ANALYSIS OF SQL INJECTION AND PHISHING ATTACKS: TECHNIQUES, IMPACTS, AND MITIGATION STRATEGIES

JULIAH JANE B. GEALON
IT IAS1: Information Assurance and Security 1

COR JESU COLLEGE, INC.
College of Computing and Information Sciences
Bachelor of Science in Information Technology

May 25, 2025
CIEMAVIL S. ALCAIN

Abstract

This research paper discusses two major cybersecurity threats: SQL Injection and Phishing. These are prevalent methods through which hackers target individuals and websites for stealing confidential information. SQL Injection allows attackers to breach vulnerable websites by submitting malicious code into forms. Phishing deceives individuals with spammed emails or messages to capture passwords, credit card numbers, or other confidential information.

The research paper describes how such attacks are done, what issues they raise such as data leakage, stolen information, and loss of money and how to prevent them. It presents actual examples and recommends countermeasures such as secure coding, input validation, employing multi-factor authentication, and educating individuals on how to identify scams. The overall aim is to educate individuals and organizations about these risks and how to defend their information and remain secure online.

Keywords: *SQL Injection, Phishing, Cybersecurity, Data Breaches, Mitigation Techniques*

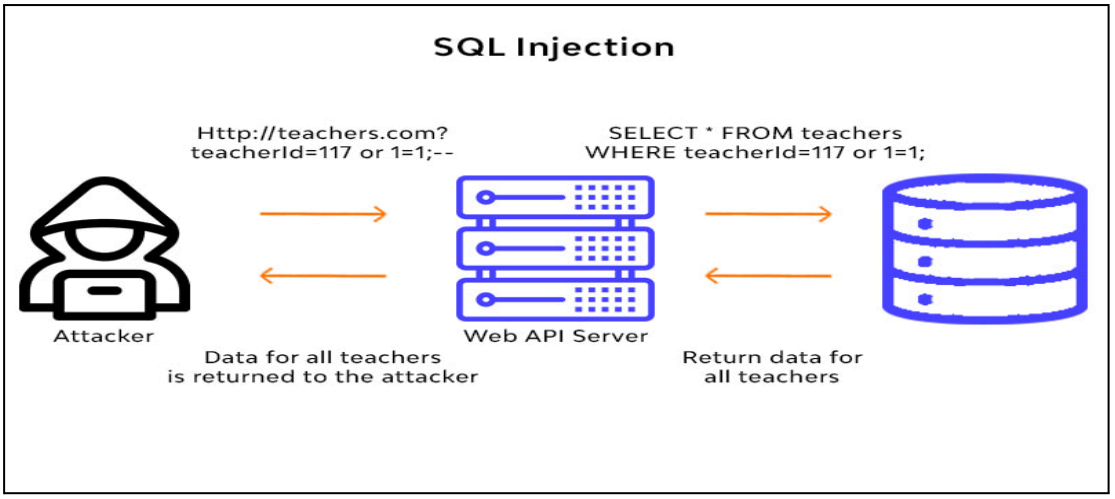
Table of Contents

1. Introduction

In the Digital Age, Cybersecurity has become one of the most concern, not just in the Philippines but worldwide. The rapid expansion of digital technologies has revolutionized the way we communicate, manage our daily routine, and businesses (Mwangi, P. 2024). Amidst all the advancements, the increasing risk of cybersecurity risk has become more critical for individuals, organizations, and governments (Rayhan, A. 2024). Life has become easier with the digital age, but it also introduced new threats. Hackers are now able to use powerful tools to hack into systems, transmit viruses, or even take over devices. These dangers not only impact individuals but also harm businesses and governments. Due to this, we need to know what these dangers are and how we can defend ourselves. One of the biggest challenges today is keeping information safe from cyber threats. Hackers now use powerful tools to break into systems, spread viruses, or take control of devices. These threats don't just affect individuals, they can disrupt businesses, steal data, and even damage a country's security (Mwangi, 2024).

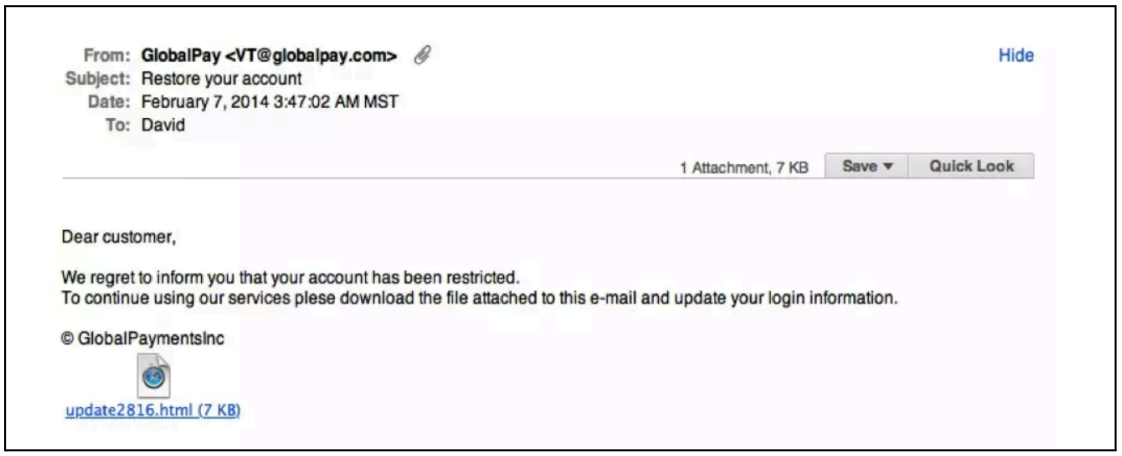
Two common types of cyberattacks are SQL injection and phishing. SQL injection happens when attackers insert harmful code into a website's input field, like a login form, to gain unauthorized access to databases. This can lead to stolen or deleted information (PortSwigger, n.d.). Phishing, on the other hand, tricks people into giving away sensitive data like passwords or bank information by pretending to be a trusted source, usually through fake emails or messages.

A web security vulnerability known as SQL injection (SQLi) enables an attacker to interfere with the database queries that an application submits. An attacker may be able to view data that they would not typically be able to access because of this. It may involve any data that the application has access to, including data that belongs to other users. An attacker can frequently alter or remove this data, changing the application's behavior or content in a permanent way. The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business (PortSwigger, n.d.).



Phishing is a kind of cybercrime whereby confidential data is shared by victims under false pretenses using phoney emails, text messages, phone calls, or websites, therefore downloading malware or otherwise exposing oneself to cybercrime . A hacker poses as a trusted individual, such as a coworker, supervisor, authority figure, or representative of a well-known company, in a conventional phishing scam. The hacker sends a message telling the victim to click on a link, open an attachment, pay an invoice, or do something else.

The user follows the directions and immediately falls into the scammer's trap since they believe the message's purported source. That "invoice" could take you straight to the account of a hacker. The user's device may get infected with ransomware as a result of that attachment. The user may be directed to a website that steals login passwords, bank account numbers, credit card numbers, and other personal information by clicking on that link (IBM, 2024).



Cyberattacks, like phishing and SQL injection, can lead to direct financial losses. Attackers can steal money from bank accounts, drain funds from businesses, or even demand ransom in exchange for stolen data. For businesses, the cost of a data breach or successful cyberattack goes beyond the immediate theft. It can include fines, legal fees, and the cost of fixing damaged systems. The longer a system remains compromised, the greater the potential financial damage (ProofPoint US., 2025).

For example, when ransomware attacks or phishing scams succeed, businesses often have to pay hefty sums to recover their data or mitigate the breach. In some cases, this can be a major setback, particularly for smaller businesses.

Personal data is a valuable asset in today's digital world. Phishing attacks or SQL injections often aim to steal sensitive personal or business information such as usernames, passwords, financial records, and even medical or health records. This data can then be used maliciously—for identity theft, fraud, or other crimes. When this data is exposed or misused, it violates an individual's privacy rights and can cause long-term harm, including financial ruin and reputational damage.

