Parag Mhatre
ITIS 5221

Application Description:

The conference management system is a web based application that provides conference managers and administrators the ability to create and manage conferences along with the conference users.

Users:

- Administrators:
    - Create conferences and make financial transactions with the credit card processor and the bank.
- Conference Organizer:
    - Create custom conference registration site, query and download conference registrations, change registration details for conference attendees, and issue refunds.
- Conference Attendee:
    - Register and pay for conference.

External Dependencies:

- Application Web Server:
    - Used to host the web application and host the authentication data.
- Database Server:
    - Used to host the registration and financial data bases.
- Bank:
    - Used to transfer funds to the conference organizer.
- Credit Card Processor:
    - Used to process credit card transactions between the site and the conference attendees.

Entry Points:

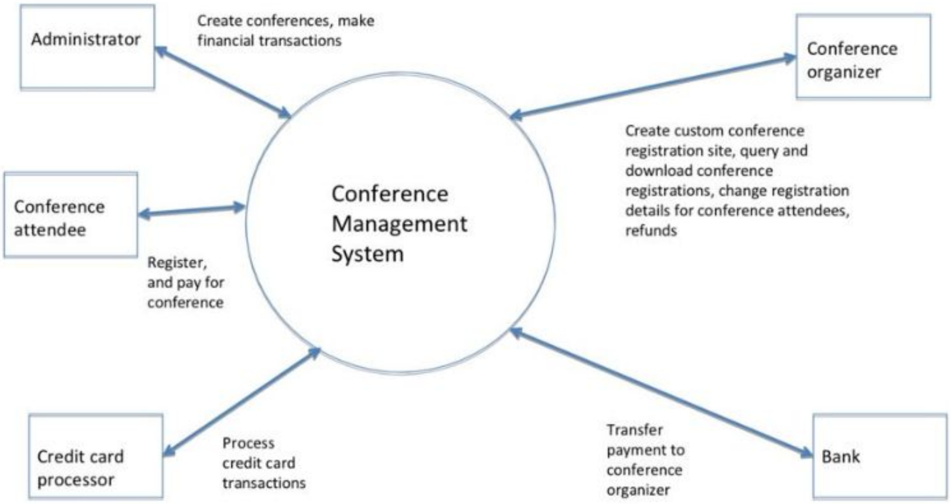
- Administration page:
    - Allows administrators to create conferences and make financial transactions with the credit card processor and the bank.
    - Should be restricted to administrators only.

- Conference Management page:
  - Allows Conference Organizers to create custom conference registration site,query and download conference registrations, change registration details for conference attendees, and issue refunds.
  - Should be restricted to Conference Organizers only.
- Conference Registration page:
  - Should only allow users to register to the site nothing else.

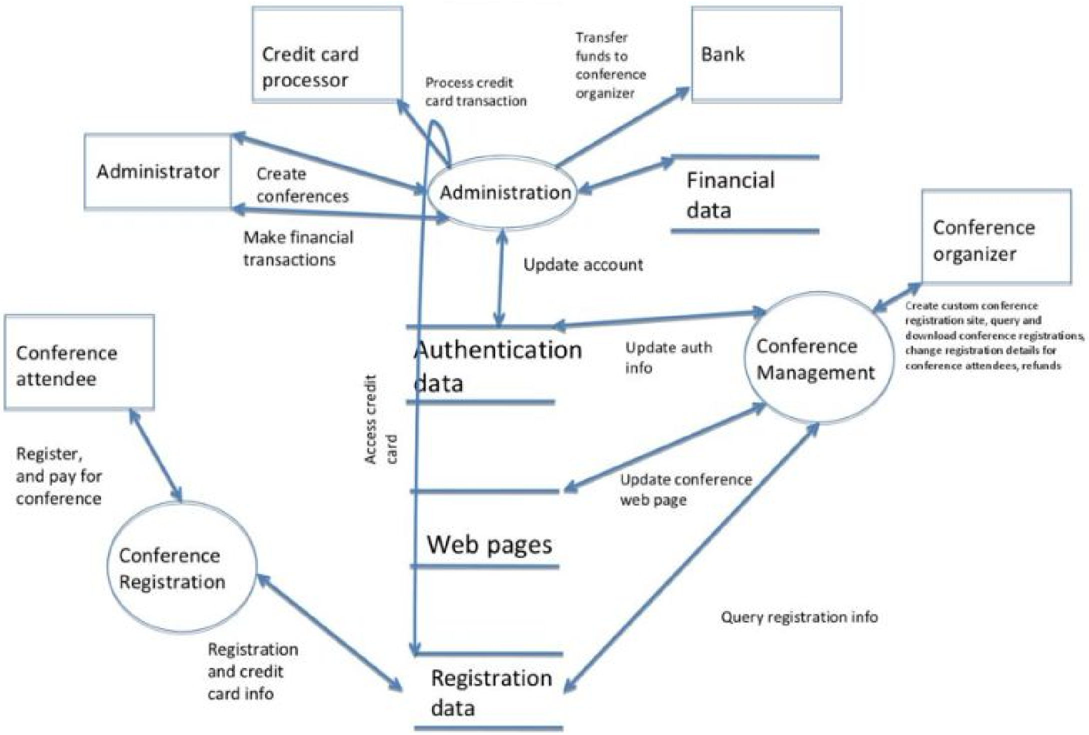
Assets:

- User registration data:
  - Registration and credit card data relating to conference attendees.
- Authentication data:
  - Administrator and Organizer user login details.
- Financial data:
  - Financial data pertaining to the conferences including transactions, credit card,and banking account data.
- Availability of registration, administration, and management pages and functionality:
  - The pages should be up and functioning.
- Availability of the databases:
  - The databases should be up and functioning

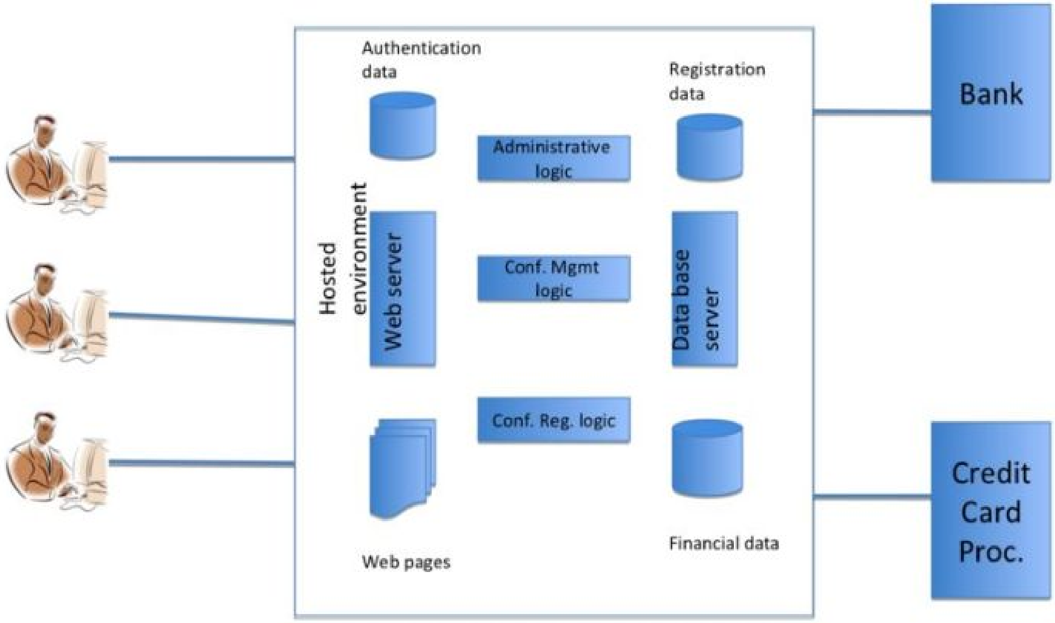
Context Diagram:


Administrator
Create conferences, make financial transactions
Conference organizer
Conference attendee
Conference Management System
Create custom conference registration site, query and download conference registrations, change registration details for conference attendees, refunds
Register, and pay for conference
Credit card processor
Process credit card transactions
Transfer payment to conference organizer
Bank

Data Flow Diagram:

