Volume 11
Number 1
2016

ISSN: 1935-8156

http://www.aisej.com

SQL Injection: A Demonstration and Implications for Accounting Students

David Henderson
University of Mary Washington

Michael Lapke
University of Mary Washington

Christopher Garcia

Author Acknowledgements
The authors would like to acknowledge the helpful comments from the participants and reviewers at the 2013 AAA AIS Section Meeting. The authors received summer research support from the University of Mary Washington.

Published by the AIS Educator Association
http://www.aiseducators.com

AIS Educator Journal

Published by the AIS Educator Association

President: Deb Cosgrove, University of Nebraska, Lincoln
Vice President & Program Chair: Susan Cockrell, Austin Peay State University
Conference Chair: Elizabeth "Betsy" Pierce, Saginaw Valley State University
Research Co-Chair: Sarah Bee, Seattle University
Research Co-Chair: Lane Lambert, University of West Florida
Training Chair: Chelley Vician, University of St. Thomas

SQL Injection: A Demonstration and Implications for Accounting Students

Volume 11, Number 1
2016
pages 1 – 8

David Henderson
University of Mary Washington

Michael Lapke
University of Mary Washington

Christopher Garcia
University of Mary Washington

ABSTRACT

The purpose of this paper is to present a pedagogical case that demonstrates how a prevalent cybersecurity threat, SQL Injection (SQLi), operates. Prompted by questions from students such as: "How do cybersecurity threats work?" and "What specific actions can organizations take to mitigate cybersecurity threats?", this paper demonstrates the technical inner-working of SQLi. Students first answer background questions on SQLi and then simulate SQLi in both a Microsoft Access and web-based environment.

Keywords:
IT security, IT internal controls, Microsoft Access, SQL, SQLi

A teaching note and electronic files are available for use with this case. If you are member of the AIS Educator Association, please go to http://www.aiseducators.com and follow the links for the AIS Educator Journal. If you are not a member of the Association, please contact the author directly at the address provided above to obtain these materials. Please provide a means for verifying your credentials as a faculty member so that we may protect the integrity of the solutions materials.

INTRODUCTION

As more organizations conduct business over the Internet, cybersecurity threats have become more prevalent. For example, according to the 2014 Internet Security Threat report published by Symantec, mega breaches, those breaches with 10 million or more identities exposed, increased 700% from 2012 to 2013 and the total number of breaches increased 62% from 2012 to 2013.

One popular cybersecurity threat is Structured Query Language Injection (SQLi). According to reports from Imperva and Firehost (Ragan 2012), SQLi has been one of the most common forms of vulnerability in web applications for years (Wood 2012). While many examples of SQLi exist, one of the most prolific hackers who used SQLi was Albert Gonzalez (BBC 2009). Between 2005 and 2007, he and his co-conspirators used SQLi attacks to steal 170 million credit cards. His targets included Dave & Buster's, CardSystems Solutions, and Heartland Payment. It is unknown exactly how much money he made by reselling the cards, but when he was eventually arrested, authorities confiscated 2.7 million dollars in cash, a luxury car, laptops, firearms, a diamond ring, and other luxury items. A more recent case occurred in July of 2012 when a hacker group stole 450,000 user passwords from Yahoo's database using SQLi (Yap 2012). While not as critical as the financial damage done by Gonzalez, it demonstrated a disconcerting lack of security at one of the world's largest web portals. Not only did Yahoo lack countermeasures for SQLi attacks, but they stored user passwords in an unencrypted state.

Cybersecurity threats, such as SQLi, impact compliance and regulatory mandates, such as Sarbanes-Oxley (SOX), that are particularly relevant to accountants. To inform accounting students of the risks and corollary internal controls associated with cybersecurity threats, Accounting Information Systems (AIS) textbooks and AIS pedagogical research frequently address cybersecurity threats. While these textbooks provide a worthwhile overview of cybersecurity threats, our experiences from teaching cybersecurity suggest that students want to know how these threats operate, prompting questions such as: "How do cybersecurity threats work?" and "What specific actions can be taken to mitigate cybersecurity threats?". Understanding the technical details underlying cybersecurity threats is important, especially for accounting students interested in career opportunities in Information Technology (IT) Auditing. Such knowledge can help these students develop a deeper understanding of the risks associated with cybersecurity threats as well as the countermeasures for mitigating such threats.