1. Objectives of the Research

This study has four main goals. One, it intends to discover and explain the exact methods used in SQL Injection (SQLi) and phishing attacks and how these exploit technical and human frailties. Two, it intends to study the actual effects of these attacks through analysis of significant case studies presenting how they affect organizations and individuals. Third, it strives to investigate and suggest sound prevention and mitigation measures to enhance cybersecurity defenses against the threats. Lastly, the study addresses the ethical issues of investigating and responding to cybersecurity incidents, such as responsible disclosure and dealing with sensitive data.

2. SQL Injection: Overview and Analysis

1. What is SQL Injection?

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

2. Types of SQL Injections Attacks

1. **Classic SQL Injection Attack**

   The hacker inserts malicious SQL commands directly into user input fields interacting with an app's database. Attackers can now manipulate the input fields and change the structure of an SQL query to access the application and data without authorization.

2. **Blind SQL Injection Attack**

   A blind SQL injection attack is when the malicious SQL commands are injected into database fields by the attacker "blindly" without the direct retrieval of the command's output by the application, as in traditional SQLi. Rather, they search for indirect hints, like HTTP responses, response time, app behavior, to deduce the command's result. They are also referred to as inferential SQL injection. There are two categories: Time-based SQLi and Boolean/content-based SQLi.

3. **Time-Based Blind SQL Injection**

   Time-based blind SQL injection is a type of blind/inferential SQL injection. The attacker manipulates an app's queries to cause delays in response deliberately. They depend on the app response time to decide whether their query is valid or invalid.

4. **Error-Based SQL Injection**

   Error-based SQL injection is a type of hacking that uses error messages from a website to find out details about its database. These messages help developers fix problems while building the site, but they should be hidden or removed when the site goes live to keep it safe.

5. **Union-Based SQL Injection**

   Union-based SQL injection is a hacking method that combines results from different database queries using the UNION command. The combined data is sent back to the hacker through the website. Hackers use this to steal information from different tables in the same database.

6. **Out-of-Band SQL Injection**

   Out-of-band SQL injection is not so common, but when it happens, it can impact your organization's reputation and finances.

7. **Second-Order SQL Injection**

   A smart type of attack where a hacker puts harmful code into a database, but it doesn't run right away. Later, when another part of the website uses that data in a new SQL query, the harmful code runs and can cause damage.

3. Real-World Examples

Microsoft SQL Server Vulnerability (2021): In 2021, researchers discovered a major SQL injection vulnerability within Microsoft SQL Server Reporting Services (SSRS). This flaw allowed attackers to execute arbitrary code by crafting malicious queries. Although there was no public exploitation of this vulnerability, it underscored the potential risks SQLi poses to critical infrastructure like Microsoft's enterprise services (Radware., n.d.).

In 2021, a notable SQL injection vulnerability was found in Microsoft SQL Server Reporting Services (SSRS), one of the popular tools utilized by companies to design, manage, and distribute reports from SQL Server data. SSRS is a vital application in enterprise situations, and any security vulnerability in it can create severe threats to business operations. The vulnerability involved the way the SSRS web interface processed user input. Researchers discovered that it failed to properly sanitize some requests, thereby allowing attackers to inject and run malicious SQL code.

This kind of vulnerability, called SQL injection (SQLi), would enable an attacker to run unauthorized SQL commands against the server database. In worse scenarios, the bug would be exploited for remote code execution, where attackers could run any command or program on the target server. Although researchers acknowledged the technical exploitability of the vulnerability, no public or active attacks were known to have occurred. The discovery, however, underscored the vulnerability of even critical infrastructure such as Microsoft's enterprise software.

7-Eleven breach (2007): A group of attackers used SQL injection to compromise the payment systems of several companies, including the 7-Eleven retail chain. This breach led to the theft of over 130 million credit card numbers. The attack was one of the largest data breaches of its time, demonstrating the immense financial and legal ramifications of SQL injection vulnerabilities (Dissent., 2009).

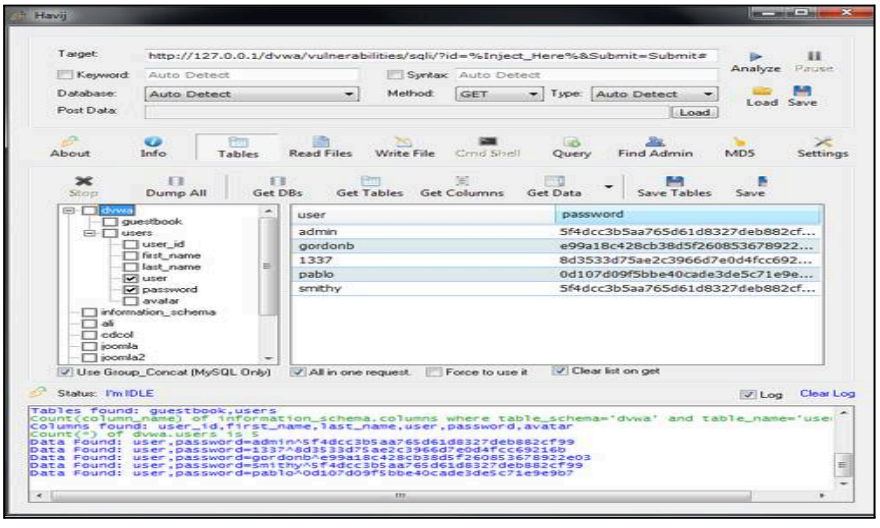
In August 2007, 7-Eleven, Inc. fell victim to a significant cyberattack involving a SQL injection vulnerability. Hackers exploited this flaw in 7-Eleven's public-facing website to gain unauthorized access to the company's servers. This breach allowed them to infiltrate systems supporting ATM terminals located within 7-Eleven stores.

The attackers, part of a larger cybercriminal group, used SQL injection techniques to install malware on the compromised servers. This malware enabled the theft of credit and debit card information from customers using certain ATMs in 7-Eleven stores over a 12-day period from October 28 to November 8, 2007 Data Breaches

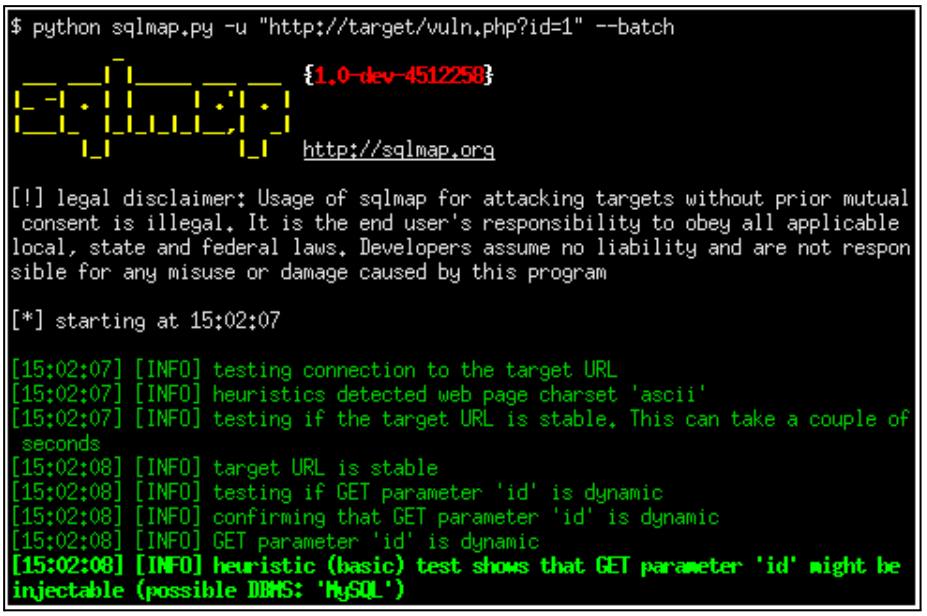
While the exact number of card numbers stolen from 7-Eleven remains undetermined, the broader operation orchestrated by Gonzalez and his co-conspirators resulted in the theft of over 130 million credit and debit card numbers from multiple companies, including Heartland Payment Systems and Hannaford Brothers (Taylor, J., 2019).

