**On**l**ine Shopping System Proposal**

**Introduction: 250 words // current: 162 words**

Due to its rapid expansion, and the large catchment area which it serves, our consultancy firm “Edney CyberSec Ltd” proposes the use of an Online Shopping System to assist the owner of “Colchester Groceries” with their business. The system will be a web application written in Python, and use SQL to securely store user information and the inventory for the business. It is vital to take into account the owner’s concerns of the high rate of cybercrime and the government’s policy on data protection. This report will first give an overview of the Online Shopping System and use a UML use case diagram to demonstrate it’s functionality. In the second section we will explore the security threats, using STRIDE and a “misuse case” diagram to highlight the areas of interest for a malicious user or hostile actor. The final section details how Edney CyberSec Ltd will mitigate the identified threats, and alleviate the concerns of the owner regarding data protection and cybercrime.

**Overview: 500 words**

A top level overview of the proposed system. This section will use a UML use case diagram to demonstrate the functionality of the system. Each actor will be explained and how they interact with the system.

A diagram of a diagram

Description automatically generated

**Fig 1: Online Shopping System Use Cases**

A sequence diagram may also be used to show the order of events, and highlight how no action can be carried out without being authenticated first.

A diagram of a diagram

Description automatically generated

**Fig 2: Online Shopping System Sequence Diagram**

**Security Threats: 500 words**

This section will explain the identified threats. A brief overview of potential threats will be given via STRIDE.

* **S**poofing – Pretending to be a legitimate user. Achieved via social engineering or brute forcing passwords.
* **T**ampering – Attempting to modify values in the database (i.e prices of stock).
* **R**epudiation – No threat identified.
* **I**nformation Disclosure – Finding users PII (personally identifiable information) such as email address or payment details.
* **D**enial of Service – Loss of access to the system.
* **E**levation of privilege – Attempting to gain access to the admin area of the system.

A “misuse case” diagram will also be used to show the potentially vulnerable points in the application.

**A diagram of a diagram

Description automatically generated**

**Fig 3: Misuse Diagram**

**Mitigation Techniques: 500 words**

This section will explain how our company will mitigate these threats and what measures will be implemented. The shop owners main concern is that of data protection. An attack tree will be used to show how a data breach may happen.

A diagram of data engineering

Description automatically generated

**Fig 4: Data Breach Attack Tree**

Brute forcing and social engineering are reoccurring items on the attack tree. Therefore it would be necessary to emphasise the secure authentication mechanism that we would have in place. A flow chart will be used to explain the login system and how we will avoid a malicious user from brute forcing someone’s account. Furthermore, we can explain how we would implement password hashing and multi factor authentication.

A diagram of a flowchart

Description automatically generated

**Fig 4: Login Flow Diagram**

**Conclusion: 250 words**

This last section will tie together the ideas from the overview, threats identified and mitigation sections.

**References**