**ONLINE SHOPPING SYSTEM REPORT**

**INTRODUCTION**

The Internet has revolutionised commerce, offering constant consumer access and lower retail overheads (Yell, 2019). In 2024, 20.1% of retail transactions are expected to occur online (Snyder, 2024). For these reasons, “Edney CyberSec Ltd” proposes using an online shopping system to assist “Colchester Groceries” in managing its large catchment area and expanding business.

This report is in three distinct sections. It will detail the design of the online shopping system and address the owner’s concerns about cybercrime and the government's policy on data protection. The first section provides an overview of the online shopping system and its benefits, using various diagrams to showcase its functionality. The second section explores security threats, using threat modelling to highlight the areas of interest for a malicious user or hostile actor. Using the findings from the threat modelling, the final section details how Edney CyberSec Ltd will mitigate the identified threats and alleviate the owner's concerns on cybercrime and the government’s policy on data protection.

**OVERVIEW**

An online shopping system is the ideal solution for Colchester Groceries to manage its growing business needs. E-commerce enables twenty-four hour access to the business for customers, and for the owner of Colchester Groceries, increasing their consumer-facing presence leads to increased profitability.

The proposed system will be a web application written in Python using the Flask framework, chosen for its lightweight nature and flexibility and, as such, allowing expansion of the shopping system at a later date (Zammetti, 2024). Although other frameworks like Django have more built-in tools, Flask is still able to access databases and use authentication and authorisation due to its available extensions (Farrell, 2023).

A diagram of a diagram

Description automatically generatedA UML “use case” diagram graphically represents how users interact with the system (Stephens, 2023). Figure 1 is such a diagram, showing the online shopping system, the identified use cases and the two types of user. The first type is the customer, who can either be a new or registered user. The second type is the owner, who, as the site's administrator, has their own set of use cases.

*Figure 1: Online Shopping System Use Cases*

This delineation of user roles prevents customers from performing unauthorised actions and complies with the principle of “least privilege”, which controls a user's access to an application (Plachkinova, 2023). Proper authorisation is vital to protect customer data and avoid exfiltration (Microsoft, N.D) and will therefore assist with the shop owner’s concerns regarding the government’s policy on data protection.

To use the system, customers must first register an account. This will enable them to log in, browse the inventory, and add items to their basket. Once the items have been added to the basket, customers will proceed to the payment system, which will be provided by a thoroughly vetted third-party, to pay for their goods. After the payment is complete, the owner will receive the order and process it. Additionally, the owner can manage the inventory and its database through an administrative console.

**A diagram of a data flow

Description automatically generated**This logic is replicated in Figure 2, a class diagram representing the online shopping system. A class diagram details the attributes of each object in the system and potential functions, along with the relationships between them. They are essential when designing and documenting an object-oriented system and its components (Rouabhia, 2024), due to mapping directly to Python and creating consistent structure (LucidChart, N.D.).

*Figure 2: Online Shopping System Class Diagram*

Overall, the Internet is a near-perfect platform for the online shopping system. E-commerce provides customers with twenty-four hour access to the business, and the business itself with a more extensive potential consumer base, thereby increasing Colchester Groceries’ profitability. The separated user roles allow a simple yet multi-faceted web application that satisfy the needs of both the customer and the shop owner. However, it is still necessary to understand the shortcomings of such a platform and not take the system's security for granted. The following sections will analyse the security threats and mitigation techniques used in the proposed online shopping system.

**SECURITY THREATS**

The owner's concerns about cybercrime and data protection are well-justified. All EU General Data Protection Regulation (GDPR) provisions have been directly incorporated into UK law (ICO, N.D.), meaning failing to comply with GDPR will result in substantial fines (European Parliament, 2021). Every retailer must ensure their systems are adequately developed and secured. Failure to do so will quickly lead to a decrease in market value and consumer trust, as can be seen in 2024 when Greggs suffered a “technical glitch” (Duell, 2024).

The Microsoft developed STRIDE is one of the most popular techniques for threat modelling and stands for **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, and **E**levation of Privilege (OWASP, N.D.). Hartman (2024) provides the meanings of each category below:

* **Spoofing –** An attacker may hide their identity by pretending to be another user or system. This can lead to unauthorised transactions and financial theft.
* **Tampering -** This is the modification of a system with malicious intent. Stock prices or even consumer details may be changed.
* **Repudiation -** This is the ability to deny having performed an action. For example, a customer may say they never authorised a transaction.
* **Information Disclosure –** An area of concern for the owner, this is the leakage of data that other users may not have the authority to view.
* **Denial of Service -** An attacker uses normal business processes to consume a system’s resources, rendering it unavailable for legitimate users. This negates one of the most significant benefits of the online shopping system.
* **Elevation of Privilege -** This is when an attacker may be able to escalate their control of a system, for example, by granting themselves administrative rights.