4. Tools for Exploitation

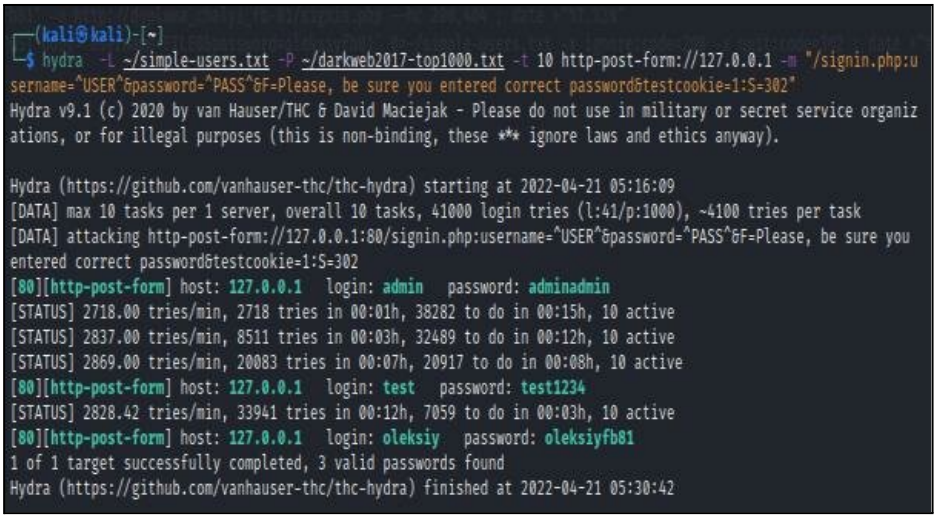
1. **Havij -** Havij, an automatic SQL Injection tool, is distributed by ITSecTeam, an Iranian security company. The name Havij means “carrot”, which is the tool’s icon. An operator can easily access the needed data thanks to the tool's user-friendly graphical user interface. The shift in attacks from code-writing hackers to non-technical people could be attributed to this ease of use. Since the publication of Havij in 2010, a number of additional automatic SQL Injection tools (like sqlmap) have been released. Havij is still in use today, nonetheless, and is frequently utilized by both novice hackers and penetration testers (Bferrite, 2015).



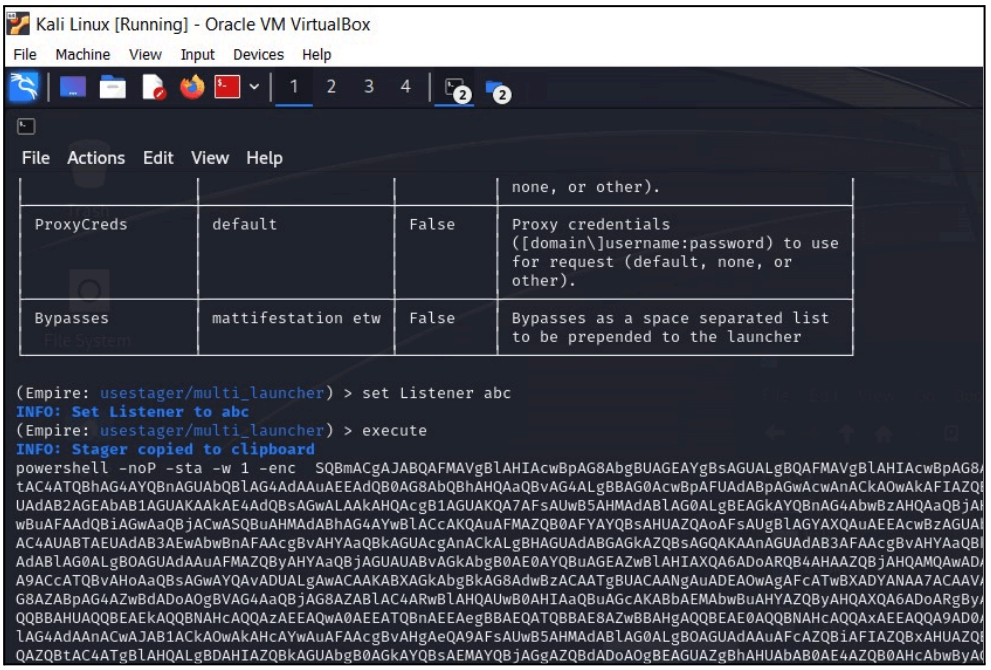
2. **SQLMap -** Sqlmap is an open source penetration testing tool that makes it easier to find and take advantage of SQL injection vulnerabilities to take control of back-end database servers. Database fingerprinting, data retrieval from the database, file system access, and OS command execution through out-of-band connections are only a few of its many functions (CISA, n.d.).



3. **Hydra -** Hydra, also known as THC-Hydra, a fast and powerful password-cracking tool used for brute-force attacks on login pages and network protocols. It is widely used by ethical hackers, penetration testers, and cybersecurity analysts to test the strength of passwords and identify weak authentication systems (Surbhi_Choudhary, 2025).



4. **PowerShell -** PowerShell is created by Microsoft, a powerful command-line shell and scripting language. The primary objective is to automate procedures, manage Windows operating system configuration, and perform system administration duties. PowerShell also works cross-platform, with support for Linux and macOS (EmpireProject, n.d.).



4. Phishing: Overview and Analysis

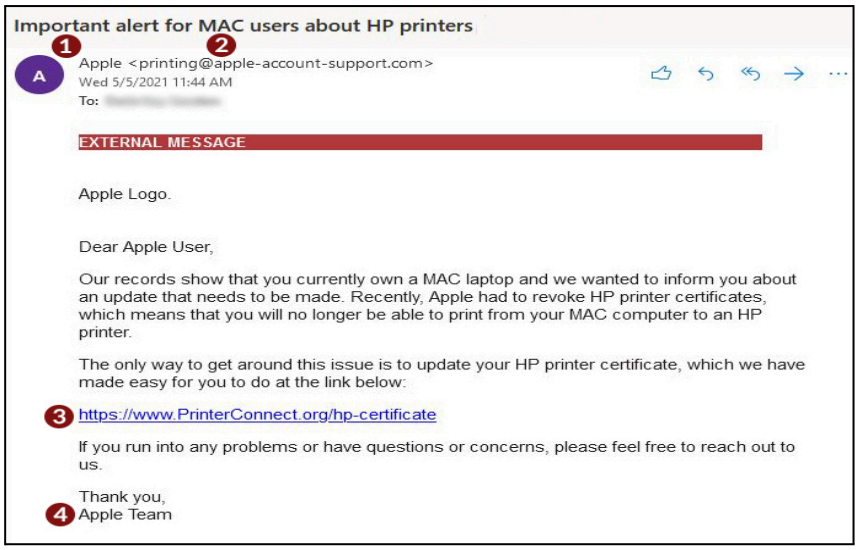
1. What is Phishing

Phishing is a form of cyberattack that employs fake emails, text messages, phone calls or websites to trick individuals into divulging sensitive information, installing malware or otherwise putting themselves at the mercy of cybercrime.

2. Types of Phishing Attacks

1. Email Phishing

- Most phishing attacks come through email. Hackers create fake websites or email addresses that look like real ones by changing or adding letters, using subdomains, or putting trusted names in the email address. These emails often create fear or urgency to trick people into acting fast without thinking or checking if the message is real.

