AdvSQLi: Generating Adversarial SQL Injections Against Real-World WAF-as-a-Service

The increasing reliance on web applications has made them prime targets for various cyber threats, with SQL injection (SQLi) being one of the most prevalent attack methods. To combat such threats, Web Application Firewalls (WAFs) have emerged as critical defensive layers. However, the advent of WAF-as-a-Service (WAFaaS) has raised concerns about their security vulnerabilities, especially as many of these services are deployed in cloud environments. The paper titled "AdvSQLi: Generating Adversarial SQL Injections Against Real-World WAF-as-a-Service" addresses these vulnerabilities by proposing a novel attack framework designed to bypass WAFaaS solutions.

AdvSQLi represents a significant advancement in the field of web security by introducing a systematic approach to generate adversarial SQLi payloads that maintain the original functionality and malicious intent of the attack while successfully evading detection by WAFs. The framework employs a hierarchical tree representation of SQLi payloads, allowing for fine-grained manipulation of the payload structure. By utilizing a weighted mutation strategy based on context-free grammar, AdvSQLi generates a diverse set of equivalent SQLi payloads. This method preserves the semantics of the original payload, ensuring that the generated attacks remain effective while circumventing WAF defenses.

The evaluation of AdvSQLi demonstrates its effectiveness against various state-of-the-art machine learning-based SQLi detectors and seven mainstream WAFaaS solutions, including AWS, Cloudflare, and F5. The results indicate that AdvSQLi achieves a maximum attack success rate (ASR) of 100% against these detectors, with notable success rates of over 79% against specific WAFs like F5. This highlights the critical deficiencies in current WAF detection mechanisms, particularly their reliance on non-robust signatures and inadequate handling of JSON-type parameters.

Moreover, the paper outlines the vulnerabilities identified in WAFaaS products, emphasizing the need for vendors to enhance their security measures. The authors conducted responsible disclosure of their findings to affected vendors, leading to prompt responses and improvements in some cases. The study also explores potential defense mechanisms, such as adversarial training and pre-processing methods, although it notes that these approaches have limitations in defending against unknown adversarial attacks.

In conclusion, AdvSQLi represents a pioneering effort to systematically assess and exploit the vulnerabilities of WAF-as-a-Service solutions. By effectively generating adversarial SQLi payloads that bypass detection, this framework underscores the urgent need for improved security measures in web application defenses. The findings serve as a wake-up call for vendors to enhance their WAF technologies to better protect against evolving threats in the cybersecurity landscape.