Understanding Software Security

Presented by: Devin Young

CTEC 450: Case Studies in Computer Security

Dr. Jackson

What is Software Security?

- Software security is the practice of protecting applications from malicious attacks and vulnerabilities
- It is important because it helps protect sensitive data, maintain customer trust, and prevent financial losses
- Software vulnerabilities can lead to data breaches, financial loss, and reputational damage because they create weak points within an application or system that threat actors can exploit, which would affect the confidentiality, integrity, and availability of data within the company

Common Vulnerabilities & Exploits >>>

Phishing Attacks

- Attempts to obtain sensitive information by pretending to be a trustworthy entity

Real-world security breach that occurred due to this vulnerability:

- “In 2020, U.S. healthcare provider Elara Caring was subjected to a phishing attack that targeted two employees” (8 Devastating Phishing Attack Examples, 2025)

- “With only these two compromised targets, attackers gained access to employee email accounts and compromised the personal information of more than 100,000 elderly patients” (8 Devastating Phishing Attack Examples, 2025)

Phishing Attacks Explained

Phishing is a cybercrime in which **scammers** try to lure you into giving up your personal information by impersonating a trusted source. Phishers can trick you through:

Text messages
Emails
Phone calls

(Stouffer, 2024)x

Malware (ransomware)

- Malicious software designed to damage or gain unauthorized access to systems

Real-world security breach that occurred due to this vulnerability:

- “CISA and the FBI said attackers deploying Ghost ransomware have breached victims from multiple industry sectors across over 70 countries, including critical infrastructure organizations” (Gatlan, 2025)

Vulnerabilities Targeted:

- This financially motivated ransomware group targets vulnerabilities left unpatched in Fortinet: CVE-2018-13379, ColdFusion: CVE-2010-2861, CVE-2009-3960, and Exchange: CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 (Gatlan, 2025)

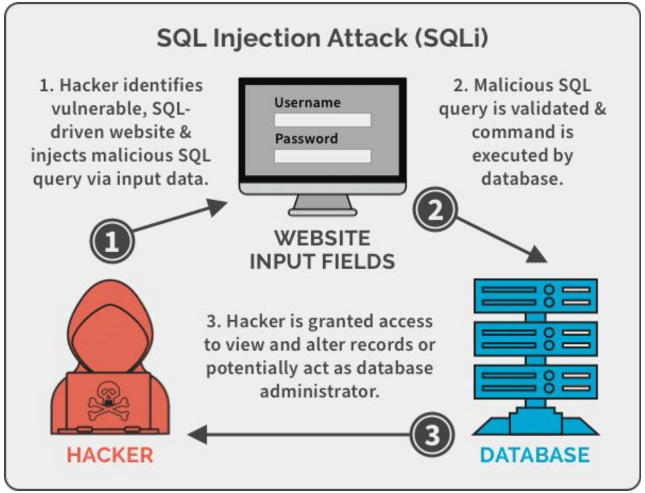
(Graham, 2025)

SQL Injection

- Involves a threat actor inserting malicious SQL code into input fields, allowing unauthorized access to a database

Real-world security breach that occurred due to this vulnerability:

- A hacking group named GambleForce used SQL injections and exploited vulnerabilities in the content management systems (CMS) of organizations in the gambling, government, retail, and travel sectors, to steal sensitive information, including user credentials (Arghire, 2023)
- Relied on open-source and publicly available tools (Arghire, 2023)


SQL Injection Attack (SQLi)
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
Username
Password
2. Malicious SQL query is validated & command is executed by database.
1
2
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator.
3
HACKER
DATABASE

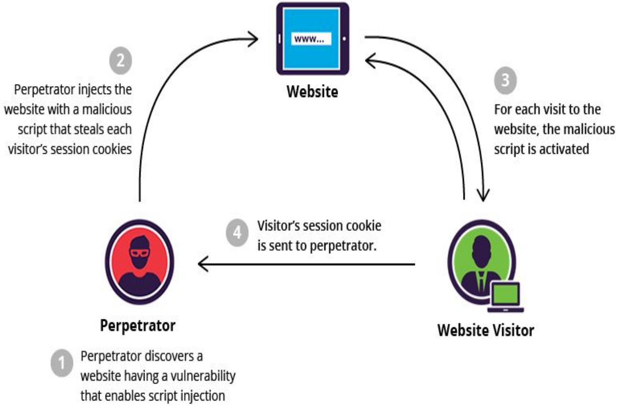
(SQL Injection Attacks — Web-based App Security, Part 4 | Spanning, 2019)

Cross Site Scripting (XSS)

- Consists of malicious scripts being injected into websites to attack users and steal data

Real-world security breach that occurred due to this vulnerability:

- “The hacking group, tracked as ResumeLooters, has been active since early 2023, selling the stolen information on Chinese-speaking hacking-themed Telegram groups” (Arghire, 2024)
- “ResumeLooters has also used XSS scripts injected into legitimate job search websites, meant to display phishing forms and harvest administrative credentials” (Arghire, 2024)
- The scripts were executed on at least four websites and on some devices with administrative access (Arghire, 2024)


www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

(Naer, 2023)

Weak Passwords

- Passwords that are easily guessed or cracked, making systems vulnerable

Real-world security breach that occurred due to this vulnerability:

- Northern Irish Parliament - In 2018, the accounts of elected officials were compromised by a brute force attack, with hackers gaining access by using a list of commonly used passwords (Walker, 2023)

(Securedatamgt, 2016)

Importance of Security and Best Practices >>>

Why Security Matters to the Company

Legal Penalties:

- Companies face fines if they fail to protect user data.