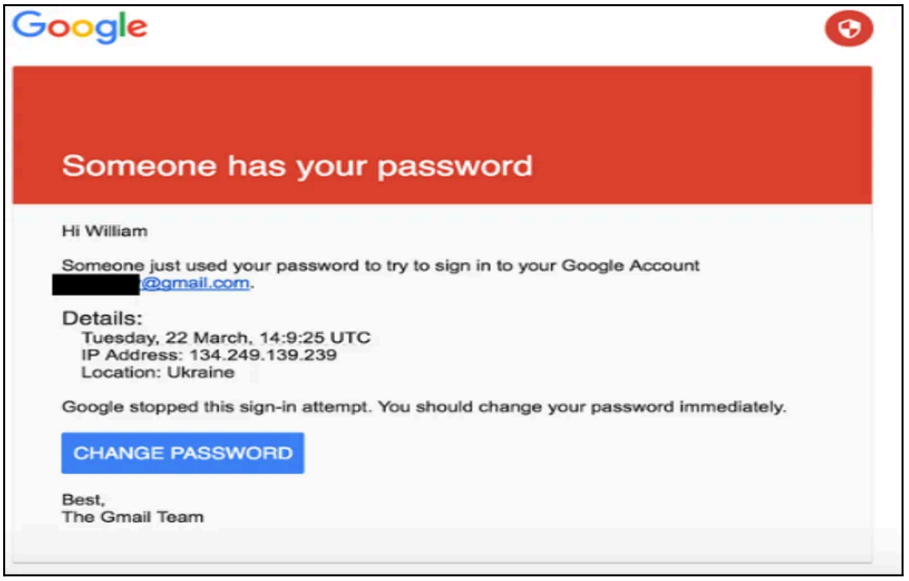


2. Spear Phishing

Spear phishing includes malicious emails sent to specific people. The attacker typically already has some or all of the following information about the victim:

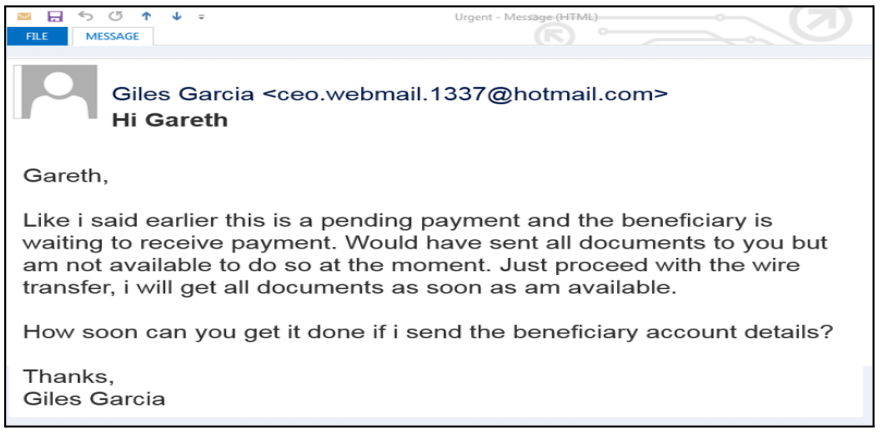
* Name
* Place of employment
* Job title
* Email address
* Specific information about their job role

This information helps increase the effectiveness of phishing emails and manipulate victims into performing tasks and activities, such as transferring money.



3. Whaling

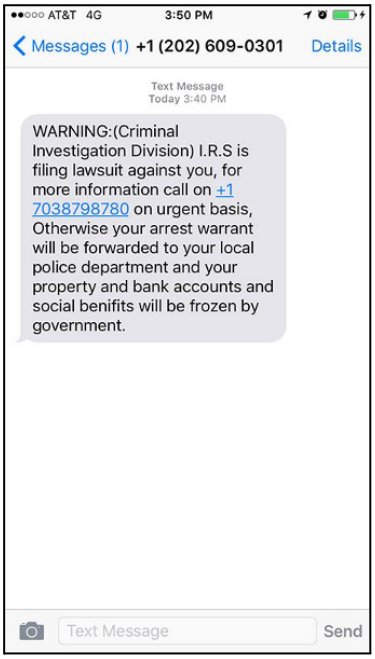
Whaling attacks are a type of phishing that targets top employees like managers or executives. These attacks are very carefully planned and use personal information found online to make the messages look real. Unlike regular phishing, they don't use obvious tricks like fake links. Instead, they send very personalized messages to fool the victim and steal sensitive information.



4. Smishing and Vishing

- A type of Phishing that uses phones instead of emails.
  - Smishing - a hacker sends fake messages.
  - Vishing - a hacker calls the victim or uses automated voice messages.

In vishing, the hacker may pretend to be from a bank or credit card company and say there's a problem with the victim's account. They then ask for personal or payment details, which they use for fraud.



3. Psychological Tactics

Cyber attackers usually employ psychological tactics to manipulate individuals into performing something risky, such as clicking a malicious link or sharing passwords. These tactics play on human emotions, including fear, trust, or curiosity. Some of the tactics used in phishing and social engineering.

1. **Urgency -** Cyber attackers usually employ psychological tactics to manipulate individThe attacker tries to make you act quickly by saying something like, “Your account will be closed in 30 minutes,” or “Limited time offer—click now!” This creates pressure, so you don’t take time to think or check if the message is real.uals into performing something risky, such as clicking a malicious link or sharing passwords.
2. **Authority -** The attacker pretends to be someone important, like your boss, a company manager, or even the police. For example, they might say, “This is your CEO—send the report now.” Because people are used to following orders from authority figures, they often do what the message says without question.
3. **Fear -** Mostcommonly used. Attackers try to scare you into acting fast. They may say things like, “Your bank account has been hacked,” or “You’re under investigation.” Fear makes it harder to think clearly, so people may respond quickly to avoid trouble.

4. Notable Phishing Campaigns

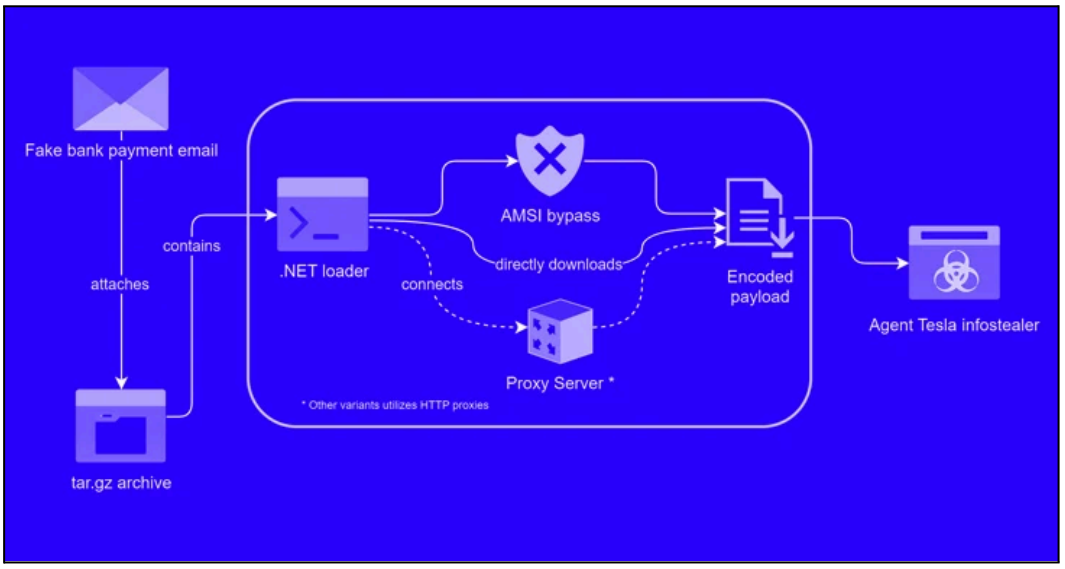
Sony Pictures Hack 2014: Sony Corporation was a technology and media giant with more than 130,000 workers and almost $70 billion in yearly revenue. In its electronics, media, gaming, music, mobile, and other segments combined, Sony had expanded from its founder's earlier radio repair shop, a modest post-war facility established in Japan in 1946 into a market leader in global consumer electronics, and Japan's 21st largest corporation in 2014. Despite its media and tech capabilities, however, the multinational corporation had gained a poor information security reputation among the hacking community. Online message board denizens even invented a word coined at the expense of the company: "Sownage," loosely meaning an act of defeat being 'owned' as it were on the Internet similar to Sony's own net humiliations (Steinberg, et.al. , 2021).