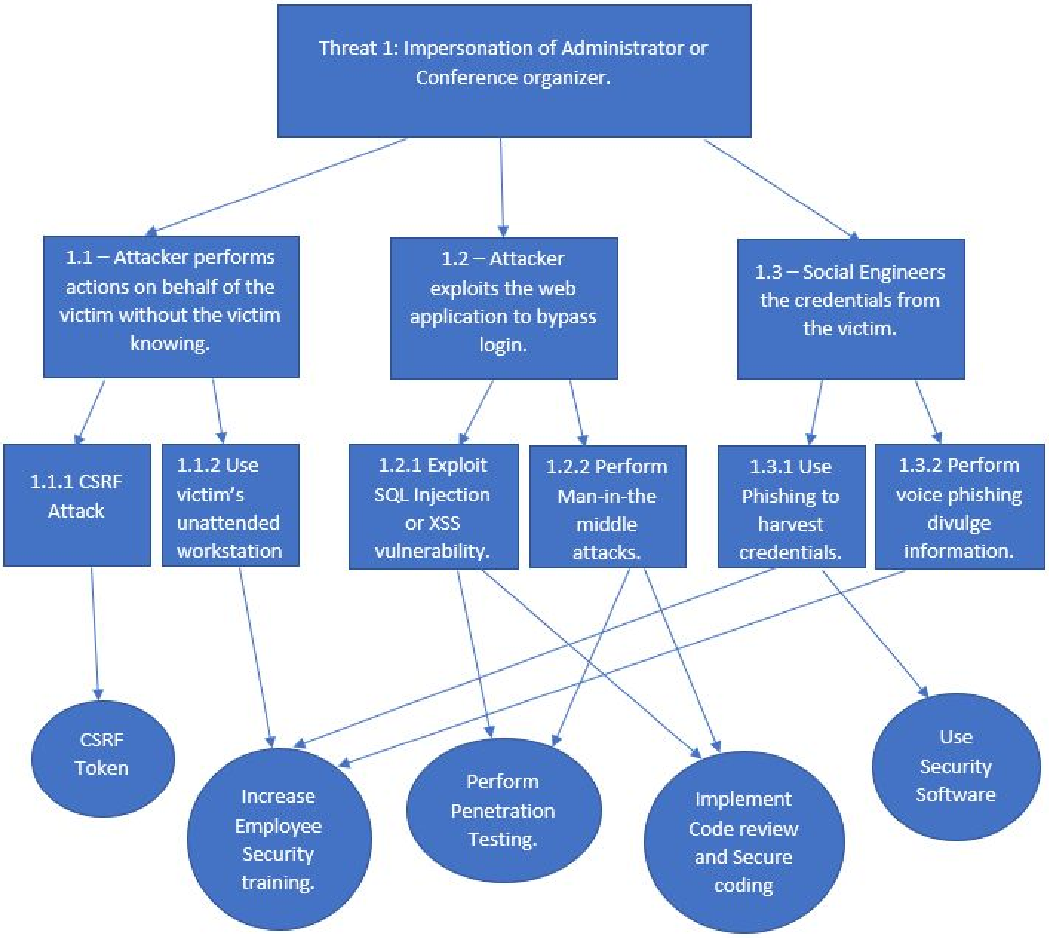

Credit card processor
Process credit card transaction
Transfer funds to conference organizer
Bank
Administrator
Create conferences
Administration
Financial data
Make financial transactions
Update account
Conference organizer
Create custom conference registration site, query and download conference registrations, change registration details for conference attendees, refunds
Conference attendee
Authentication data
Update auth info
Conference Management
Access credit card
Register, and pay for conference
Update conference web page
Web pages
Conference Registration
Query registration info
Registration and credit card info
Registration data

Physical System View:



Threats:

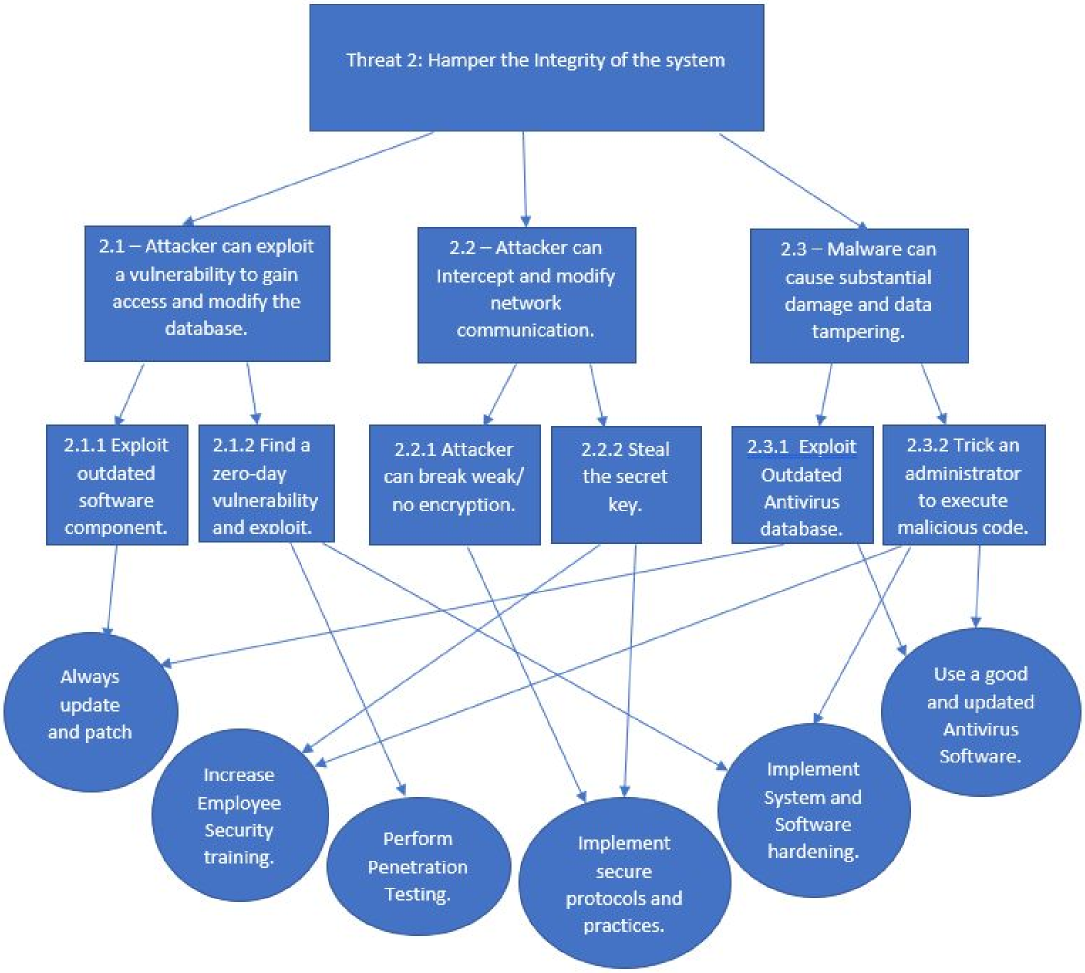
- **Threat 1:**
  - Category: Spoofing


Threat 1: Impersonation of Administrator or Conference organizer.
1.1 – Attacker performs actions on behalf of the victim without the victim knowing.
1.2 – Attacker exploits the web application to bypass login.
1.3 – Social Engineers the credentials from the victim.
1.1.1 CSRF Attack
1.1.2 Use victim's unattended workstation
1.2.1 Exploit SQL Injection or XSS vulnerability.
1.2.2 Perform Man-in-the middle attacks.
1.3.1 Use Phishing to harvest credentials.
1.3.2 Perform voice phishing divulge information.
CSRF Token
Increase Employee Security training.
Perform Penetration Testing.
Implement Code review and Secure coding
Use Security Software

DREAD Score = 15

D	Damage potential	High (3) - The attacker can get full trust authorization; run as administrator; upload content.
R	Reproducibility	High (3) - The attack can be reproduced every time and does not require a timing window.
E	Exploitability	High (3) - A novice programmer could make the attack, and then repeat the steps.
A	Affected users	High (3) - All users can be affected.
D	Discoverability	High (3) - The vulnerability is in a commonly used feature.

