Securing the Stack: SQL Injection Vulnerabilities and Defensive Strategies
(Technical Topic)

Ethical Horizons in Cybersecurity Education: Balancing Technical Skills with Social Responsibility
(STS Topic)

A Thesis Project Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Michael Park

Fall, 2024

Technical Project Team Members: Jared Conway, Lilli Hrncir, Sami Kedir

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signature _____Michael Park_____

Approved _____William Davis_____ Date ____12/7/2024____

William Davis, Assistant Professor of STS, Department of Engineering and Society

Approved _____Nada Basit_____ Date _____5/9/2025_____

Nada Basit, Associate Professor, Department of Computer Science

I. Overall Introduction

In April 2024, security researchers Ian Carroll and Sam Curry uncovered a critical SQL Injection (SQLi) vulnerability in FlyCASS, an airline system responsible for managing Known Crewmember (KCM) and Crew Access Security System (CASS) processes. These systems play crucial roles in aviation security, including verifying crewmember identities and determining security clearance for accessing restricted areas, such as commercial airline cockpits. The SQLi vulnerability allowed malicious actors to inject unvalidated SQL commands into the system's database queries, potentially bypassing Transportation Security Administration (TSA) protocols. Exploiting this flaw could grant unauthorized individuals access to sensitive information or even permit physical access to highly secure locations, posing a severe risk to passenger safety and national security.

SQLi is one of the most dangerous and widely known web application vulnerabilities, where attackers manipulate improperly sanitized user inputs to execute arbitrary SQL commands. These commands can be used to exfiltrate sensitive data, modify databases, or escalate privileges. Despite being one of the most well-documented attack vectors, SQLi remains alarmingly prevalent due to insufficient developer training and poor coding practices. Developers and students often lack hands-on experience with SQLi vulnerabilities, leaving them ill-equipped to understand how such attacks exploit flawed database queries or how to implement proper safeguards, such as parameterized queries and input validation.

This research aims to address the critical gap between theoretical knowledge of SQLi vulnerabilities and practical defense strategies by creating an interactive, educational platform. The project investigates how experiential learning—where participants actively engage with simulated SQLi attacks and defensive coding techniques—can enhance understanding of SQLi mechanics and improve secure coding practices. By equipping developers and students with both theoretical foundations and practical skills, this research contributes to reducing the risks of SQLi attacks in real-world applications, ultimately fostering a more secure digital environment.

II. Technical Topic

My project focuses on creating an interactive website to educate users on SQL injection (SQLi) vulnerabilities and defense strategies through 12 modules of hands-on challenges. SQLi attacks occur when attackers manipulate user inputs to alter database queries, potentially granting unauthorized access to sensitive data. These vulnerabilities represent a significant risk for organizations across various industries, as illustrated by incidents like the 2017 Equifax breach, which exposed millions of users' information and led to severe financial and reputational damage (Equifax, 2017). Such cases underscore the urgent need for effective SQLi prevention strategies, yet many developers lack hands-on experience in recognizing and addressing these vulnerabilities (CWE/SANS, 2024). My project aims to fill this gap by providing a secure, interactive module that immerses users in realistic SQLi scenarios, helping them build essential skills to tackle these risks.

The motivation for this project stems from a notable deficiency in practical cybersecurity education, especially around SQLi. While theoretical knowledge of SQLi risks is common, real-world experience in understanding how these attacks work—and how to defend against them—remains limited. The interactive educational module I am developing offers learners an engaging environment to explore SQLi mechanics safely. Addressing this educational need helps foster stronger, more secure coding practices, thereby reducing SQLi-related risks. This module equips users with both technical knowledge and practical experience, essential for identifying and mitigating actual SQLi vulnerabilities.

The module's primary goal is to provide my user-base with the knowledge and experience necessary to recognize and counteract SQLi attacks. Through a series of 12 hands-on challenges, users progress from basic SQLi concepts to advanced attack techniques, learning defensive methods and the reasoning behind their effectiveness, such as input validation, parameterized queries, and prepared statements. By the end

of the module, they will have developed valuable skills in secure coding practices applicable in real-world scenarios.