Considering the increasing need for accounting students to develop a better understanding of cybersecurity threats, the purpose of this paper is to present a case that explores a popular cybersecurity threat, SQL Injection (SQLi). This case provides relevant background reading on SQLi and offers a tutorial on how to execute SQLi. Students initially answer questions about SQLi from the assigned readings and then execute SQLi attacks within a Microsoft Access database and web-based environment. AIS instructors can use this case when covering cybersecurity threats and/or Information Technology (IT) security topics. By providing hands-on experience executing SQLi, this case will help students develop a solid understanding of the technical aspects and business implications of SQLi, as well as a better understanding of how to mitigate risks from SQLi.

RELEVANCE OF SQL INJECTION TO ACCOUNTING STUDENTS

From a technical perspective, SQLi can result in unauthorized access to data, as well as unauthorized inserts, updates, and deletes of data. Naturally, malicious users who employ a

SQLi attack to view, insert, delete or update sensitive corporate data could also then disclose such data, thereby negatively impacting compliance with various regulatory mandates (e.g. SOX, HIPAA). Moreover, malicious users could employ SQLi to execute a denial of service attack by shutting down a corporate database.

Since SQLi can result in unauthorized disclosure of sensitive data, such as customer credit card information, organizations may incur significant remediation costs after a SQLi attack (SEC 2011). These may include the costs of repairing system damage caused by a SQLi attack or offering credit reports to customers. SQLi attacks may also result in significant cybersecurity protection costs including purchasing technologies to prevent future attacks, training employees or hiring outside consultants. Due to the potential damage to a firm's reputation following the unauthorized disclosure of sensitive customer data (e.g., credit card information) stemming from a SQLi attack, firms may experience significant difficulty in retaining and attracting customers, thereby negatively affecting future revenues and investor confidence. Since a SQLi attack can result in the unauthorized disclosure of customer data or even deletion or unauthorized updates to customer data, organizations exploited by a SQLi attack may be subject to significant future litigation costs.

Since cybersecurity threats such as SQLi can result in unauthorized access, unauthorized deletion of data, and unauthorized updates of data, they have the potential to impact important compliance issues such as SOX. SOX section 404 requires management to establish, assess, and monitor the effectiveness of internal controls over financial reporting (ITGI 2006; Richards et al. 2005). In an e-business environment, the integrity of the financial reporting process is reliant on the adequacy of internal controls, including IT-based internal controls (COSO 2011a; Klamm and Watson 2009, 2011). As such, in order to comply with SOX section 404 requirements, organizations must assess the effectiveness of internal controls, including IT-based internal controls that significantly impact financial reporting (Merhout and Havelka 2006). Organizations must validate the effectiveness of IT controls in order to certify the integrity of financial reporting for SOX compliance (ITGI 2006; Rozek 2008; Walters 2007). Consequently, assessing and mitigating IT risks has become more important for audit committees (Scharf 2007). Reflecting this importance, compliance and regulatory mandates have started to address IT risks on a deeper level. For example, the revised COSO Internal Control framework (COSO 2011a, 2011b) emphasizes the importance of IT-based risks and controls.

Cybersecurity threats may also expose an organization to further compliance risks (Annaswamy 2009; Klamm and Watson 2011). The most important of these compliance issues for accounting professionals center on the security of information systems resources and the privacy and protection of sensitive data. The Health Insurance Portability and Accountability Act (HIPAA) (relating to privacy of patient information within the health services industry), Gramm-Leach-Bliley Act (GLBA) (relating to privacy and protection of sensitive consumer data within the financial services industry), and Payment Card Industry Data Security Standards (PCI DSS) (relating to security of credit card and other personally identifiable information within the PCI industry) are salient examples. SQLi is important to consider when complying with HIPAA, GLBA, and PCI DSS because it can be used to steal, update or delete sensitive customer or patient data. To assess and mitigate cybersecurity threats, accounting students need to understand how these threats operate. Such understanding will help students identify, assess, and mitigate risks from cybersecurity threats.

The risks associated with cybersecurity threats have prompted the SEC to offer guidance regarding the disclosure of the risks associated with cybersecurity and cyber threats. According to the SEC, registrants should periodically reexamine their disclosures concerning cybersecurity risks and cyber incidents and revise them as deemed appropriate. If cyber incidents pose a significant investment risk in the company then registrants are advised to provide this disclosure. Additionally, cybersecurity risks and cyber incidents should be addressed in the Management Discussion and Analysis (MD&A) if these risks can severely impact the financial condition of the organization.

