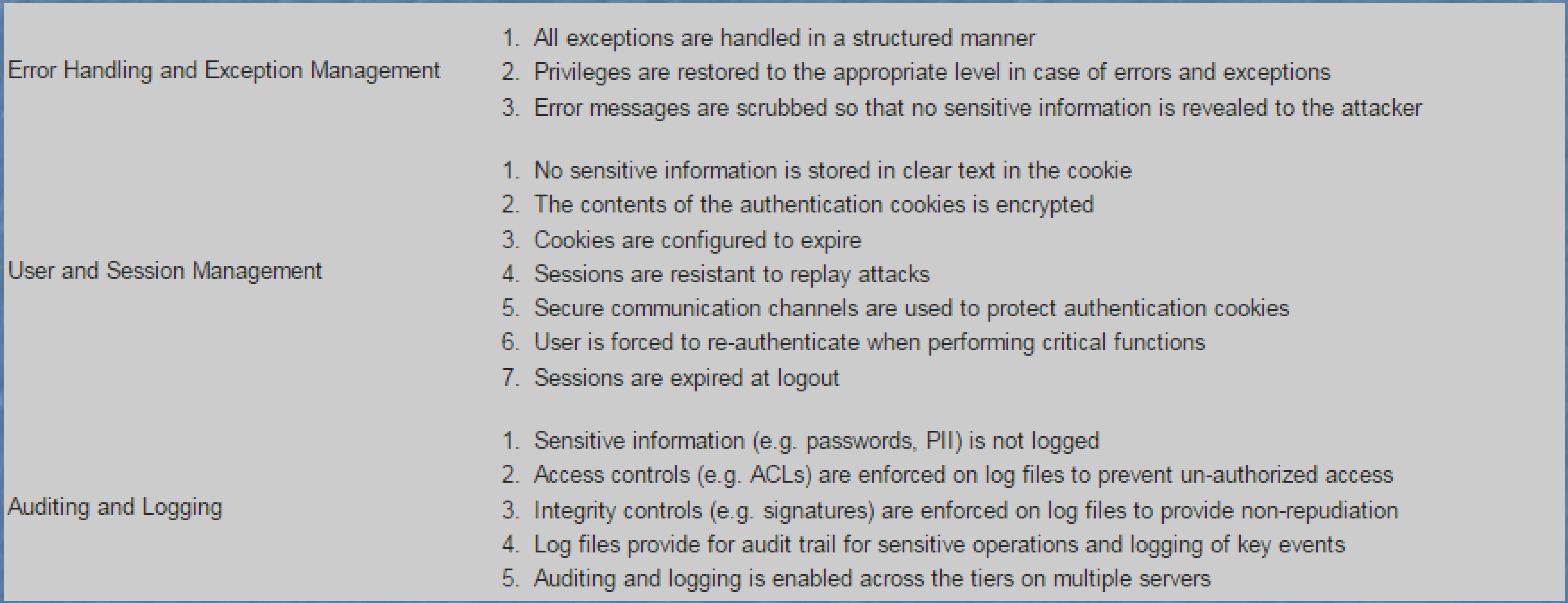
Mitigation Strategies

- **Do nothing:** for example, hoping for the best
- **Inform about the risk:** for example, warning user population about the risk
- **Mitigate the risk:** for example, by putting countermeasures in place
- **Accept the risk:** for example, after evaluating the impact of the exploitation (business impact)
- **Transfer the risk:** for example, through contractual agreements and insurance
- **Terminate the risk:** for example, shutdown, turn-off, unplug or decommission the asset

