GROUP MEMBERS.

AINAMAANI ISAAC	21/U/1058
SERUNJOGI HUZAIFA	21/U/07918/EVE
WAMIMBI RONALD	21/U/0688
PAPA JAMES BORN EMUSUGUT	21/U/08338/EVE
MATSIKO AMON	21/U/04593/EVE

QUESTION THREE.

a)

Threat modeling is a systematic approach to identifying and addressing potential security risks in a software application. In the context of our job portal software project, this is how we are going to follow and use the steps in the threat modeling process.

1. **Identify Assets:**

This step involves defining the key assets of your system. In the case of our job portal, these might include user data, job listings, user credentials, and communication channels.

2. **Create an Architecture Overview:**

This entails developing an architectural overview of your system, highlighting the key components, interactions, and data flows. This includes user interfaces, databases, servers, and communication protocols.

3. **Decompose the Application:**

This has breaking down the application into its individual components and modules. For our job portal, this could involve user authentication, job posting, job viewing, and communication functionalities.

4. **Identify Threats:**

Here, we consider potential threats to each component and the system as a whole. Threats could include unauthorized access, data breaches, denial of service attacks, and more. Specifically for our case, a job portal, we will be concerned about fake job postings, identity theft, or SQL injection attacks.

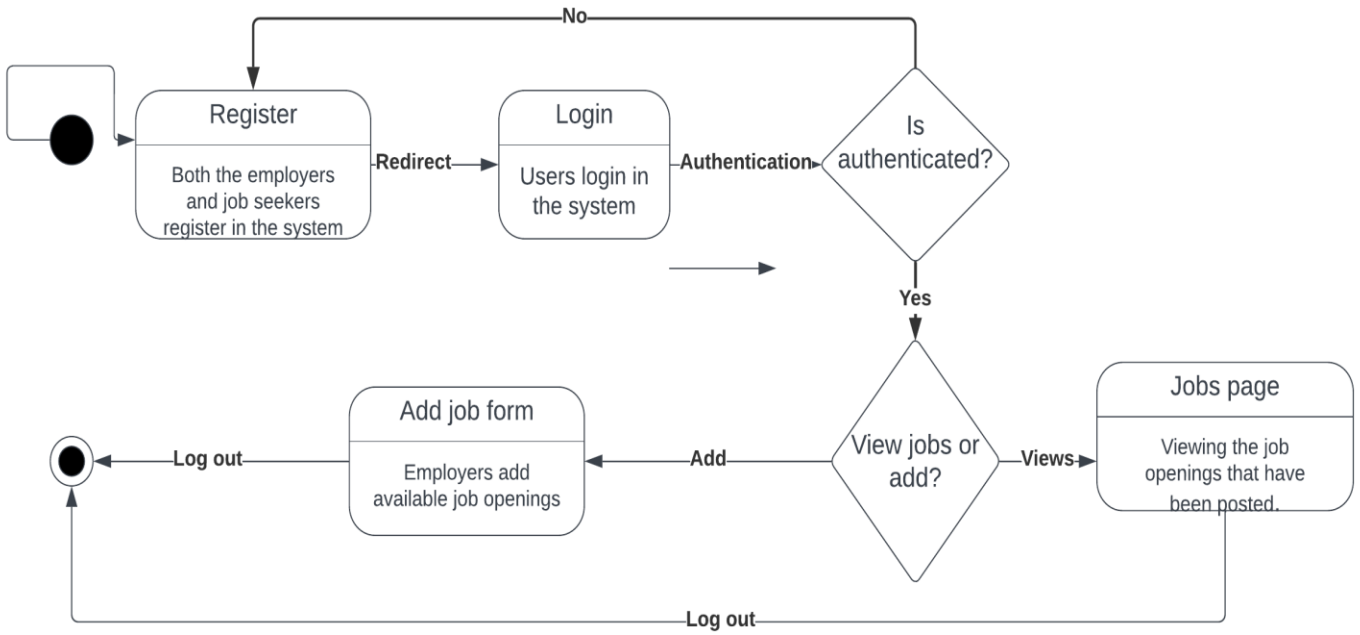
5. **Document the Threats:**

This involves creating a comprehensive list of identified threats. We will document the details of each threat, including the affected components, potential vulnerabilities, and the likelihood of exploitation. For example, we will document a threat related to insufficient input validation in the job posting module.

