Risk Analysis of University Admission website

Himanshu || 231024 || M.Sc Cyber Security

Phase 1: Business Value of System

High-Level Goals:

1. Enhance Student Experience
2. Secure and Efficient Data Management
3. Streamline Administrative Processes
4. Maintain Institutional Reputation

Goal Breakdown:

1. Enhance Student Experience:

- Provide User-Friendly Interface:
  - Simplify navigation and accessibility for prospective students.
  - Implement responsive design for various devices (desktops, tablets, smartphones).
- Offer Real-Time Support:
  - Integrate chat support and FAQs to assist applicants.
  - Provide timely responses to inquiries via email and chat.
- Ensure Smooth Application Process:
  - Enable easy document uploads and application form submissions.
  - Provide clear instructions and status updates throughout the application process.

2. Secure and Efficient Data Management:

- Ensure Data Confidentiality:
  - Implement strong encryption for sensitive data (personal details, financial information).
  - Restrict data access to authorized personnel only.
- Maintain Data Integrity:
  - Regularly update and patch system components to prevent vulnerabilities.
  - Conduct routine data integrity checks and audits.
- Enhance Data Availability:
  - Use robust backup solutions to prevent data loss.
  - Implement failover systems to ensure continuous data availability.

3. Streamline Administrative Processes:

- Automate Admission Workflow:

    - Automate application review and decision-making processes.
    - Integrate electronic notifications for application status updates.
- Optimize Resource Allocation:
    - Allocate staff resources effectively based on application volumes.
    - Use analytics to predict and manage application trends.
- Improve Data Processing Efficiency:
    - Implement batch processing for large volumes of data.
    - Optimize database queries to reduce processing times.

4. Maintain Institutional Reputation:

- Protect Against Data Breaches:
    - Implement comprehensive security measures (firewalls, intrusion detection systems).
    - Conduct regular security assessments and penetration testing.
- Ensure High Availability:
    - Implement load balancing and redundancy to prevent downtime.
    - Monitor system performance and address issues proactively.
- Promote Transparency and Trust:
    - Communicate security measures and privacy policies clearly to users.
    - Ensure transparency in handling data breaches and incidents.

Business Architecture

High-Level Use Cases (Business Processes):

a. Admissions Management:

- Use Case: Manage Application Submissions
    - Actors: Prospective Students, Admissions Staff
    - Description: Prospective students submit applications through the portal. Admissions staff review and process these applications.
- Use Case: Application Review and Decision
    - Actors: Admissions Staff, Faculty Members
    - Description: Admissions staff and faculty members review applications, make admission decisions, and communicate outcomes to applicants.
- Use Case: Payment Processing
    - Actors: Prospective Students, Financial Department
    - Description: Applicants pay application fees through the portal. The financial department handles the payment processing and reconciliation.