The educational module is developed using HTML, JavaScript, jQuery, and PHP and hosted on a Linux virtual machine with Apache and MariaDB. This setup ensures a safe, isolated environment where users can engage in SQLi challenges without risking actual systems. A critical feature of the project is the use of prepared statements, a best-practice defense against SQLi, which processes user inputs separately from SQL commands to neutralize malicious code. By presenting both successful and unsuccessful SQLi attempts, users experience firsthand the impact of secure coding practices and gain insights into why certain defensive methods are effective.

This project addresses the critical need for accessible, practical SQLi training. While many resources focus on theoretical aspects, few offer immersive opportunities for hands-on secure coding. My project bridges this gap by presenting realistic SQLi attack and defense scenarios, guiding users through SQLi mechanics and teaching how to prevent them. By learning secure coding techniques in a controlled, risk-free environment, learners are better prepared to respond effectively to SQLi threats, reducing potential vulnerabilities in real applications.

The module caters to users with a range of skill levels, from beginners to advanced learners. Beginners are supported with foundational information and hints to help them complete challenges, while advanced users face complex scenarios that encourage problem-solving with minimal guidance. Ultimately, this project aims to reduce SQLi vulnerabilities by promoting a security-first mindset among developers and students, who are critical players in safeguarding digital assets. This interactive training module is a valuable resource for educators and learners in cybersecurity, enhancing users' ability to recognize and defend against SQLi threats effectively. By contributing to the broader goal of creating a safer digital

landscape, this project enables learners to proactively safeguard sensitive data and apply secure coding practices in their professional careers.

III. STS Topic

Teaching cybersecurity skills to students, professionals, or enthusiasts is increasingly essential in today's interconnected digital society. However, with this knowledge comes the responsibility to prevent its misuse. Misuse in this context refers to the intentional or unintentional exploitation of vulnerabilities for harmful purposes, such as data breaches, financial fraud, or disruptions to critical infrastructure. For instance, a lack of ethical grounding in cybersecurity education can lead individuals to misuse techniques like SQL injection (SQLi), which, as studies show, remains one of the most exploited vulnerabilities in web applications (Dolev & Nir, 2014; OWASP, 2023). This project explores how structured, ethically informed training programs can equip learners with technical skills while fostering a culture of responsibility. As Hirsh and Sovacool (2010) assert, "the dissemination of technical knowledge must include ethical grounding to prevent unintended harm" (p. 73). Without such guidance, cybersecurity education risks creating skilled practitioners who inadvertently or intentionally cause harm, leading to severe societal consequences.

Cybersecurity operates within a sociotechnical system—a complex interaction of human behavior, technology, and societal norms. Historically, training has focused on technical skills, often neglecting the ethical implications of those skills. This imbalance reinforces harmful practices and excludes the broader social responsibilities tied to technical expertise. Hirsh and Sovacool (2010) emphasize that "systems resist alteration as they mature," suggesting that without deliberate efforts to integrate ethics, existing practices will perpetuate harmful norms (p. 75). Evidence underscores the risks of unregulated knowledge. The 1988 Morris Worm incident demonstrated how unintended consequences of technical experiments can disrupt networks nationwide. Similarly, the recent FlyCASS vulnerability, where SQLi could bypass TSA security checks, reveals how cybersecurity flaws can threaten national security (Gatlan,

2024). Such examples highlight the critical need for education programs that balance technical rigor with ethical considerations, aligning cybersecurity practices with societal values.

Research indicates that many cybersecurity education programs include ethical disclaimers but lack structured guidance on applying ethics in real-world contexts (Russo & Sabelfeld, 2009). For example, students often perceive ethics as secondary to technical mastery, a view reinforced by curricula that prioritize skill development over reflective practice. Anderson (2022) notes that "students must navigate a complex interplay of skills and values, often without clear guidance on how to reconcile them." This gap can foster a culture where technical exploits are valorized, even when they pose risks to others. A study by Novak and Vilceanu (2019) on public reactions to the Equifax data breach revealed that breaches erode trust in digital systems, demonstrating how unethical or negligent practices in cybersecurity can have lasting societal impacts. This insight underscores the importance of embedding ethical principles into technical training, ensuring learners consider the broader implications of their actions.