6. **Rate the Threats:**

This typically involves assessing the severity of each threat by considering the potential impact and likelihood of occurrence. We will use a rating system to prioritize which threats need immediate attention as high-risk threats may require more robust security measures.

b)



Using the simple basic diagram above, we identify critical areas to be.

i. User authentication
ii. Job posting
iii. User credentials storage
iv. Communication channels

Under each area we identify various threats for example under the User authentication, we identify credential theft and brute force attacks threats, under the job posting area we identify the fake job posting and SQL injection attacks, under the user credentials storage(database), we have the credential theft, unauthorized access to personal information, Insecure Direct Object References (IDOR) and then under the communication channels for example from the application to the server, we have the man in the middle attack threat and the data interception threat.

i) The DREAD model stands for Damage, Reproducibility, Exploitability, Affected Users, and Discoverability, and it is a method for evaluating the severity of a threat.

The critical threats to be rated by DREAD are SQL injections, fake job posting, credential theft.

SQL injection attack

D-3, R-3, E-3, A-3, D-2

Fake job postings

D-3, R-3, E-3, A-3, D-3

Credential theft

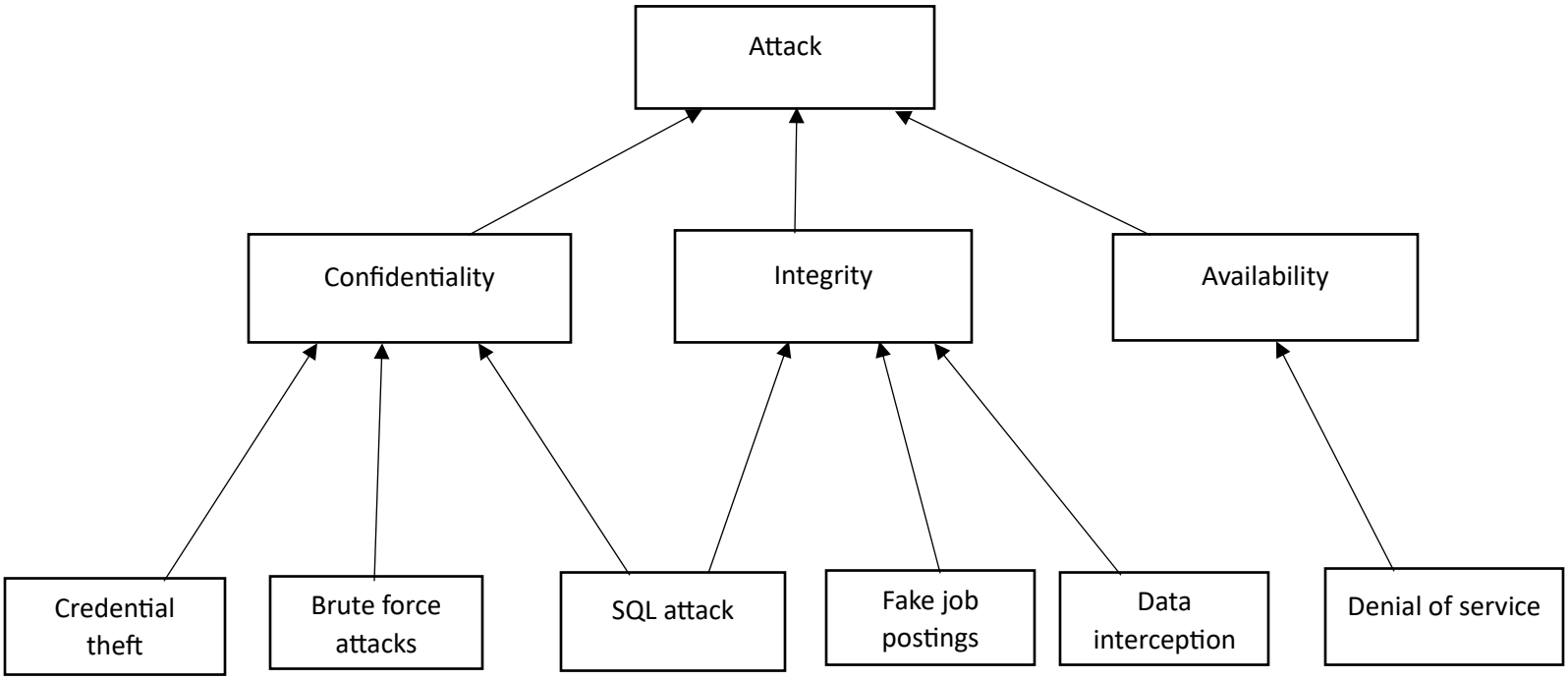
D-2, R-2, E-1, A-2, D-3

A table to show the DREAD rating for all the threats.

Threats	**D**	**R**	**E**	**A**	**D**	**Total**	**Rating**
SQL Injection attack	3	3	3	3	2	14	High
Fake job postings	3	3	3	3	3	15	High
Credential theft	2	2	1	2	3	10	Medium

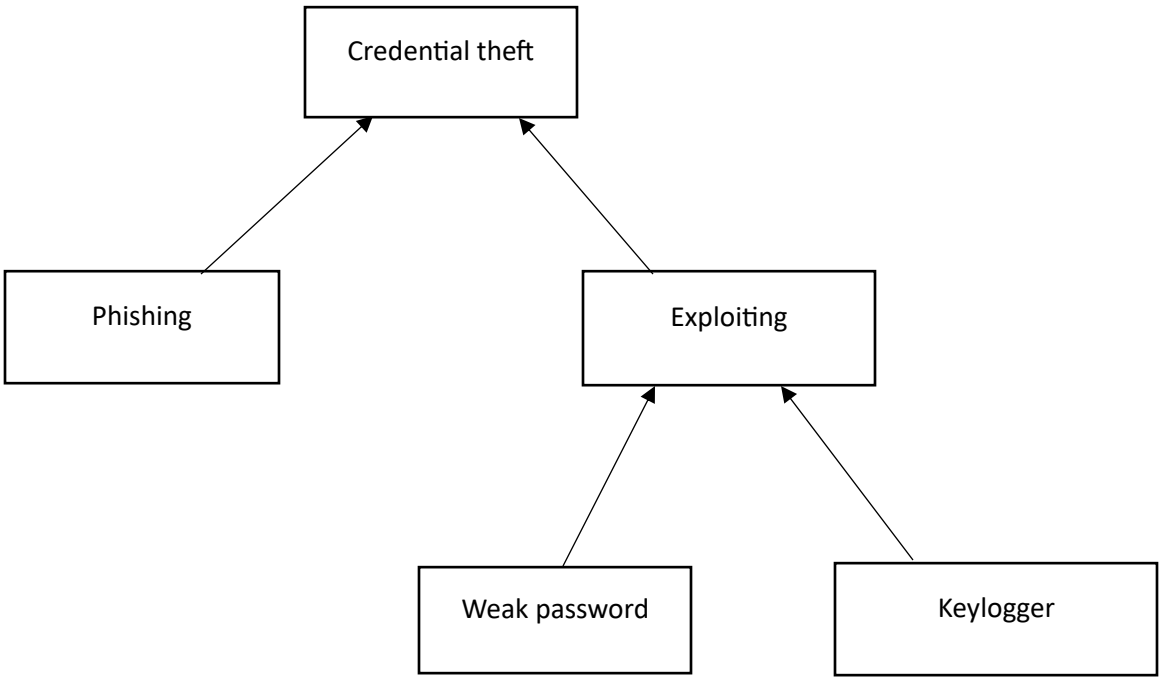
ii) Identifying critical threats using threat trees

Below is a broad overview of the possible threats on our system.