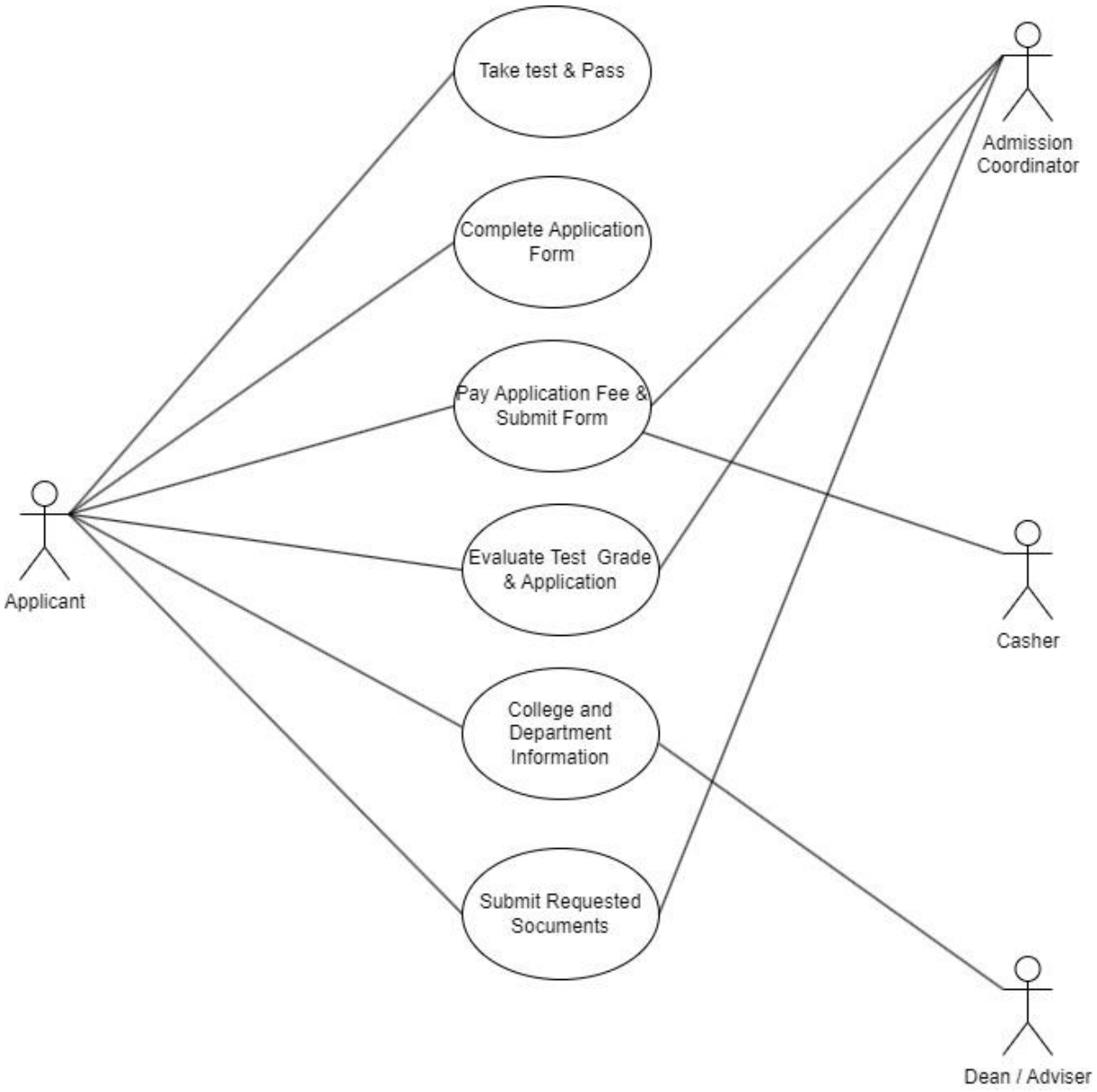
b. User Support and Communication:

- Use Case: Provide Real-Time Support
    - Actors: Prospective Students, Support Staff

    - Description: Support staff assist prospective students through chat and email support integrated into the portal.
- Use Case: Send Notifications and Updates
    - Actors: Admissions Staff, Prospective Students
    - Description: The system sends notifications to applicants about their application status, important deadlines, and other relevant information.

c. Data Management:

- Use Case: Maintain Applicant Data
    - Actors: Admissions Staff, IT Staff
    - Description: Admissions staff and IT personnel manage and maintain the integrity of applicant data in the database.
- Use Case: Data Backup and Recovery
    - Actors: IT Staff
    - Description: IT staff ensure regular backups of data and implement recovery procedures in case of data loss.



Negative Business Impact of Breach

Loss event	Abuse case no.	Abuse case	Attacked Asset	Impacted Actor
Unauthorized access to applicant data	1	Data breach	Web application, database	External, Internal
Financial fraud (unauthorized transactions)	2	Payment fraud	Payment gateway, database	External
Denial of service (website unavailable)	3	Denial of Service (DoS) attack	Web application, network	External
Data corruption or loss	4	Data tampering, accidental deletion	Database	Internal

Reputational damage	5	Negative publicity due to breach	Website, organization's brand	External, Internal

Phase 2 - System Definition and Decomposition

1. Functions

Assets	Version	function type
Ubuntu Server	10.04 LTS	Platform
Vmware ESXI	7.0.3	Platform
Windows Server 2016	1709	Platform
Apache2	2.4.50	Platform
My Sql Server	8.0.27	Database
Wordpress	4.1.34	Database
MS SQL SERVER 2019 CU25+GDR	9.6	Database
Web Application		Service
Authentication data		Data
Payments Info		Data
User Info		Data
User Documents		Data
WordPress Database		Data
Data Centre Trust boundary		Network
DMZ Zone Trust Boundary		Network

2. Actors and Accounts

Actors:

- Prospective Students: Users who access the portal to submit applications and check their status.
- Admissions Staff: Users who review and manage applications.
- IT Staff: Users responsible for maintaining and securing the system.
- Support Staff: Users who provide assistance to prospective students.