Another threat modelling technique commonly used with STRIDE is “DREAD”, which analyses the likelihood and severity of threats, ranking them numerically, and is similar to a risk assessment (Yokoyama, 2023). DREAD stands for **D**amage Potential, **R**eproducibility, **E**xploitability, **A**ffected Users, and **D**iscoverability (Ingeno, 2018). This report will first analyse the potential threats in Table 1 using STRIDE.

|  |  |
| --- | --- |
| Threat Category | Potential Threat |
| Spoofing | An attacker may pretend to be a legitimate user of the online shopping system or an administrator. |
| Tampering | An attacker may modify values in a database, such as user passwords or prices of items. |
| Repudiation | A user may deny having performed an action, claiming their session was hijacked, or they didn’t authorise a transaction. |
| Information Disclosure | An attacker may find a user’s PII (personally identifiable information), such as email addresses or bank details. |
| Denial of Service | An attacker may be able to take down the system, thereby reducing commerce. |
| Elevation of privilege | An attacker may gain administrative privileges to the online shopping system. |

*Table 1: Online shopping system threats as per STRIDE*

The potential threats are then ranked on a severity of 1 to 3 ( 1 – low, 2 – medium, 3 – high). An average score is taken for each threat. This will produce a DREAD risk assessment, as shown in Table 2.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **D** | **R** | **E** | **A** | **D** | **Average Score** |
| **S** | 2 | 2 | 2 | 1 | 2 | **1.8** |
| **T** | 3 | 1 | 1 | 3 | 1 | **1.8** |
| **R** | 1 | 1 | 1 | 1 | 1 | **1** |
| **I** | 3 | 2 | 1 | 3 | 2 | **2.2** |
| **D** | 3 | 1 | 1 | 3 | 1 | **1.8** |
| **E** | 3 | 1 | 1 | 2 | 1 | **1.6** |

*Table 2: DREAD Threat Model*

In the DREAD model, Information Disclosure has the highest average score, which corresponds with the owners concerns about the government’s policy on data protection. Failure to protect a consumer’s PII (personally identifiable information) can lead to fines or reputational damage, as can be seen by the data leak of 23andMe users who are now being investigated by the ICO (Rahman-Jones, 2023).

Various threat modelling techniques may be used when developing the online shopping system. The simplicity of STRIDE is adequate for this online shopping system, however should the system grow more complex a model such as PASTA would be recommended (Azam, 2023).

A diagram of data engineering

Description automatically generatedTo gain a greater understanding of how a data breach can occur, an attack tree can be used. An attacker's potential objective is at the top of the tree, and the branches are the means of achieving that objective (Tidmarsh, 2023). Figure 3 identifies two methods for an attacker to cause a data breach: brute-forcing and socially engineering passwords, or information disclosure from a database. The following section will explore mitigation techniques based on the threat modelling used.

*Figure 3: Data Breach Attack Tree*

**THREAT MITIGATION STRATEGIES**

As Deogun (2018) states, “Security is a concern, not a feature,” meaning a programmer must not take a reactive approach to security. Security must be properly implemented during the design phase. McGraw agrees with this sentiment. They have advocated for a *proactive* approach to security design as far back as 1998, due to most security violations stemming from poor coding and development practices (Williams, 2019). Although the threat list in the above STRIDE/DREAD model is not exhaustive, it will still enable the development of mitigation strategies for potential threats, effectively securing the online shopping system.

The first measure that needs to be implemented is secure session management. This is vital in negating a potential spoofing attack (McDonald, 2024) and will be enforced via a robust log-in mechanism. Figure 4 is a flow diagram demonstrating the proposed system’s log-in procedure.

To use the system, a user must first supply their credentials. The online shopping system will check these credentials against a database. If the credentials exist, the user can access the online shopping system. If not, they have three attempts to supply the correct credentials. Failure to supply correct credentials after three attempts will lock out their account. Once the user has been successfully verified, using a random, unguessable number as a session-id cookie will protect their session (Singh, 2020).

A diagram of a flowchart

Description automatically generated

*Figure 4: Login Mechanism Flow Diagram*

This system's benefit is its ability to prevent brute-forcing passwords. As per the previous section’s threat modelling, social engineering is another threat that could lead to a data breach. To prevent this, a multi-factor authentication mechanism can be provided. The customer may be sent a PIN via text to verify their identity. This can be implemented through the various available Python modules (Adedeji, 2023). Although multi-factor authentication increases the system's complexity for both the developer and the customer, verifying the correct user will reduce the risk of spoofing and repudiation threats (IBM, 2024).

