James Galbreath

6/11/25

CS-405

In May 2023, a major security breach involving MOVEit Transfer, a popular file-sharing tool used by businesses and government agencies, caught worldwide attention. A vulnerability that was previously unknown to the developers was being exploited through SQL injection attacks. Unfortunately, this led to a massive amount of user information being leaked such as social security numbers, banking information, and health records. This small security flaw would impact hundreds of people before it was discovered. CIOp ransom group was find to be the culprits of this attack.

MOVEit transfer is used many large companies and government organizations making them a prime target for attacks. The immediate risk was the exposure of private information, but the potential long-term effects were just as serious things like identity theft, financial fraud, and targeted phishing attacks. A situation like this could have been avoided by building more secure software from the start. Developers should always validate and sanitize user input to block attacks like SQL injection. Regular code reviews, vulnerability scans, and tools like web application firewalls could have helped detect and block the attack sooner. Organizations also benefit from strong policies like secure software development processes and regular patching schedules to stay ahead of these kinds of threats.

Ultimately, this case is a powerful reminder of the importance of cybersecurity best practices. Using layers of defense what’s known as "defense in depth" helps reduce risk even if one layer fails. Simple but critical safeguards like multi-factor authentication, proper user access controls, and thorough logging (for tracking who accessed what and when) all work together to keep systems safe. The MOVEit breach shows how even trusted software can become an attack vector, and why secure development and strong policies are essential for protecting sensitive data.