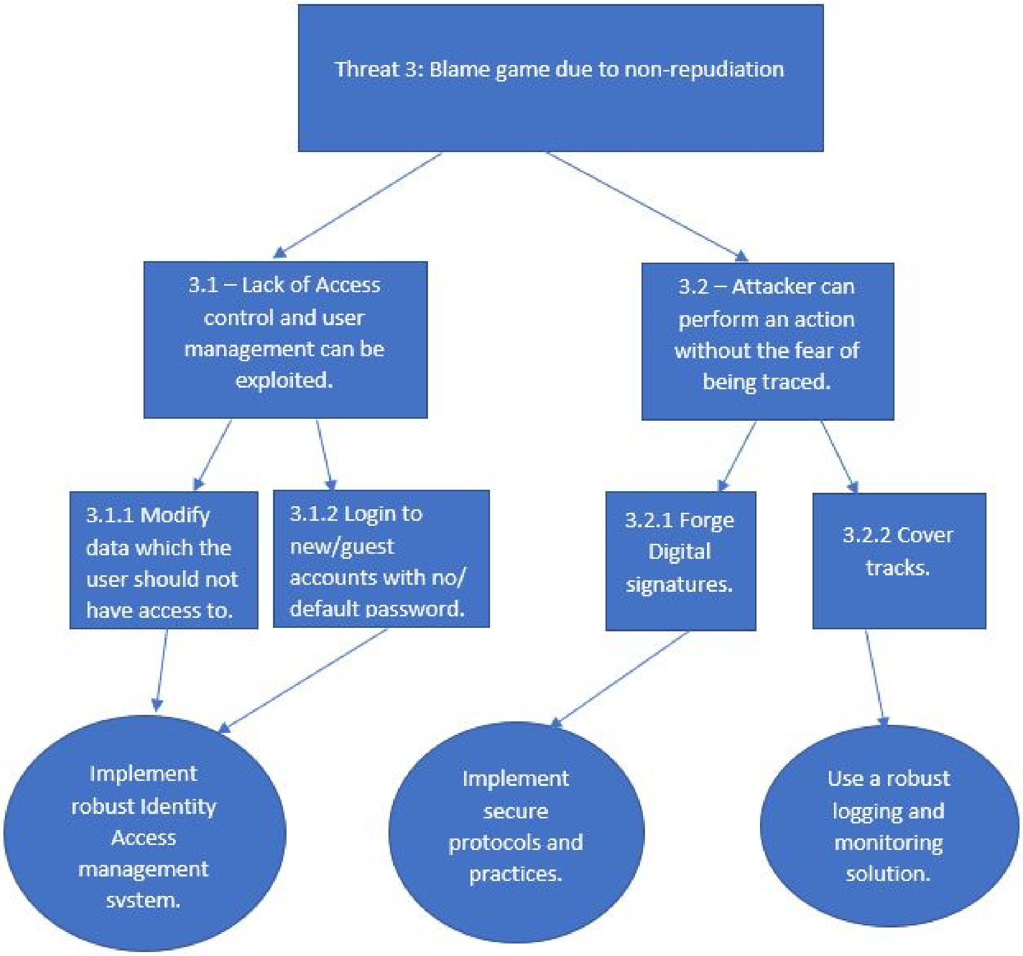
- **Threat 2:**
    - Category: Tampering


Threat 2: Hamper the Integrity of the system
2.1 – Attacker can exploit a vulnerability to gain access and modify the database.
2.2 – Attacker can Intercept and modify network communication.
2.3 – Malware can cause substantial damage and data tampering.
2.1.1 Exploit outdated software component.
2.1.2 Find a zero-day vulnerability and exploit.
2.2.1 Attacker can break weak/ no encryption.
2.2.2 Steal the secret key.
2.3.1 Exploit Outdated Antivirus database.
2.3.2 Trick an administrator to execute malicious code.
Always update and patch
Increase Employee Security training.
Perform Penetration Testing.
Implement secure protocols and practices.
Implement System and Software hardening.
Use a good and updated Antivirus Software.

DREAD Score = 15

D	Damage potential	High (3) - The attacker can get full trust authorization; run as administrator; upload content.
R	Reproducibility	High (3) - The attack can be reproduced every time and does not require a timing window.
E	Exploitability	High (3) - A novice programmer could make the attack, and then repeat the steps.
A	Affected users	High (3) - All users can be affected.
D	Discoverability	High (3) - The vulnerability is in a commonly used feature.