Researchers have noted the prevalence of communication problems between financial and IT auditors which have the potential to impair the overall financial audit effectiveness (Brazel 2008; Carmichael 2004; Curtis et al. 2009). Educating accounting students about cybersecurity threats can help alleviate this communication gap in several ways. First, training accounting students in cybersecurity can help accounting students understand technical terms and concepts and to speak the technical language of IT auditors. Second, understanding the technical details behind cybersecurity threats can also help accounting students connect technical issues to business implications—an important skill especially on an integrated audit. Overall, training accounting students in cybersecurity threats may help these students, many of whom will become financial auditors, to better work together with IT auditors to identify, assess and mitigate e-business risks.

Case Learning Objectives

The purpose of this case is to provide an overview of SQL Injection (SQLi), a cybersecurity threat. This case demonstrates how one specific cybersecurity threat, SQLi, operates as well as the appropriate technical countermeasures for mitigating SQLi.

As shown in Appendix A, the learning objectives for the SQLi case are to develop students' abilities to:

1. Identify and understand the risks of SQL injection and how cybersecurity threats, such as SQLi, impact the financial reporting process.
2. Understand SEC guidance for addressing the impact of cybersecurity threats on the financial reporting process.
3. Understand the technical inner-workings of SQLi.
4. Identify and understand countermeasures for controlling risks from SQLi.

THE SQL INJECTION CASE

The student case, teaching notes with suggested solutions and PowerPoints are available for downloaded from the journal website.

Case Efficacy

The questions in Appendix A provide AIS instructors a way to indirectly assess student learning. These questions are derived from the learning objectives and employ 5-point Likert Type scale response items. Collectively these questions provide a set of self-reported measures which gauge student reactions to the case. Instructors may distribute these questions during the class period upon completion of the case. Instructors may also choose to allow students to insert additional comments relating to the case at the end of the survey.

Tables 1 and 2 display a summary of student survey results collected from two implementations of this case. Data from these student surveys were collected from a small public liberal arts university in the southeastern United States from Spring 2013 to Spring 2014. Responses were coded from 1 (strongly disagree) to 5 (strongly agree), with 3 representing the neutral choice.

Instructor 1 reviewed the case and questionnaire within a senior-level undergraduate course in AIS, while instructor 2 reviewed the case and questionnaire within a graduate-level course in Management Information Systems (MIS). As such, questions 5, 8, and 9 were specific to accounting concerns and not applicable for instructor 2's course.

In addition to reporting the means and standard deviations, we also tested the hypothesis that average student response was above the neutral element (neutral = 3) for each question using a single-mean t-test. For all applicable questions, each of the corresponding p-values indicated significance ($p < 0.05$). Since all questions were positively worded, the significance of these results indicates that students perceived this case to be beneficial across each of these measures. This held true for both undergraduate students in AIS as well graduate students in MIS.

Table 1: Summary of student evaluations (5-point Likert-Type scale) in the undergraduate Accounting Information Systems course

Number	Question	n	Average	SD	t-stat	p-value
1	This case helped me to understand how frequently SQL injection attacks occur.	7	4.86	0.38	13.00	0.00
2	This case helped me to understand how the connection between internal controls and cybersecurity risks.	7	4.57	0.54	7.76	0.00
3	This case helped me understand the technical inner-working of SQL injection.	7	4.43	0.98	3.88	0.00
4	This case helped to identify the risks associated with SQL injection.	7	5.00	0.00	Inf.	0.00
5	This case helped me to understand SEC guidance for cybersecurity attacks.	7	4.00	0.58	4.58	0.00
6	This case helped me to identify and understand countermeasures for controlling risks from SQL injection.	7	4.43	0.54	7.07	0.00
7	This case improved my ability to read and create SQL statements.	7	4.43	0.54	7.07	0.00
8	This case helped to understand the connections between IT security and accounting.	7	4.57	0.54	7.76	0.00
9	This case helped me to understand why cybersecurity risks are relevant to accountants.	7	4.71	0.49	9.27	0.00

Table 2: Summary of student evaluations (5-point Likert-Type scale) in the graduate Management Information Systems course