Accounts:

- Student Accounts: Created by prospective students to submit applications and track their progress.
- Admin Accounts: Used by admissions and IT staff to access the backend system and manage applications.
- Support Accounts: Used by support staff to assist students with their queries.

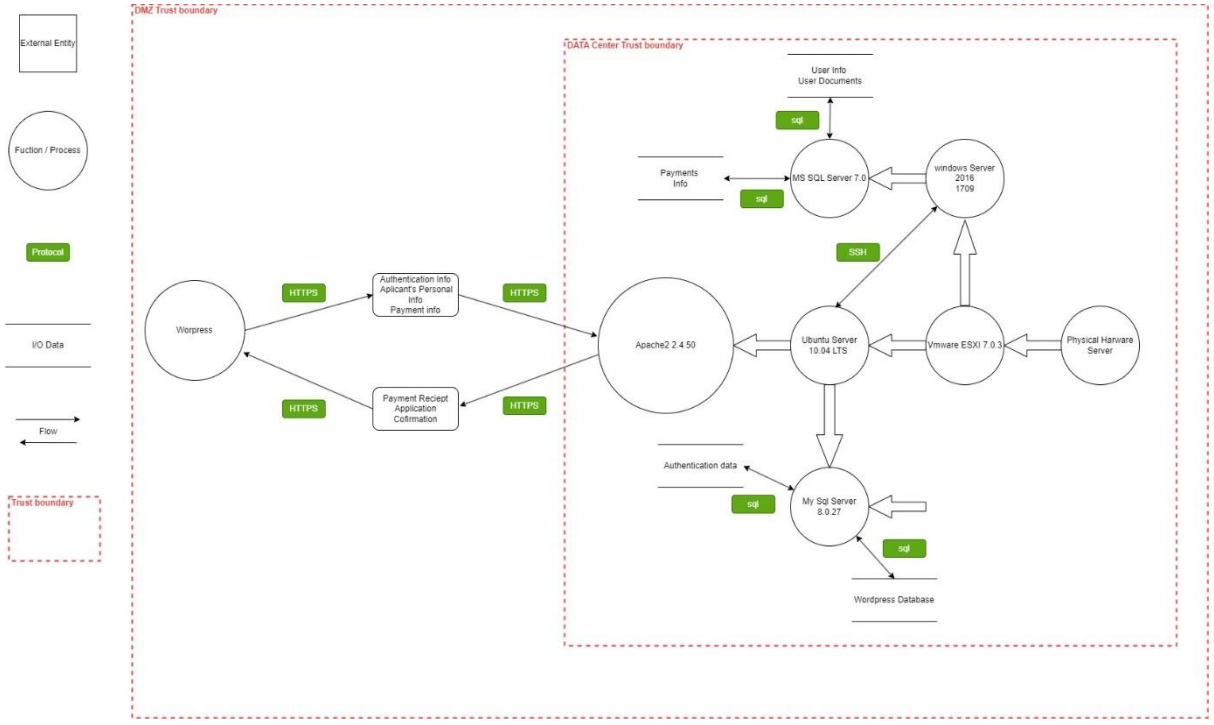
Authorization:

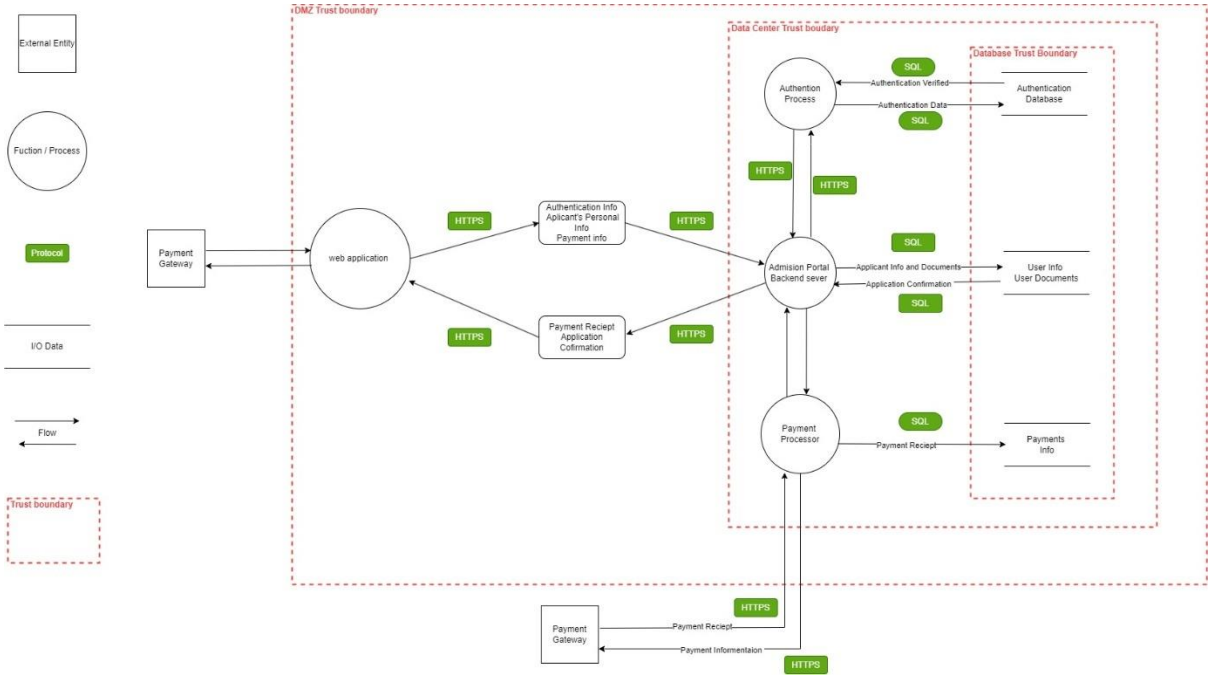
- Student Accounts: Can create, read, update, and delete their own applications.
- Admin Accounts: Can read, update, and delete all applications; can also manage user accounts.
- Support Accounts: Can read student applications and provide assistance; limited update capabilities.

3. Communication Channels

- Internet: Used by students to access the admission portal.
- Internal Network: Used by staff to access the backend system.
- HTTPS: Secure protocol for data transmission between the web server and users.

Data Flow Diagram





Phase 3 - Threat Analysis

Potential Attacker Profiles

Attacker	**Script kiddie**	**Organized crime targeting ransomware**	**Expelled Student**
Risk tolerance	low/medium	high	high
concern for collateral damage	medium/high	low	high
Skill (quality, domain)	low/medium	high	medium/high
resources (time, headcount, tools)	medium	high	medium/high
sponsorship	none	medium/high	none
Derived threat capability	20%	10%	80%

Potential abuse cases

Abuse case (threat action or attack goal)	Data breach	Payment fraud	Denial of Service (DoS) attack	Data tampering, accidental deletion	Negative publicity due to breach
Number of abuse case	1	2	3	4	5
Target asset	User data	Financial information	website	data	Applicant Data, Document and Payment Info
attack surface	Web application, database	Payment gateway, database	Web application, network	Database	Website, organization's brand
Accessibility to attack surface (attack surface is not necessarily the asset that the abuse case relates to)	High	High	High	High	High

Window of opportunity	High	mid	High	mid	High
Probability of Contact (PoC) in percentage	100%	20%	80%	60%	10%
Concern for collateral damage (Attacker)	Mid/High	Mid	Low	Mid/High	Low
Risk tolerance (Attacker)	Low	mid	High	Mid	High
Ability to repudiate	Low	mid	High	Mid/High	High
Perceived deterrence	mid	mid	mid	mid	mid
Perceived ease of attack	low/mid	low	High	mid	low/mid
Perceived benefit of success	high	High	mid/high	High	low
Probability of Action (PoA)	12%	15%	40%	5%	7%
Threat Event Probability (TEP) in percentage = (PoC * PoA)					
loss event	Unauthorized access to applicant data	Financial fraud (unauthorized transactions)	Denial of service (website unavailable)	Data corruption or loss	Reputational damage
CIA impact breach	Confidentiality	integrity	availability	integrity	Confidentiality
Attacker	Organized Crime	Organized Crime	Script kiddie	Expelled Student	Expelled Student