- **Threat 3:**
  - Category: Repudiation

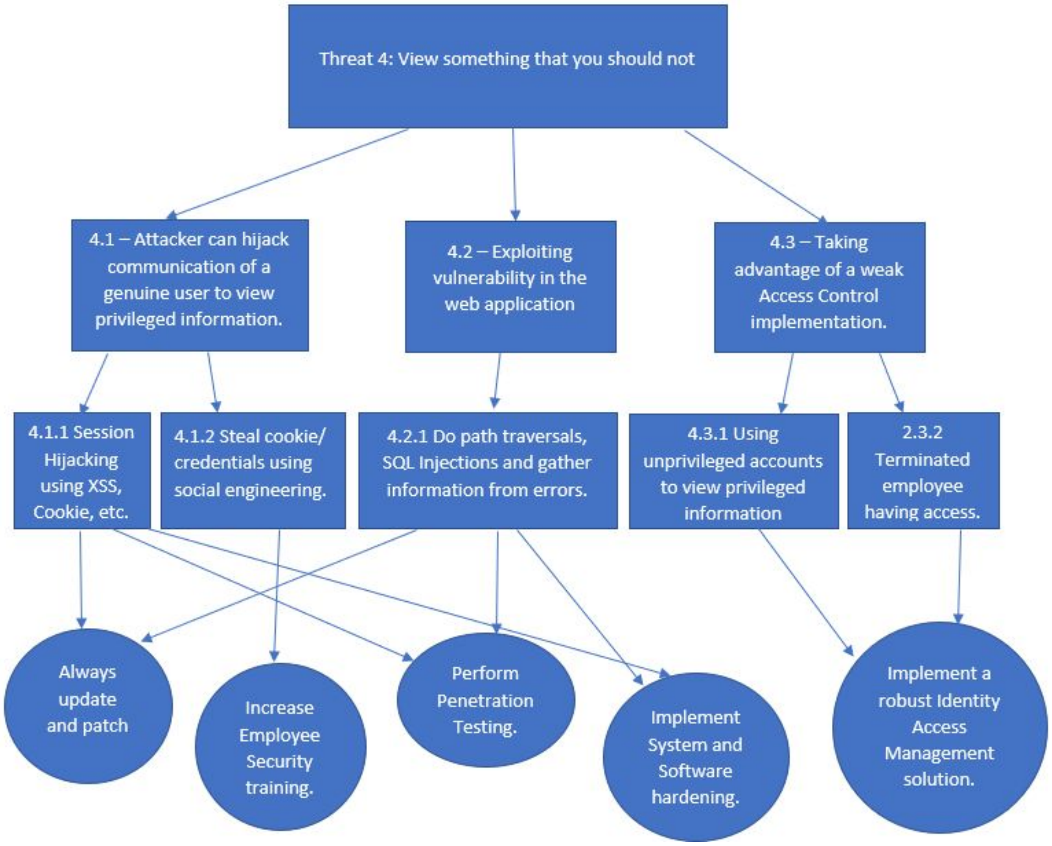

Threat 3: Blame game due to non-repudiation
3.1 – Lack of Access control and user management can be exploited.
3.2 – Attacker can perform an action without the fear of being traced.
3.1.1 Modify data which the user should not have access to.
3.1.2 Login to new/guest accounts with no/ default password.
3.2.1 Forge Digital signatures.
3.2.2 Cover tracks.
Implement robust Identity Access management system.
Implement secure protocols and practices.
Use a robust logging and monitoring solution.

DREAD Score = 15

D	Damage potential	High (3) - The attacker can get full trust authorization; run as administrator; upload content.
R	Reproducibility	High (3) - The attack can be reproduced every time and does not require a timing window.
E	Exploitability	High (3) - A novice programmer could make the attack, and then repeat the steps.
A	Affected users	High (3) - All users can be affected.
D	Discoverability	High (3) - The vulnerability is in a commonly used feature.