SQL injection is another threat identified that may cause a data breach. SQL injection is the technique used to input arbitrary code into an application, with one outcome being potentially revealing information. This type of threat accounts for approximately 65.1% of online attacks (Galluccio, 2020). It is stopped through secure coding, with the user unable to enter any characters that will cause an SQL injection attack. Not only does this prevent information disclosure, but it will stop a malicious user’s arbitrary code from tampering with the databases.

The final method Edney CyberSec Ltd will implement to prevent a data breach and protect user data is “hashing” the data in the databases. Hashing is a function that consistently transforms a variable-length input into a fixed-length output (Chapple, 2024). It is irreversible, so if an attacker has managed to gain access to the databases, they will not know the values of the data. This will significantly reduce the risk of Information Disclosure.

The use of secure coding and log-in procedures, along with session management and multi-factor authentication provide “defence in depth” to the online shopping system (Olmsted, 2024). This will reduce the possibility of cybercrime and a data breach, consequently alleviating the owner’s concerns.

**CONCLUSION**

This report has proposed using an online shopping system to help Colchester Groceries with its increased business. Using an online shopping system will increase the customer’s access to the company, consequently increasing Colchester Groceries’ profitability. The owner is concerned about cybercrime and the Government’s policy on data protection. Edney CyberSec Ltd has identified potential threats through threat modelling and will use methods such as hashing, multi-factor authentication, and cookies to prevent attacks. This will avoid the possibility of a data breach and reduce the risk of cybercrime, alleviating the owner’s two primary concerns about using an online shopping system.