Number	Question	n	Average	SD	t-stat	p-value
1	This case helped me to understand how frequently SQL injection attacks occur.	15	4.33	0.98	3.62	0.01
2	This case helped me to understand how the connection between internal controls and cybersecurity risks.	15	4.07	0.96	2.94	0.01
3	This case helped me understand the technical inner-working of SQL injection.	15	4.27	0.96	3.49	0.01
4	This case helped to identify the risks associated with SQL injection.	15	4.27	0.96	3.49	0.01
5	This case helped me to understand SEC guidance for cybersecurity attacks.	15	N/A	N/A	N/A	N/A
6	This case helped me to identify and understand countermeasures for controlling risks from SQL injection.	15	3.87	1.13	2.04	0.04
7	This case improved my ability to read and create SQL statements.	15	4.00	0.82	3.24	0.01
8	This case helped to understand the connections between IT security and accounting.	15	N/A	N/A	N/A	N/A
9	This case helped me to understand why cybersecurity risks are relevant to accountants.	15	N/A	N/A	N/A	N/A

REFERENCES

Annaswamy, S. 2009. A road map for regulatory compliance. *ISACA Journal* 4: 1–3.

BBC. 2009. *US man stole 130m card numbers*. Available at: http://news.bbc.co.uk/2/hi/americas/8206305.stm

Brazel, J. 2008. How do financial statement auditors and IT auditors work together? *The CPA Journal* 78 (11): 38–41.

Carmichael, D. 2004. The PCAOB and the social responsibility of the independent auditor. *Accounting Horizons* 18 (2): 127–133.

Committee of Sponsoring Organization of the Treadway Commission (COSO). 2011a. *Internal Control Integrated Framework Exposure Draft.* COSO. Available at: www.ic.coso.org.

Committee of Sponsoring Organization of the Treadway Commission (COSO). 2011b. *Internal Control Integrated Framework Executive Summary Exposure Draft.* COSO. Available at: www.ic.coso.org.

Curtis, M., J. G. Jenkins, J. Bedard, and D. Deis. 2009. Auditors' training and proficiency in information systems: A research synthesis. *Journal of Information Systems* 23 (1): 79–96.

Damele, D., Stampar, M. 2012. Sqlmap Website. Available at: http://sqlmap.org/
Imperva (2012). *Imperva's Web Application Attack Report.* Available at: http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed3.pdf.

Information Technology Governance Institute (ITGI). 2006. *IT Control Objectives for Sarbanes Oxley.* Rolling Meadows, IL: ITGI. Available at: http://www.isaca.org.

Klamm, B. K., and M. W. Watson. 2009. SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems* 23 (2): 1–23.

Klamm, B. K., and M. W. Watson. 2011. IT control weaknesses undermine the information value chain. *Strategic Finance* 8 (February): 39–45.

Lapke, M. (2010) Injecting Security into the Development Process. *Portuguese Journal for Management Studies* 15 (2): 235–247.

Litchfield, D. 2003. *SQL Server Security.* Emeryville, CA: McGraw-Hill Osbourne.

Merhout, J., and D. Havelka. 2006. Developing information risk management, security and assurance curricula for AIS/MIS/IT education. *Issues in Information Systems* 7 (1): 289–293.

Ragan, S. 2012. *SQL Injection Remains Top Web Application Attack Vecto*r. Available at: http://www.securityweek.com/sql-injection-remains-top-web-application-attack-vector.

Richards, D. A., A. S. Oliphant, and C. H. LeGrand. 2005. *Global Technology Audit Guide (GTAG)1: Information Technology Controls*. Altamonte Springs, FL: Institute of Internal Auditors.

Rozek, P. 2008. Solving the puzzle of IT for Sarbanes-Oxley: IT's role in Sarbanes-Oxley compliance. *Information Systems Control Journal* 5: 1–3.

Scharf, S. 2007. Audit committees more concerned with IT risk. *Internal Auditor* 64 (4): 15 –16.

SEC. 2011. *CF Disclosure Guidance*. Available at: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Symantec. 2014. Internet Security Threat Report. Volume 19. Downloaded on 5/27/2014 from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

Walters, L. M. 2007. A draft of an information systems security and control course. *Journal of Information Systems* 21 (1): 123–148.

Wood, P. 2012. *Security Think Tank: Several factors feed SQLi attacks.* Available at: http://www.computerweekly.com/opinion/Security-Think-Tank-Several-factors-feed-SQLi-attacks.

Yap, J. 2012. *450,000 user passwords leaked in Yahoo breach.* Available at: http://www.zdnet.com/450000-user-passwords-leaked-in-yahoo-breach-7000000772/.