Threat 4:

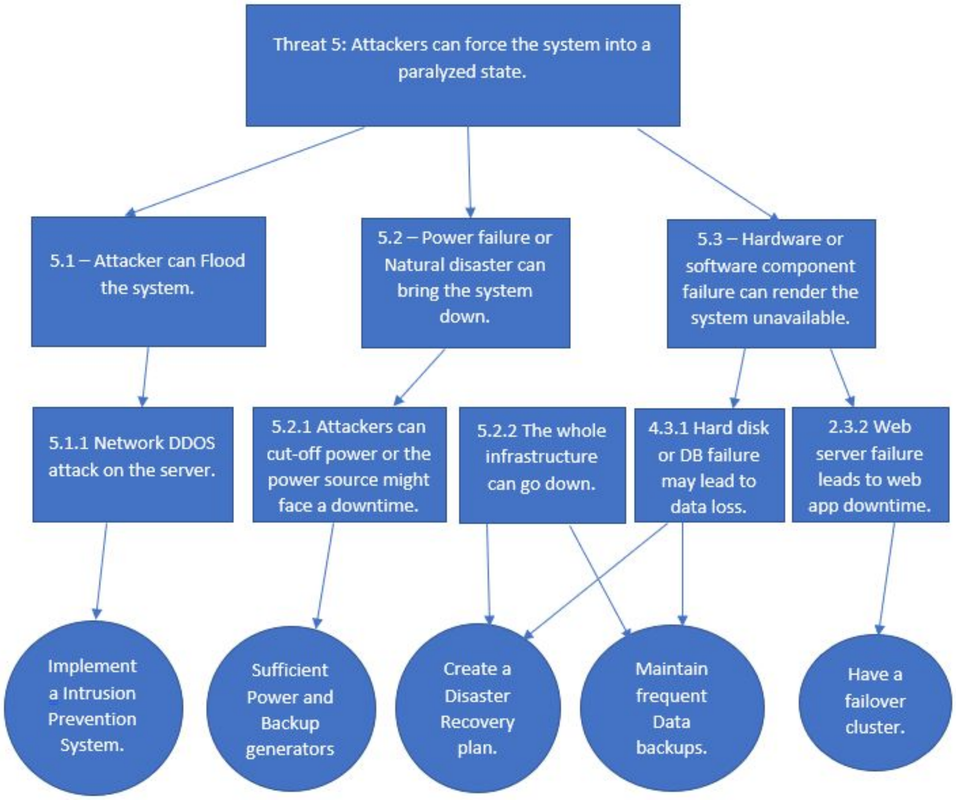
- Category: Information Disclosure


Threat 4: View something that you should not
4.1 – Attacker can hijack communication of a genuine user to view privileged information.
4.2 – Exploiting vulnerability in the web application
4.3 – Taking advantage of a weak Access Control implementation.
4.1.1 Session Hijacking using XSS, Cookie, etc.
4.1.2 Steal cookie/ credentials using social engineering.
4.2.1 Do path traversals, SQL Injections and gather information from errors.
4.3.1 Using unprivileged accounts to view privileged information
2.3.2 Terminated employee having access.
Always update and patch
Increase Employee Security training.
Perform Penetration Testing.
Implement System and Software hardening.
Implement a robust Identity Access Management solution.

DREAD Score = 15

D	Damage potential	High (3) - The attacker can get full trust authorization; run as administrator; upload content.
R	Reproducibility	High (3) - The attack can be reproduced every time and does not require a timing window.
E	Exploitability	High (3) - A novice programmer could make the attack, and then repeat the steps.
A	Affected users	High (3) - All users can be affected.
D	Discoverability	High (3) - The vulnerability is in a commonly used feature.