**References**

* Adedeji, O. (2023). *Full-Stack Flask and React: Learn, Code, and Deploy Powerful Web Applications with Flask 2 and React 18* (1st ed.). Packt Publishing, Limited. Available from: <https://learning.oreilly.com/library/view/full-stack-flask-and/9781803248448/B18554_FM.xhtml> [Accessed 01 July 2024].
* Azam, N. et al. (2023) Data Privacy Threat Modelling for Autonomous Systems: A Survey From the GDPR’s Perspective. *IEEE transactions on big data* 9 (2): 388–414. DOI: 10.1109/TBDATA.2022.3227336
* Chapple, M. (2024) *CC Certified in Cybersecurity Study Guide.* 1st ed. Newark: John Wiley & Sons, Incorporated. Available from: <https://learning.oreilly.com/library/view/cc-certified-in/9781394213832/> [Accessed 01 July 2024].
* Deogun, D. et al. (2018) *Secure by design*. 1st edition. Shelter Island, New York: Manning. Available from: <https://ebookcentral.proquest.com/lib/universityofessex-ebooks/reader.action?docID=6642757&ppg=1> [Accessed 26 June 2024].
* Duell, M. (2024) Greggs IT glitch wipes £40million off the bakery chain’s value after tills went down for two hours – as cyber attack on its 2,500 stores is ruled out. Available from: <https://www.dailymail.co.uk/news/article-13218689/Greggs-company-value-technical-problem.html> [Accessed 30 June 2024].
* European Parliament. No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> [Accessed 03 May 2024].
* Farrell, D. (2023) *The Well-Grounded Python Developer: How the Pros Use Python and Flask*. 1st edition. New York: Manning Publications Co. LLC. Available from: <https://learning.oreilly.com/library/view/the-well-grounded-python/9781617297441/> [Accessed 01 July 2024].
* Galluccio, E. et al. (2020) *SQL Injection Strategies: Practical Techniques to Secure Old Vulnerabilities Against Modern Attacks*. 1st edition. Birmingham: Packt Publishing, Limited. Available from: <https://learning.oreilly.com/library/view/sql-injection-strategies/9781839215643/> [Accessed 30 June 2024].
* Ghimire, D. (2020) Comparative Study on Python Web Frameworks: Flask and Django. Available from: <https://www.theseus.fi/bitstream/handle/10024/339796/Ghimire_Devndra.pdf?sequence=2&isAllowed=y> [Accessed 21 June 2024].
* Hartman, S. (2024) *Hands-On Ethical Hacking Tactics : Strategies, Tools, and Techniques for Effective Cyber Defense*. First edition. Birmingham, England: Packt Publishing Ltd. Available from: <https://learning.oreilly.com/library/view/hands-on-ethical-hacking/9781801810081/> [Accessed 28 June 2024].
* IBM. (2024) Multi-Factor Authentication (MFA). Available from: <https://www.ibm.com/docs/en/cics-ts/6.x?topic=cics-multi-factor-authentication-mfa> [Accessed 28 June 2024].
* ICO. (N.D.) Overview – Data Protection and the EU. Available from: <https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/#:~:text=The%20EU%20GDPR%20is%20an,law%20as%20the%20UK%20GDPR>. [Accessed 29 June 2024].
* Ingeno, M. J. (2018) *Software architect’s handbook : become a successful software architect by implementing practical architecture concepts*. 1st edition. Birmingham ; Packt Publishing. Available from: <https://learning.oreilly.com/library/view/software-architects-handbook/9781788624060/> [Accessed 25 June 2024].
* Jensen, J. et al. (N.D.) *Experimental Threat Model Reuse with Misuse Case Diagrams, Information and Communications Security*. Berlin, Heidelberg: Springer Berlin Heidelberg. Available from: <https://link-springer-com.uniessexlib.idm.oclc.org/chapter/10.1007/978-3-642-17650-0_25> [Accessed 28 June 2024].
* LucidChart. (N.D.) Introduction to Class Diagrams. Available from: <https://www.lucidchart.com/blog/introduction-to-class-diagrams> [Accessed 1 July 2024].
* Luhach, A. K. (2021) *Advanced Informatics for Computing Research : 4th International Conference, ICAICR 2020, Gurugram, India, December 26–27, 2020, Revised Selected Papers, Part I*. Singapore: Springer Nature Singapore. DOI: https://doi.org/10.1007/978-981-16-3660-8
* McDonald, M. (2024) *Grokking Web Application Security.* 1st ed. New York: Manning Publications Co. LLC. Available from: <https://learning.oreilly.com/library/view/grokking-web-application/9781633438262/> [Accessed 28 June 2024].
* Microsoft. (N.D.) What is Authentication? Available from: <https://www.microsoft.com/en-gb/security/business/security-101/what-is-authentication> [Accessed 27 June 2024].
* Olmsted, A. (2024) *Security-Driven Software Development : Learn to Analyze and Mitigate Risks in Your Software Projects*. First edition. Birmingham, England: Packt Publishing Ltd. Available from: <https://learning.oreilly.com/library/view/security-driven-software-development/9781835462836/> [Accessed 28 June 2024].
* OWASP. (N.D.) Threat Modelling Cheat Sheet. Available from: <https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html> [Accessed 22 June 2024].
* Plachkinova, M. & Knapp, K. (2023) Least Privilege across People, Process, and Technology: Endpoint Security Framework. *The Journal of computer information systems* 1–13. DOI: 10.1080/08874417.2022.2128937
* Rahman-Jones, I. (2024) Genetic Testing Firm 23andMe Investigated Over Hack. Available from: <https://www.bbc.co.uk/news/articles/c3gg17pq5y9o> [Accessed 30 June 2024].
* Rouabhia, D. & Ismail Hadjadj (2024) Enhancing Class Diagram Dynamics: A Natural Language Approach with ChatGPT. *arXiv.org*. DOI: 10.48550/arxiv.2406.11002
* Singh, T. & Meenakshi (2020) Prevention of session hijacking using token and session id reset approach. *International journal of information technology* 12 (3): 781–788. DOI: 10.1007/s41870-020-00486-w
* Snyder, K. (2024) 33 E-Commerce Statistics for 2024. Available from: <https://www.forbes.com/uk/advisor/business/ecommerce-statistics/#:~:text=E%2Dcommerce%20sales%20are%20expected%20to%20grow%208.8%25%20in%202024> [Accessed 30 June 2024].
* Stephens, R. (2023) *Beginning software engineering*. Second edition. Hoboken, New Jersey: John Wiley & Sons, Inc. Available from: <https://learning.oreilly.com/library/view/beginning-software-engineering/9781119901709> [Accessed 28 June 2024].
* Tidmarsh, D. (2023) What You Need to Know About Attack Trees. Available from: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/attack-trees-cybersecurity/#:~:text=They%20help%20security%20professionals%20comprehend,to%20enter%20an%20IT%20system>. [Accessed 27 June 2024].
* Williams, L. (2019) Secure Software Lifecycle Knowledge Area. Available from: <https://www.cybok.org/media/downloads/Secure_Software_Lifecycle_issue_1.0.pdf> [Accessed 26 June 2024].
* Yokoyama, R. & Arima, C. H. (2023) Application of the Threat Modeling Method In an Operating System. *GeSec : Revista de Gestão e Secretariado* 14 (4): 5102–5122. DOI: 10.7769/gesec.v14i4.1645
* Yell. (2019) How an Online Store Benefits Your Business. Available from: <https://business.yell.com/insights/e-commerce/what-are-the-benefits-of-an-online-store-for-businesses/> [Accessed 30 June 2024].
* Zammetti, F. W. (2024) *Web Development Career Master Plan : Learn What It Means to Be a Web Developer and Launch Your Journey Toward a Career in the Industry.* 1st ed. Birmingham: Packt Publishing, Limited. Available from: <https://learning.oreilly.com/library/view/web-development-career/9781803247083/> [Accessed 28 June 2024].