This project addresses the sociotechnical problem of integrating ethical awareness into cybersecurity training. The research question is: How can cybersecurity education programs effectively balance technical skill development with ethical responsibility to mitigate risks of misuse? By examining the interplay between technical knowledge and ethical frameworks, this study aims to create a model that prepares learners to navigate real-world challenges responsibly. The anticipated deliverable is an educational module that incorporates ethical considerations into cybersecurity training. This module will include interactive exercises where learners test SQLi vulnerabilities paired with scenarios that challenge them to consider the ethical implications of their actions. It will also feature case studies of incidents like the Morris Worm and FlyCASS to illustrate the societal consequences of misuse, alongside structured discussions that guide ethical debates and encourage reflection on responsibilities as cybersecurity professionals.

This research seeks to advance the sociotechnical understanding of cybersecurity training by embedding ethical awareness into its core. As Hirsh and Sovacool (2010) observe, “human stakeholders play important roles in channeling momentum… because of their concern for political control, influence, money, and power” (p. 82). By equipping learners with both technical skills and a strong ethical foundation, this project aims to reduce the societal risks of cybersecurity misuse while promoting trust and responsibility in the digital age.

IV. Overall Conclusion

This project integrates technical and ethical dimensions of cybersecurity education by creating an interactive module on SQL injection (SQLi) defense strategies while promoting responsible use of skills. The technical component provides hands-on experience in identifying and mitigating SQLi vulnerabilities, equipping learners with secure coding skills. Meanwhile, the STS analysis emphasizes the importance of ethics in cybersecurity, examining how structured guidance can prevent misuse and foster responsibility among future professionals.

Together, these components contribute to a comprehensive approach to cybersecurity education. By merging technical proficiency with ethical awareness, this project aims to reduce risks associated with SQLi and other vulnerabilities, helping users not only defend against threats but also understand their broader societal impact. The project demonstrates that effective cybersecurity training requires both skill and ethical guidance, providing a model for future programs. Ultimately, it underscores the need for a holistic approach to cybersecurity that balances technical knowledge with social responsibility, contributing to a safer and ethically grounded digital landscape.

V. Reference List

Dolev, S., & Nir, S. (2014). SQL injection: Techniques and defense mechanisms. Journal of Cybersecurity, 2(3), 105–117.

Demilie, W. B., & Deriba, F. G. (2022). Detection and prevention of SQL injection attacks and developing a comprehensive framework using machine learning and hybrid techniques. Journal of Big Data, 9, Article 124. https://doi.org/10.1186/s40537-022-00678-0

Halfond, W. G., Viegas, J., & Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. Proceedings of the IEEE International Symposium on Secure Software Engineering.

Hirsh, R. F., & Sovacool, B. K. (2010). Technological systems and momentum change. Technology and Culture, 51(4), 925–952.

Ma, L., Zhao, D., Gao, Y., & Zhao, C. (2019). Research on SQL injection attack and prevention technology based on web. 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA), 176–179. https://doi.org/10.1109/ICCNEA.2019.00042

Novak, A. N., & Vilceanu, M. O. (2019). "The internet is not pleased": Twitter and the 2017 Equifax data breach. The Communication Review, 22(3), 196–221. https://doi.org/10.1080/10714421.2019.1651595

OWASP Foundation. (2023). OWASP top ten: SQL injection. https://owasp.org/www-project-top-ten/2023/A01_2023-SQL_Injection

Russo, A., & Sabelfeld, A. (2009). Security analysis of dynamic languages. ACM Computing Surveys, 41(4), Article 19. https://doi.org/10.1145/1592434.1592437

Spagnuolo, M., Maggi, F., & Zanero, S. (2011). Towards automatic discovery of SQL injection vulnerabilities in web applications. Proceedings of the 3rd USENIX Conference on Web Application Security.

Gatlan, S. (2024, August 30). Researchers find SQL injection to bypass airport TSA security checks. BleepingComputer. https://www.bleepingcomputer.com/news/security/researchers-find-sql-injection-to-bypass-airport-tsa-security-checks/