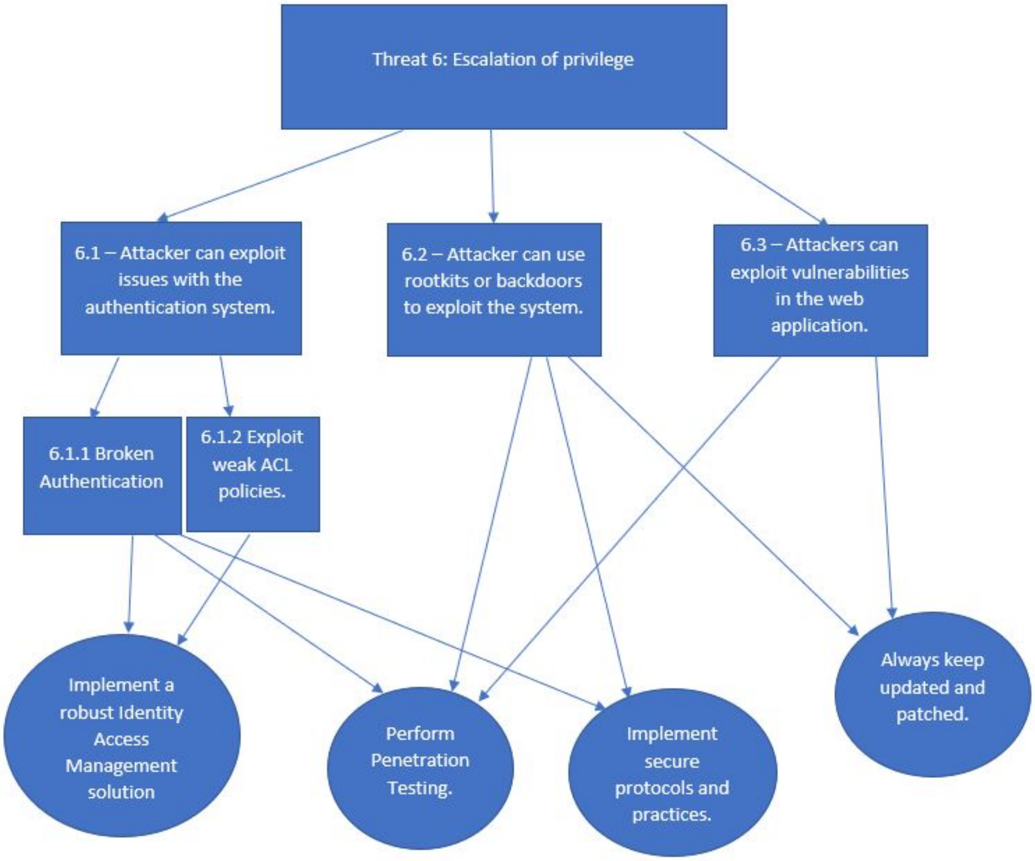
- **Threat 5:**
    - Category: Denial of Service


Threat 5: Attackers can force the system into a paralyzed state.
5.1 – Attacker can Flood the system.
5.2 – Power failure or Natural disaster can bring the system down.
5.3 – Hardware or software component failure can render the system unavailable.
5.1.1 Network DDOS attack on the server.
5.2.1 Attackers can cut-off power or the power source might face a downtime.
5.2.2 The whole infrastructure can go down.
4.3.1 Hard disk or DB failure may lead to data loss.
2.3.2 Web server failure leads to web app downtime.
Implement a Intrusion Prevention System.
Sufficient Power and Backup generators
Create a Disaster Recovery plan.
Maintain frequent Data backups.
Have a failover cluster.

DREAD Score = 15

D	Damage potential	High (3) - The attacker can get full trust authorization; run as administrator; upload content.
R	Reproducibility	High (3) - The attack can be reproduced every time and does not require a timing window.
E	Exploitability	High (3) - A novice programmer could make the attack, and then repeat the steps.
A	Affected users	High (3) - All users can be affected.
D	Discoverability	High (3) - The vulnerability is in a commonly used feature.

- **Threat 6:**
    - Category: Elevation of Privilege


Threat 6: Escalation of privilege
6.1 – Attacker can exploit issues with the authentication system.
6.2 – Attacker can use rootkits or backdoors to exploit the system.
6.3 – Attackers can exploit vulnerabilities in the web application.
6.1.1 Broken Authentication
6.1.2 Exploit weak ACL policies.
Implement a robust Identity Access Management solution
Perform Penetration Testing.
Implement secure protocols and practices.
Always keep updated and patched.

DREAD Score = 15

D	Damage potential	High (3) - The attacker can get full trust authorization; run as administrator; upload content.
R	Reproducibility	High (3) - The attack can be reproduced every time and does not require a timing window.
E	Exploitability	High (3) - A novice programmer could make the attack, and then repeat the steps.
A	Affected users	High (3) - All users can be affected.
D	Discoverability	High (3) - The vulnerability is in a commonly used feature.