Customer Trust:

- A breach can cause long-term damage to customer loyalty.

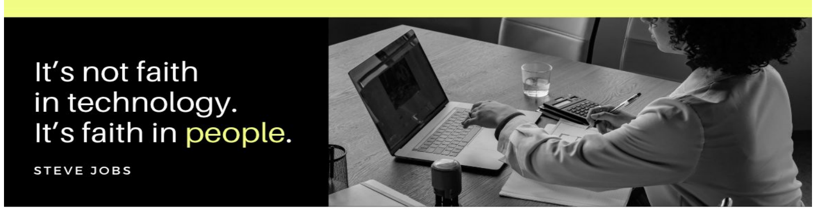
Operational Disruptions:

- Recovery efforts and system downtime can halt business operations.

Average Recovery Costs:

- The average recovery costs for a data breach in 2024 was $4.88 million, which includes efforts to investigate the breach and restore compromised systems, notifying affected users, identity theft protection for affected users, legal fees, reputation management efforts, and possible ransomware fees (Moore, 2025)

Best Practices for Non-Technical Staff



1. Create strong complex passwords
2. Avoid reusing passwords across multiple sites
3. Be cautious with emails, links, or attachments from unknown sources
4. Look out for poor grammar, an unusual sense of urgency, and suspicious sender addresses in emails
5. Verify requests for sensitive information through other channels of communication
6. Continue to update software regularly
7. Avoid public Wi-Fi for work activities
8. Report Suspicious Activities
9. Stay updated on new threats

In addition:

- Always use multi-factor authentication

Best Practices for Technical Teams

Secure Coding:

- Validate input, avoid hardcoding secrets, use strong cryptography.

Dev Pipeline:

- Automate security testing (static, dynamic), integrate vulnerability scans.

Threat Modeling:

- Identify risks, update threat models, apply security controls.

Authentication/Authorization:

- Use MFA, enforce strong passwords, implement RBAC.

Software Design:

- Modular architecture, secure protocols, session management.

Best Practices for Technical Teams

Vulnerability Assessments:

- Regular penetration testing, patch management.

Security Training:

- Educate developers on secure coding, phishing, and social engineering.

Incident Response:

- Have a plan, conduct drills, review after incidents.

Deployment & Maintenance:

- Secure configurations, least privilege, continuous monitoring.

Compliance:

- Follow regulatory standards, protect data, and conduct audits.

Bibliography

Arghire, I. (2024, February 6). Millions of User Records Stolen From 65 Websites via SQL Injection Attacks. SecurityWeek. https://www.securityweek.com/millions-of-user-records-stolen-from-65-websites-via-sql-injection-attacks/

Arghire, I. (2023, December 14). New Threat actor Uses SQL Injection Attacks to Steal Data From APAC Companies. SecurityWeek. https://www.securityweek.com/new-threat-actor-uses-sql-injection-attacks-to-steal-data-from-apac-companies/

8 Devastating Phishing Attack Examples (and Prevention Tips). BlueVoyant. (n.d.). https://www.bluevoyant.com/knowledge-center/8-devastating-phishing-attack-examples-and-prevention-tips

Gatlan, S. (2025, February 19). CISA and FBI: Ghost ransomware breached orgs in 70 countries. BleepingComputer. https://www.bleepingcomputer.com/news/security/cisa-and-fbi-ghost-ransomware-breached-orgs-in-70-countries/

Graham, K. (2025, January 6). Top 7 ransomware attack vectors. Bitsight. https://www.bitsight.com/blog/top-7-ransomware-attack-vectors-and-how-avoid-becoming-victim

Bibliography

Moore, J. (2025, February 5). What is the Average Recovery Cost of Cyberattacks?. ElevityIT. https://www.elevityit.com/blog/cost-to-recover-from-a-cyberattack

Naer, S. (2023, December 20). What is XSS | Stored Cross Site Scripting Example | Imperva. Learning Center. https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/

Securedatamgt. (2016, March 21). Passwords all employees should avoid - Secure Data MGT. Secure Data MGT. https://www.securedatamgt.com/passwords-all-employees-should-avoid/

SQL Injection Attacks — Web-based App Security, Part 4 | Spanning. (2019, July 18). Spanning. https://www.spanning.com/blog/sql-injection-attacks-web-based-application-security-part-4/

Stouffer, C. (2024, December 30). What is phishing? How to spot and avoid it. https://us.norton.com/blog/online-scams/what-is-phishing

Walker, C. (2023, May 4). The Top 4 Instances When a Weak Password Led to a Major Hacking Incident. Cybernews. https://cybernews.com/security/cost-of-week-password-hacking