An overseas cyber hacking crew compromised SPE's network through malware, hijacking the company's online business and gaining access to a large array

of sensitive employee information, personal emails and future movies. The breach caused severe disruptions, leaked material and huge controversy for an imminent movie premiere (Vergelis, 2018).

Malware Disguised as a Bank Payment Notice: The news post **"Alert: New Phishing Attack Delivers Keylogger Disguised as Bank Payment Notice"** by The Hacker News showcases a detailed examination of a sophisticated phishing campaign that was found in March 2024. The Hacker News is a renowned cybersecurity news site that publishes timely news, threat intelligence, and expert opinions on data breaches, malware, and other cyber threats to professionals and IT decision-makers.

This specific article explains how the attackers are sending a phishing email that pretends to be a bank payment notice. The email has an archive file titled "Bank Handlowy w Warszawie - dowód wpłaty_pdf.tar.gz" that, upon opening, triggers the execution of a malicious keylogger called Agent Tesla. Malware is packed inside a .NET-based loader that applies intense obfuscation and polymorphic methods in order to evade detection. Also, it evades the antivirus application by patching the Windows Antimalware Scan Interface (AMSI) (The Hacker News, n.d.).



5. Comparative Analysis: SQL Injection and Phishing

SQL Injection is a type of cyber attack that targets websites and databases. It is a technical attack, meaning the attacker must know how websites and databases work. They use special code in places like login forms to trick the system and access private data. Phishing, on the other hand, is a human-based attack. It targets people by

tricking them into giving personal information like passwords or credit card numbers, usually through fake emails or websites (IJISRT., n.d.).

SQL Injection is harder to do because it needs coding and database knowledge. Phishing is easier because attackers can use ready-made tools and send fake messages to many people without much skill. Both attacks can seriously harm companies. SQL Injection can lead to stolen or deleted data, and even full control of a system. Phishing can also cause big problems if employees are tricked, allowing attackers to steal data or install harmful software (Radware, n.d.).

For individuals, SQL Injection may expose their information if a company's database is hacked, but the attack isn't aimed at them. Phishing is aimed directly at people, and victims can lose money, have their identity stolen, or lose control of their online accounts. In short, SQL Injection attacks systems, while Phishing targets people. SQL Injection is harder but affects systems more. Phishing is easier and harms both people and companies. Knowing how these attacks work helps us stay safe online (Jnguyen, 2022).

6. Mitigation and Prevention Strategies

Preventing SQL Injection requires a multi-layered approach. Input validation ensures that all user inputs are sanitized and validated. Parameterized queries use placeholders to prevent direct execution of user-provided data. Object-relational mapping (ORM) abstracts database interactions, reducing the exposure to raw SQL commands. Additionally, web application firewalls (WAFs) help monitor and filter malicious traffic to protect web applications (OWASP, n.d.).

Phishing mitigation centers around user-focused strategies. Education is critical; users must be trained to recognize and report phishing attempts. Multi-factor authentication (MFA) adds an extra security layer, even if credentials are compromised. Advanced email filters can detect and block phishing attempts before they reach the user (Valimail, n.d.).

General strategies applicable to both threats include regular security audits to uncover and address vulnerabilities, comprehensive incident response plans to quickly

contain breaches, and well-defined cybersecurity policies to guide organizational behavior (CISA, n.d.).

7. Ethical Considerations

Ethical handling of cybersecurity research involves several considerations. Responsible disclosure entails promptly reporting discovered vulnerabilities to affected parties. Ethical research practices avoid exploiting systems and ensure that testing does not result in harm. Additionally, researchers must handle sensitive information with confidentiality and integrity to maintain trust and accountability.

8. Trends

Emerging trends highlight the increasing sophistication of both SQLi and phishing attacks. AI-powered phishing is becoming more prevalent, with attackers using artificial intelligence to craft highly convincing phishing emails, complicating detection efforts (The Guardian, 2024). On the SQLi front, attackers are developing advanced techniques to exploit modern applications, prompting continuous evolution in security protocols (IJISRT, n.d.).

Phishing kits—pre-packaged tools that enable even novice attackers to launch phishing campaigns—are now widely accessible, contributing to the rising volume of attacks. Additionally, mobile phishing and cloud-based SQLi are growing concerns as more services migrate to cloud environments and mobile platforms (Keepnet Labs, 2025).

9. References

Bferrite, & Bferrite. (2015, May 14). *Analysis of the Havij SQL Injection tool*. Check Point Blog. https://blog.checkpoint.com/security/analysis-havij-sql-injection-tool/

CISA. (n.d.). *Cybersecurity Best Practices*. Retrieved from https://www.cisa.gov/topics/cybersecurity-best-practices

CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/services/sqlmap

Dissent. (2009, August 18). *7-Eleven statement regarding 2007 credit card fraud – DataBreaches.Net*. https://databreaches.net/2009/08/18/7-eleven-statement-regarding-2007-credit-card-fraud/?

Dissent. (2009a, August 17). *Three indicted for hacking Heartland, 7-Eleven, and Hannaford; Over 130 million credit and debit card numbers stolen – DataBreaches.Net*. https://databreaches.net/2009/08/17/three-indicted-for-hacking-heartland-7-eleven-and-hannaford-over-130-million-credit-and-debit-card-numbers-stolen/?

EmpireProject. (n.d.). *GitHub - EmpireProject/Empire: Empire is a PowerShell and Python post-exploitation agent.* GitHub. https://github.com/EmpireProject/Empire

IBM. (2024, May 17). *What is phishing?* IBM. https://www.ibm.com/think/topics/phishing

IJISRT. (n.d.). *Comprehensive review of advanced techniques for mitigating SQL injection vulnerabilities in modern applications*. Retrieved from https://www.ijisrt.com/comprehensive-review-of-advanced-techniques-for-mitigating-sql-injection-vulnerabilities-in-modern-applications

Jnguyen. (2022, June 17). *What is Phishing? Types of Phishing Attacks*. Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/

Keepnet Labs. (2025). *2025 Phishing Statistics: Top Phishing Stats, Insights & Trends*. Retrieved from https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

Mwangi, P. (2024). Cybersecurity threats and national security in the digital age. *American Journal of International Relations*, *9*(1), 26–35. https://doi.org/10.47672/ajir.1938

OWASP. (n.d.). *SQL Injection Prevention Cheat Sheet*. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

PortSwigger. (n.d.). *What is SQL Injection? Tutorial & Examples*. Retrieved May 21, 2025, from https://portswigger.net/web-security/sql-injection

Rayhan, A. (2024). *Cybersecurity in the digital age: Assessing threats and strengthening defenses*. ResearchGate. https://doi.org/10.13140/RG.2.2.31480.25607

Radware. (n.d.). *SQL Injection: Examples, real life attacks & 9 defensive measures | Radware*. https://www.radware.com/cyberpedia/application-security/sql-injection/

Sharadin, G. (2023, December 21). *What is phishing | Attack techniques & scam examples | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/phishing-attack-scam/

Steinberg, S., Stepan, A., Neary, K., Picker Center Digital Education Group, & Columbia's School of International and Public Affairs. (2021). The hacking of Sony Pictures: A Columbia University case study. *SIPA*, 1–3.

https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf

Surbhi_Choudhary. (2025, May 18). Hydra || Offensive Security Tooling|| TryHackme|| Cybersecurity||. *Medium*. https://medium.com/@surbhichoudhary_5136/hydra-offensive-security-tooling-tryhackme-cybersecurity-a65af74b82fa

Taylor, J. (2019, October 25). 7-Eleven fuel app data breach exposes users' personal details. *The Guardian*. https://www.theguardian.com/technology/2019/oct/25/7-eleven-fuel-app-data-breach-exposes-users-personal-details

