**Scenario:**

You are building a secure website that will be used by a recruitment firm. Users will securely upload and download user information and CVs documents.

The website will have the following features and functionality:

* User registration, authentication, and authorisation/access controls (see Sections 3 and 4)
* File upload, file sharing and downloads in a secure manner (see Sections 4, 5 and 6)
* Logging (see Section 7).

**Section 1**

**Identify Threats and Possible Exploits (KU1.3, 5 marks)**

Identify at least 2 assets and at least 2 threats to the website to be developed. Use the templates in Appendix A and write appropriate documentation to:

* identify at least 3 trust levels (1 mark)
* identify at least 2 assets (2 marks)
* identify at least 2 threats related to the identified assets (2 marks)

**Note:** The marks for the mitigation strategy are awarded in Section 2.

**Note:** You need to identify your own assets; and threats. Using the assets; and threats in the sample documentation do not count towards the limit.

**Note:** You may use relevant trust levels in the appendix if the trust levels are correct for the identified assets and threats.

**Trust Levels:**

|  |  |  |
| --- | --- | --- |
| Id | Name | Description |
| T1 | Remote Anonymous User | A user who has not yet authenticated to the website |
| T2 | Generic User | A registered user with valid credentials |
| T3 | Manager | User who can review and manage job applications & CV’s |
| T4 | Admin | A user who can configure the website. |
| T5 | IT Employee | A user responsible for technical maintenance & support |
| T6 | Employer | A user who can maintain job postings and review CV’s |

**Assets:**

|  |  |  |  |
| --- | --- | --- | --- |
| Id | Name | Description | Trust Level |
| A1.1 | User’s login Credentials | User’s username & password | T2 – Generic User  T3 – Manager  T4 – Admin  T5 – IT Employee  T6 - Employer |
| A1.2 | User Personal Information | Personal data pertaining to the user such as name, email, phone number, etc. | T2 – Generic User  T3 – Manager  T4 – Admin  T5 – IT Employee  T6 - Employer |
| A1.3 | Uploaded CV’s & Documents | CV’s & Documents uploaded by the users | T2 - Generic User  T3 - HR Manager  T6 - Recruiter |
| A1.4 | Job Postings Data | Information about job postings including job description, requirements, etc. | T4 - Website Admin  T6 - Employer |

**Threats:**

|  |  |
| --- | --- |
| Id | TR1 |
| Name | Unauthorised File Access |
| Description | An attacker accesses or modifies uploaded CV’s and documents without permission |
| STRIDE | Tampering, Information Disclosure |
| Entry Points | File upload/download page |
| Assets | A1.3 - Uploaded CV’s & Documents |
| Mitigation Strategy | Implement file access controls, Use encryption, Secure file storage |

|  |  |
| --- | --- |
| Id | TR2 |
| Name | Malicious File Upload |
| Description | An attacker uploads a file containing malicious code (E.g. a script or executable) |
| STRIDE | Tempering, Information Disclosure, Elevation of Privilege. |
| Entry Points | File upload page |
| Assets | A1.3 - Uploaded CV’s & Documents |
| Mitigation Strategy | Validate file types, restrict file execution permissions, sanitise filenames |

|  |  |
| --- | --- |
| Id | TR3 |
| Name | Modification to Job Posting Data |
| Description | An attacker attempts to modify job postings, altering descriptions, requirements, etc. |
| STRIDE | Tempering, Elevation of Privilege. |
| Entry Points | Admin Control panel |
| Assets | A1.4 - Job Postings Data |
| Mitigation Strategy | Implementing Role Based Access Control (RBAC), Input validation. |

**Section 3**

**Identify Threats and Possible Exploits (AA2.1, 7 marks)**

User input should be validated properly. Use data annotations in the model to validate user input and the ModelState.IsValid check. Show, using screenshots your use of:

• A Data Annotation that makes sure that the file extension is of an appropriate type (you require to create a custom annotation for this). This custom annotation will take comma separated values of valid extension files. (2 marks).

Custom annotation created:

A computer screen shot of a program

Description automatically generated

Custom annotation being used:

A computer screen shot of a program code

Description automatically generated

• Use the data annotation implemented to verify that uploaded documents have one of the following extensions: “.docx” or “.pdf”. The Action that receives the document to be uploaded will use IsValid to verify that the file has the correct extension before processing the file (1 mark).

Using custom annotation, using IsValid to check it.

A computer screen with text

Description automatically generated