Threat & Countermeasures List

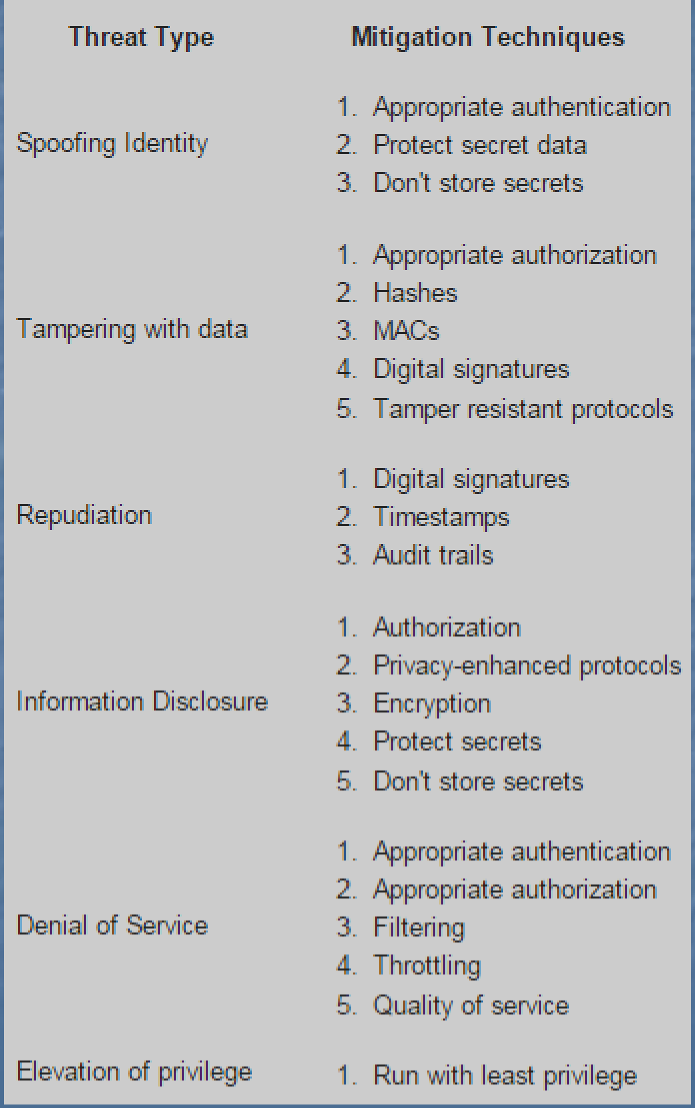


Threat Type	Countermeasure
Authentication	1. Credentials and authentication tokens are protected with encryption in storage and transit
	2. Protocols are resistant to brute force, dictionary, and replay attacks
	3. Strong password policies are enforced
	4. Trusted server authentication is used instead of SQL authentication
	5. Passwords are stored with salted hashes
	6. Password resets do not reveal password hints and valid usernames
	7. Account lockouts do not result in a denial of service attack
Authorization	1. Strong ACLs are used for enforcing authorized access to resources
	2. Role-based access controls are used to restrict access to specific operations
	3. The system follows the principle of least privilege for user and service accounts
	4. Privilege separation is correctly configured within the presentation, business and data access layers
Configuration Management	1. Least privileged processes are used and service accounts with no administration capability
	2. Auditing and logging of all administration activities is enabled
	3. Access to configuration files and administrator interfaces is restricted to administrators
Data Protection in Storage and Transit	1. Standard encryption algorithms and correct key sizes are being used
	2. Hashed message authentication codes (HMACs) are used to protect data integrity
	3. Secrets (e.g. keys, confidential data) are cryptographically protected both in transport and in storage
	4. Built-in secure storage is used for protecting keys
	5. No credentials and sensitive data are sent in clear text over the wire
Data Validation / Parameter Validation	1. Data type, format, length, and range checks are enforced
	2. All data sent from the client is validated
	3. No security decision is based upon parameters (e.g. URL parameters) that can be manipulated
	4. Input filtering via white list validation is used
	5. Output encoding is used



Error Handling and Exception Management	1. All exceptions are handled in a structured manner 2. Privileges are restored to the appropriate level in case of errors and exceptions 3. Error messages are scrubbed so that no sensitive information is revealed to the attacker
User and Session Management	1. No sensitive information is stored in clear text in the cookie 2. The contents of the authentication cookies is encrypted 3. Cookies are configured to expire 4. Sessions are resistant to replay attacks 5. Secure communication channels are used to protect authentication cookies 6. User is forced to re-authenticate when performing critical functions 7. Sessions are expired at logout
Auditing and Logging	1. Sensitive information (e.g. passwords, PII) is not logged 2. Access controls (e.g. ACLs) are enforced on log files to prevent un-authorized access 3. Integrity controls (e.g. signatures) are enforced on log files to provide non-repudiation 4. Log files provide for audit trail for sensitive operations and logging of key events 5. Auditing and logging is enabled across the tiers on multiple servers

Threat & Mitigation Techniques List



Threat Type	Mitigation Techniques
Spoofing Identity	1. Appropriate authentication 2. Protect secret data 3. Don't store secrets
Tampering with data	1. Appropriate authorization 2. Hashes 3. MACs 4. Digital signatures 5. Tamper resistant protocols
Repudiation	1. Digital signatures 2. Timestamps 3. Audit trails
Information Disclosure	1. Authorization 2. Privacy-enhanced protocols 3. Encryption 4. Protect secrets 5. Don't store secrets
Denial of Service	1. Appropriate authentication 2. Appropriate authorization 3. Filtering 4. Throttling 5. Quality of service
Elevation of privilege	1. Run with least privilege

Application Threat Modeling Example