The Hacker News. (n.d.). *Alert: New phishing attack delivers keylogger disguised as bank payment notice*. https://thehackernews.com/2024/03/alert-new-phishing-attack-delivers.html

Valimail. (n.d.). *Complete Guide to Phishing: Techniques & Mitigations*. Retrieved from https://www.valimail.com/resources/guides/guide-to-phishing/

Vergelis, M. (2018, December 20). 2018 Fraud World Cup. *Securelist*. https://securelist.com/2018-fraud-world-cup/85878/

What is phishing? - meaning, attack types & more | ProofPoint US. (2025, April 18). Proofpoint. https://www.proofpoint.com/us/threat-reference/phishing

10. Appendices

Appendix A: Classic Sql Injection Attack

*SELECT * FROM products WHERE name = '' OR '1'='1'; --';*

Appendix B: Blind SQL Injection Attack

Cookie: TrackingId=u5YD3PapBcR4lN3e7Tj4

SELECT TrackingId FROM TrackedUsers WHERE TrackingId = 'u5YD3PapBcR4lN3e7Tj4'

Appendix C: Time-Based Blind SQL Injection

*SELECT * FROM users WHERE username = '' OR IF(1=1, SLEEP(5), 0) --' AND password = '';*

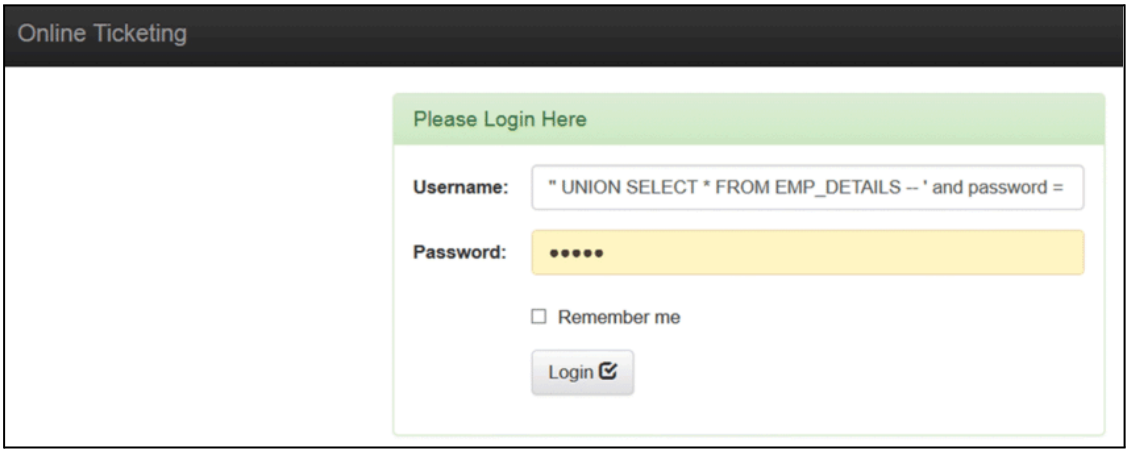
- IF(1=1, SLEEP(5), 0) is a condition that makes the database sleep for 5 seconds if 1=1 (which is always true).
- The -- makes everything after it a comment, so the rest of the query is ignored.
- The server now delays the response by 5 seconds if the injection is successful.

Appendix D: Error-Based SQL Injection

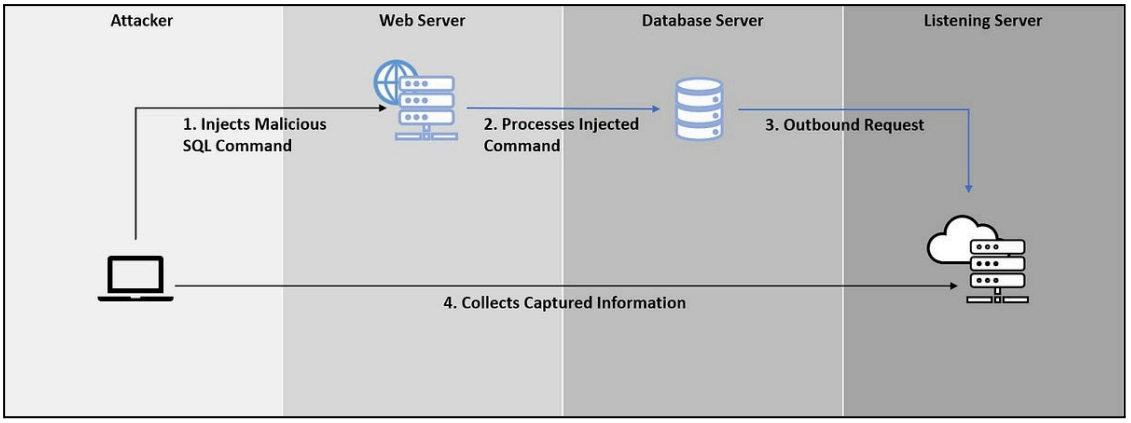
UNION SELECT null, table_name, column_name FROM information_schema.columns WHERE table_name='users' –

A malicious actor inputs an SQL command that generates error messages intentionally from the database server. This lets them gain knowledge about the structure of the target database. They can also determine data values, column names, and table names with this method.

Appendix E: Union-Based SQL Injection



Appendix F: Out-of-Band SQL Injection



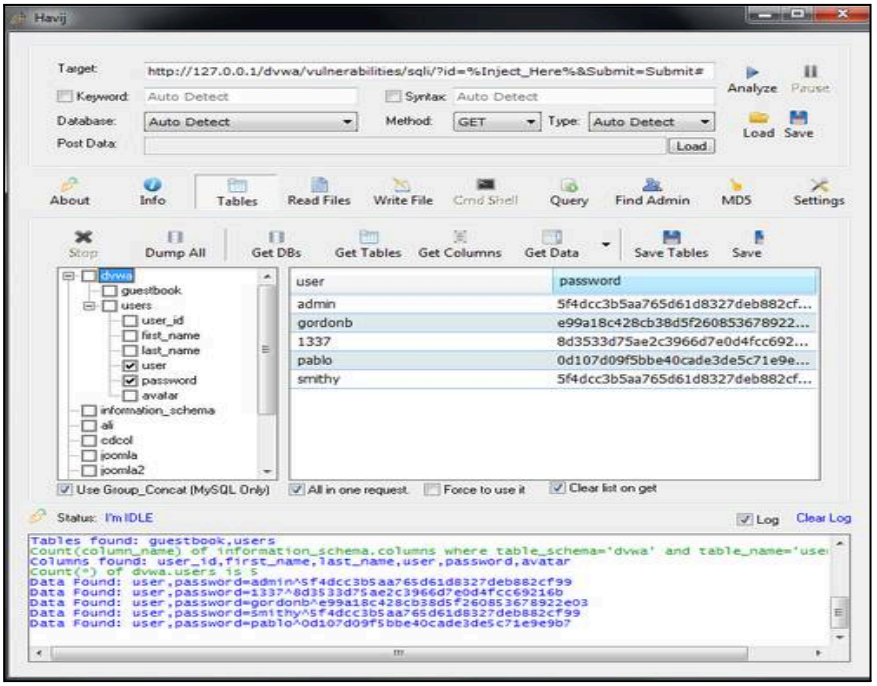
Appendix G: Second-Order SQL Injection

execute immediate *'SELECT username FROM sessiontable WHERE session ='"'||sessionid||'"'* into username;