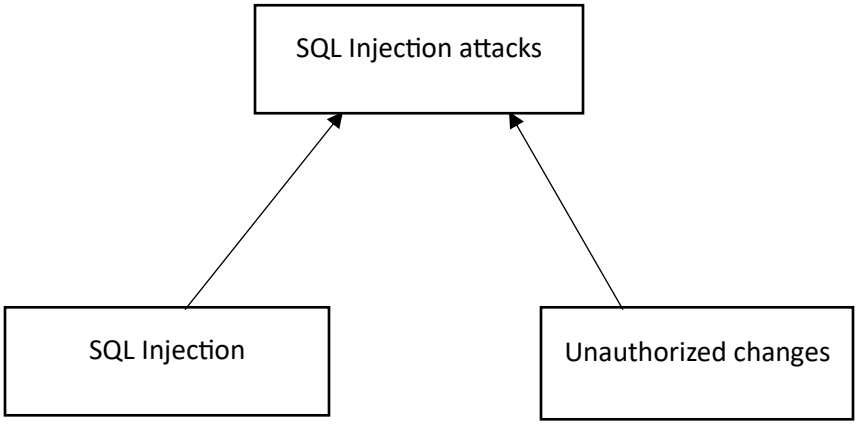


Below is a further breakdown of some of the attacks identified.

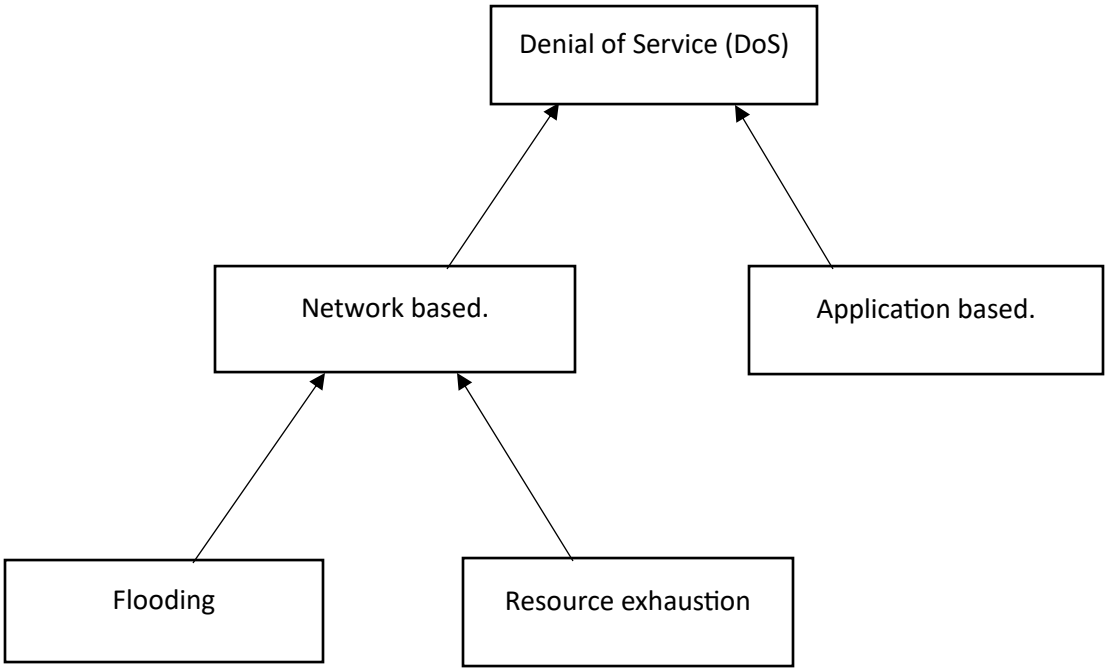
Credential theft



SQL Injection attacks



Denial of Service for the job seekers and employers/recruiters.



iii) identify the critical threats using STRIDE

STRIDE is a threat modeling framework that stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Let's apply STRIDE to the identified threats in the Jobs portal project.

S – **Spoofing**

Credential Theft (User Authentication):

Spoofing is a concern here as attackers could impersonate legitimate users if credentials are stolen.

T- **Tampering**

SQL Injection Attacks (Job Posting):

Tampering is a significant threat as SQL injection attacks can manipulate or tamper with the job posting database, leading to unauthorized changes.

R- **Repudiation**

Adding fake job postings and denying it.

I- **Information Disclosure**

Exposing user credentials along the job postings they made

D- **Denial of service**

Flooding the server with very many requests leading to the employers and job seekers not being able to access the system.

E- **Elevation of Privilege**

Being able to add a job posting yet you don’t have the employer privileges.