In the summary of the Case Study of Security Testing at Twitter, Twitter grew from 2.5 million to 10million daily users in 2009. (Kim et al., 2016) It had problems for many years which many users would see their fail error page of a whale. The security problems during this time were frequent and Twitter had two of their first most serious breaches in security would happen in 2009. (Kim et al., 2016)

The security breach had President Barrack Obama’s account hacked, then later the admin accounts of twitter were backed with brute-force dictionary attack. (Kim et al., 2016) These two breaches of security would make the Federal Trade Commission dictate that “Twitter was misleading its users into believing that their accounts were secure” (Kim et al., 2016) Which then the Federal Trade Commission would issue their “consent order” which would force Twitter to create new processes that would be set for the future. (Kim et al., 2016) The following actions were taken: They would have to set employees responsible for the security plan, then Identify every risk they were aware of and a plan for mitigation (Kim et al., 2016) Also be able to maintain user privacy.

There were a few problems Twitter needed to fix:

* Prevention of repeated security mistakes
* Create new security objectives into their current developer tools
* Maintain the amount of trust they have in the development of Twitter
* Keep the “flow through infosec through automation” (Kim et al., 2016)
* Create a way for security to be “self-service” (Kim et al., 2016)

As the years passes Twitter was able to achieve their goals by implementing a tool called Brakeman. Brakeman helps find the security vulnerabilities in their code by 60%. (Kim et al., 2016)

Reference:

Kim, G., Debois, P., Willis, J. O., & Humble, J. (2016). *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. https://dl.acm.org/citation.cfm?id=3044729