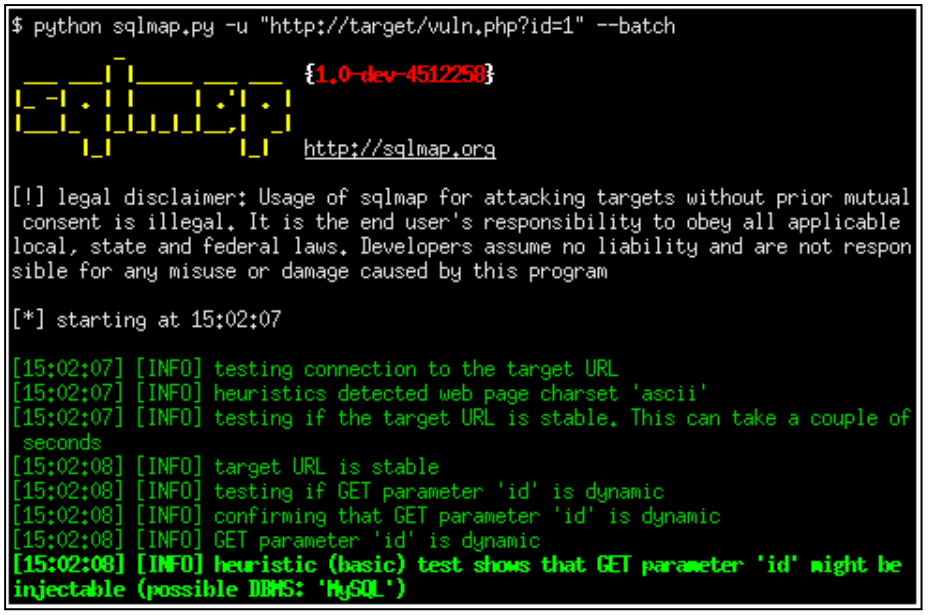
execute immediate *'SELECT ssn FROM users WHERE 'username='"'||username||'"'* into ssn;

This will be injectable if the attacker had earlier on the "Create Account" screen created a username such as: *XXX' OR username='JANE* Which creates the query: *SELECT ssn FROM users WHERE username='XXX' OR username='JANE'* If the user XXX does not exist, the attacker has successfully retrieved Jane's social security number.