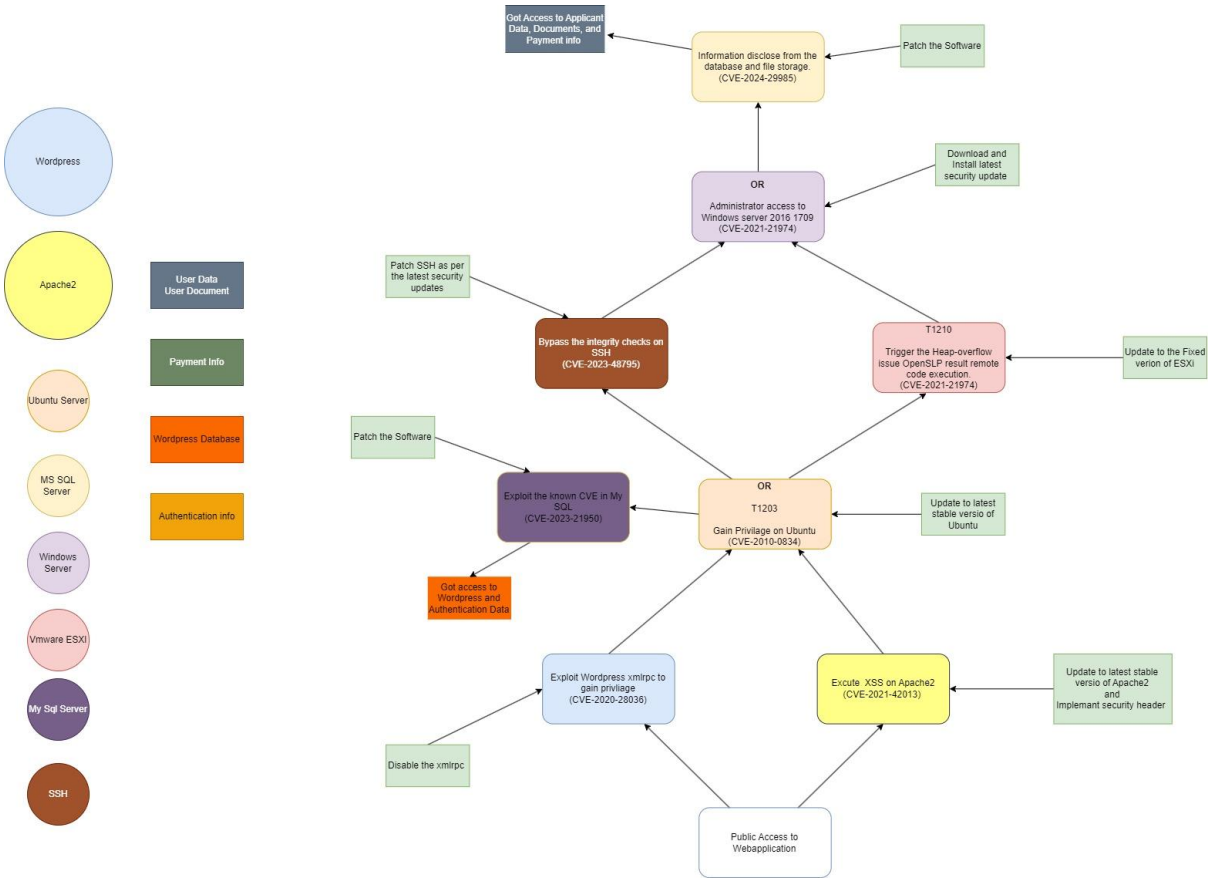
Phase 4 - Vulnerability Identification and Attack Graph Development

Step 1: List Vulnerabilities

Assets	**Version**	**Severity**	**Notes**	**CVE'S Score**	**Potential CVE's**
Ubuntu Server	10.04 LTS	Critical	Resource Management Errors, Use of Unmaintained Third-Party Components, Code Injection	9.8-10	CVE-2010-0834
VMWare ESXi	6.7	High	Improper Input Validation	7.5-8.9	CVE-2021-21974
Windows Server 2016	1709	High	Improper Privilege Management	7.5-8.9	CVE-2018-0751

Apache2	2.4.50	Medium - High	Improper Input Validation, Path Traversal, Cross-site Scripting	4.3-8.6	CVE-2021-42013
MySQL Server	8.0.27	High	SQL Injection	7.5-8.9	CVE-2023-21950
WordPress	5.5.2	Critical	SQL Injection, Path Traversal, Improper Input Validation, Unrestricted Upload of File with Dangerous Type, Improper Authentication	9.8-10	CVE-2020-28036
Plugins	3.21.0	Varies (High to Critical)	Vulnerable Plugin version		
Themes		High	SQL Injection	7.5	
			LDAP Injection	7.5	
		High	OS Command Injection	7.5	
		High	Improper Input Validation	8.8	
		High	XML-RPC is enabled	7.5-8.9	
		High	WordPress Cron Enabled	7.5-8.9	
MS SQL Server 2019 CU25+GDR		High	Remote Code Execution	7.7-8.8	CVE-2024-29985
SSH	9.6	High	bypass integrity checks	2.2-5.9	CVE-2023-48795

Attack Graphs



Phase 5 - Risk assessment and recommendations