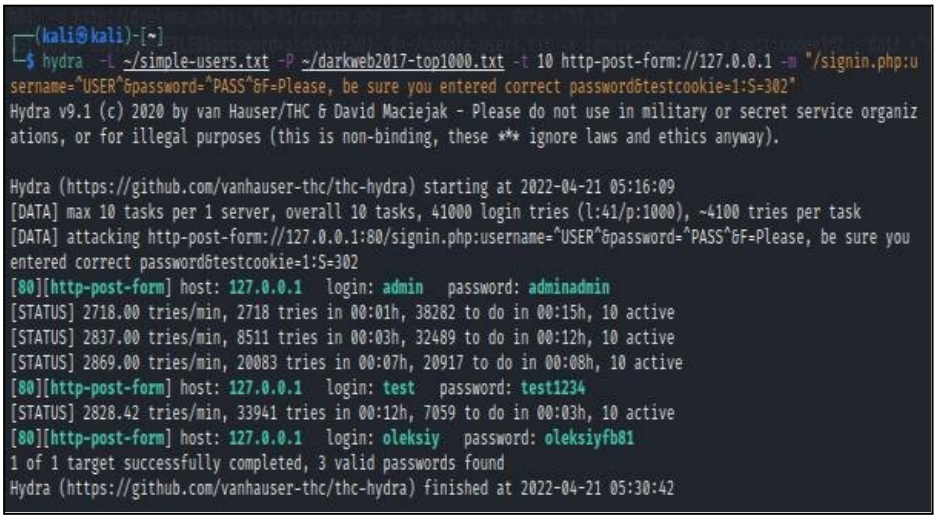
Appendix H: Havij Screenshot



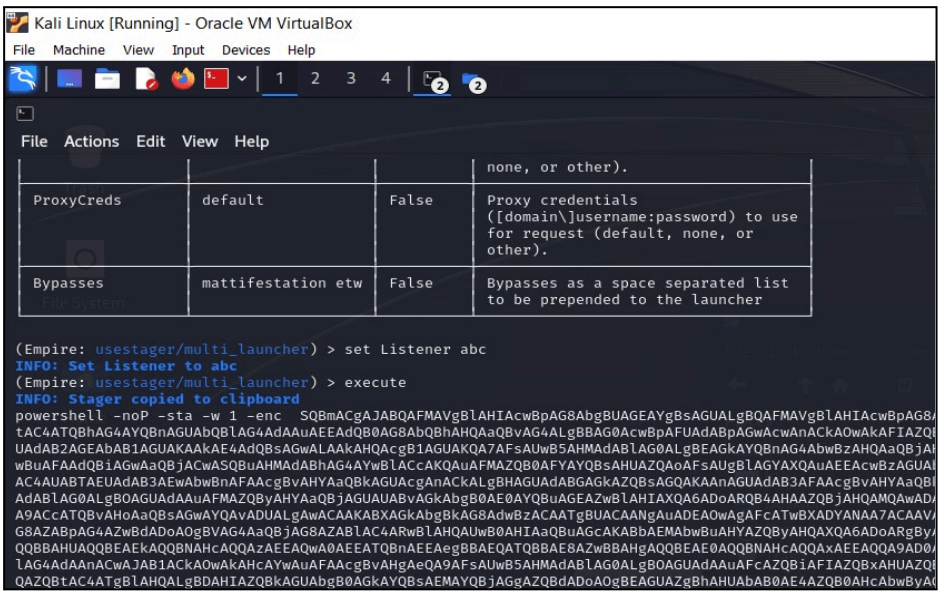
Appendix I: SQLMap Screenshot



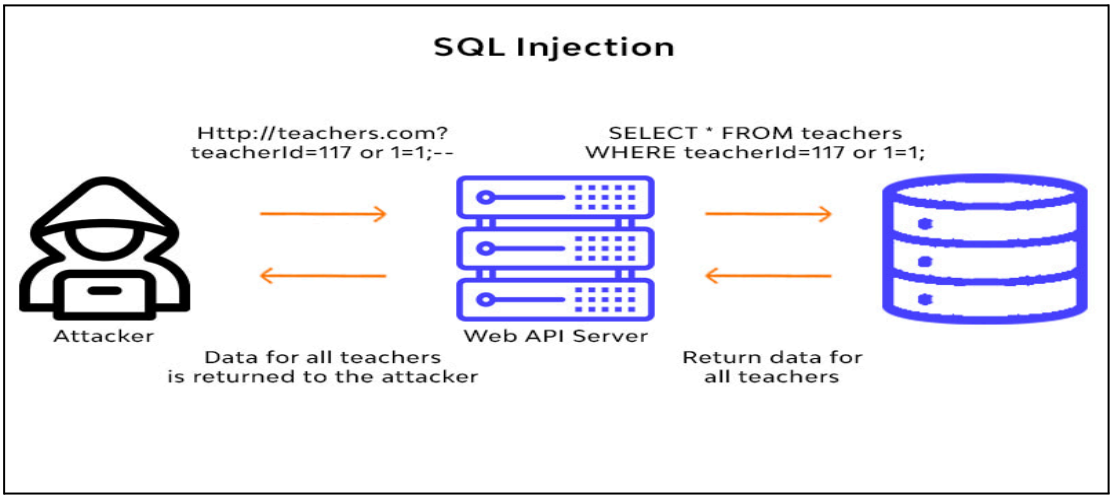
Appendix J: Hydra Screenshot



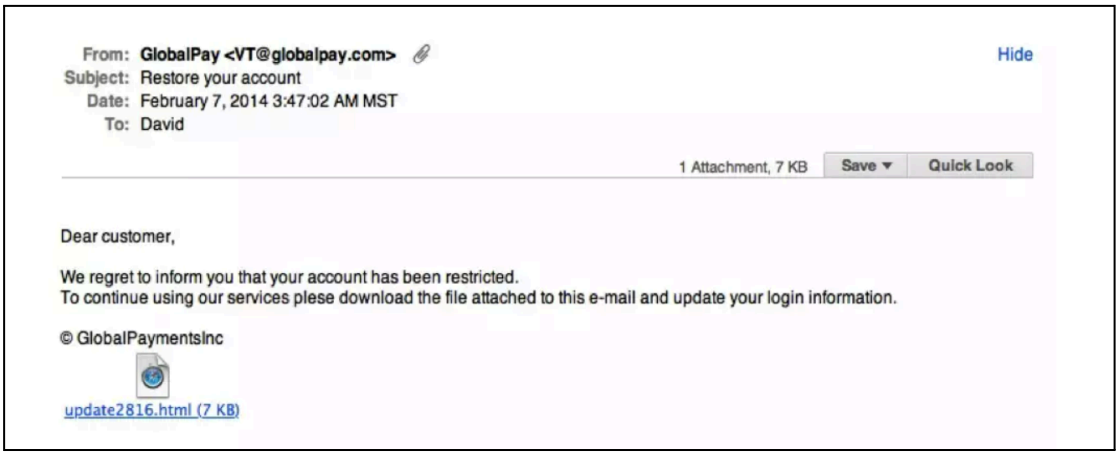
Appendix K: Powershell Screenshot



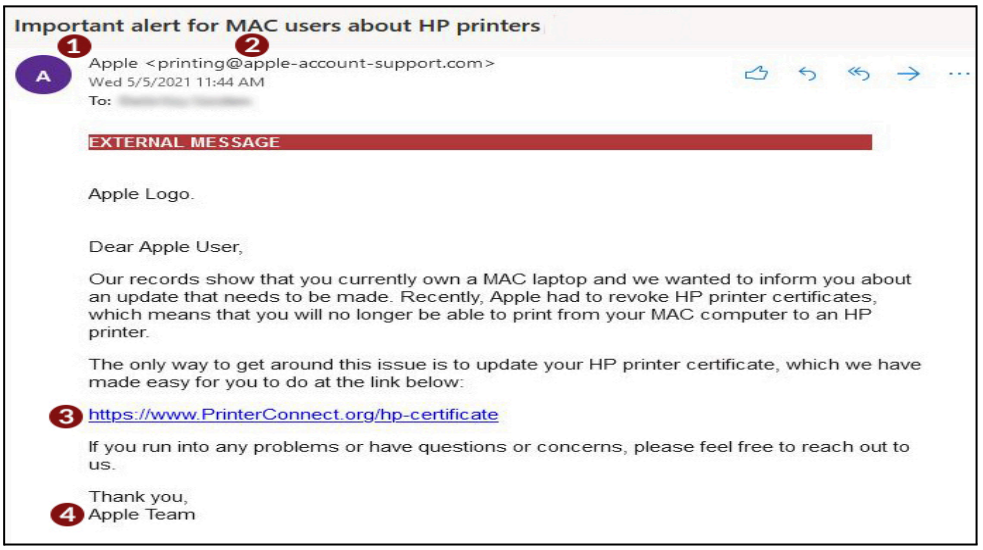
Appendix L: SQL Injection



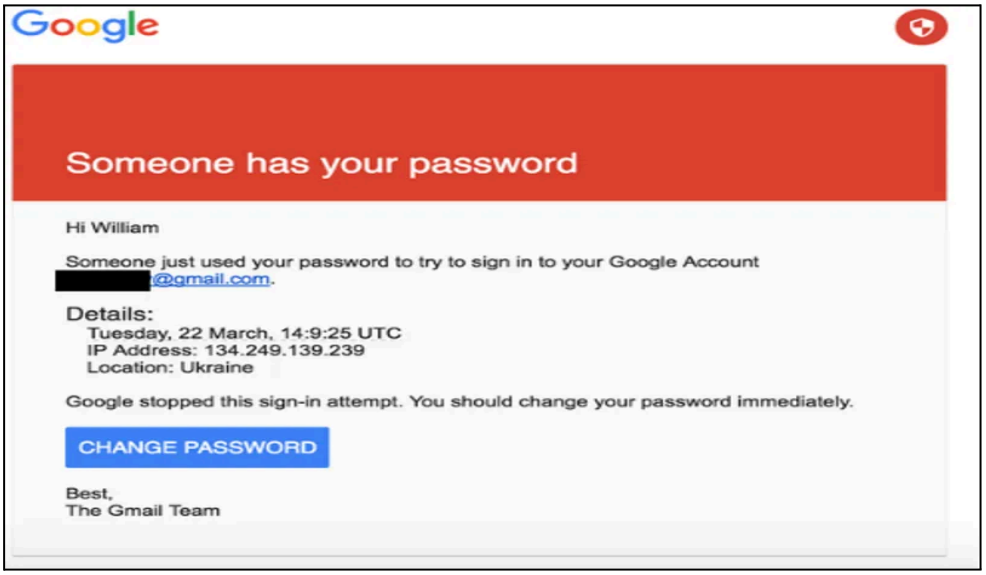
Appendix M: Phishing



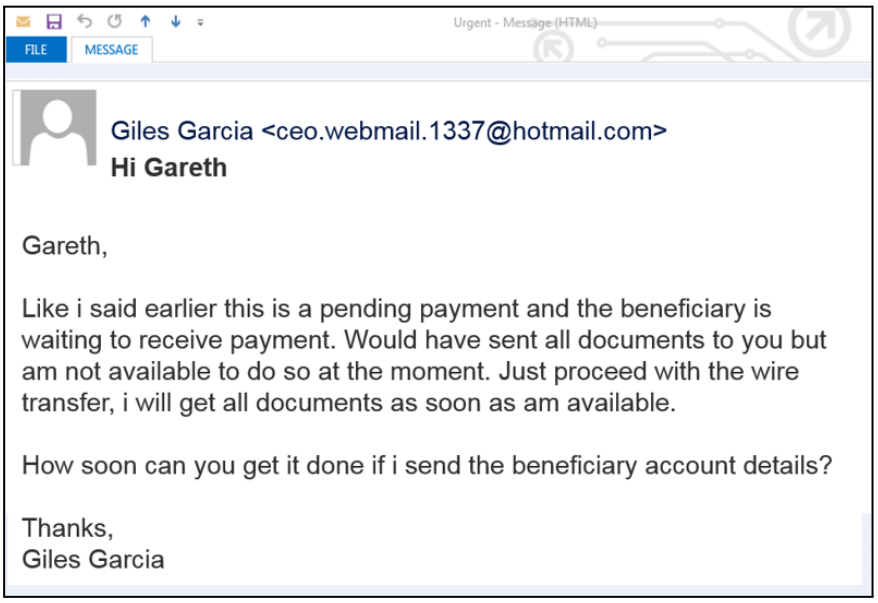
Appendix N: Email Phishing Example



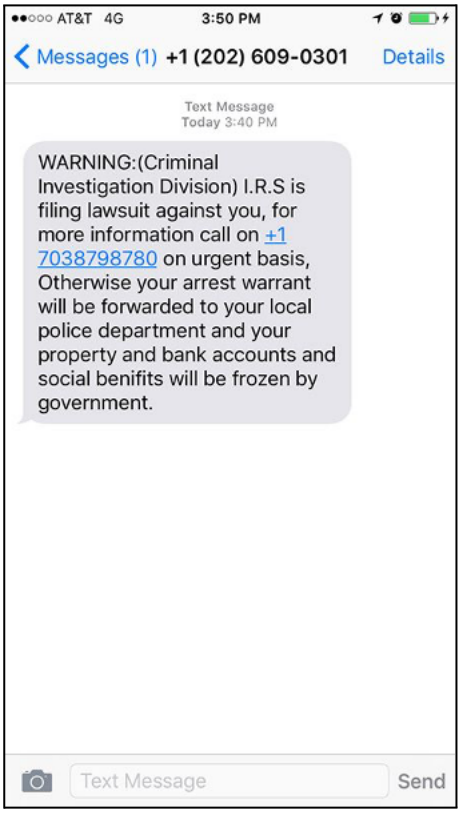
Appendix O: Spear Phishing Example



Appendix P: Whaling Example



Appendix Q: Smishing Example



Appendix R: What is Vishing and How Prevent it