TU Clausthal

Abschlussvortrag Masterarbeit Muhammad Danish

„Automatic Detection of Login Vulnerabilities in REST APIs Using black-box Testing“

In the recent 2023 survey conducted by OWASP, broken authentication has been identified as the second most common type of security vulnerability impacting web APIs. Addressing this critical issue, our research paper introduces ”SecuREST,” a cutting-edge, black-box methodology designed for the automatic detection of three specific vulnerabilities within the broken authentication category affecting APIs. These vulnerabilities encompass scenarios such as the allowance of credential stuffing, the capability for password brute force attacks without implementing account lockout mechanisms, and the acceptance of invalid or non-authenticated tokens within requests.
Our proposed SecuREST method utilizes information derived from an API’s specification to autonomously identify potential targets for attack. It does so by pinpointing API operations and parameters that could be exploited. Following the identification process, SecuREST generates tailored security testing scenarios aimed at exploiting these identified vulnerabilities through a series of HTTP interactions with the target API. The execution trace of these HTTP requests is then meticulously analyzed by our oracles, which are designed to detect and report any non-conforming behavior as indicative of potential vulnerabilities within the API.
The efficacy of the SecuREST approach has been rigorously tested and validated against a selection of real-world public APIs. The results from these tests have demonstrated the method’s high effectiveness in identifying and uncovering security vulnerabilities, thereby underscoring the potential of our approach to significantly enhance the security posture of web APIs against the prevalent threat of broken authentication.

Betreuer der Arbeit:	Prof. Dr. Mohammad Ghafari, PD Dr. Christoph Knieke
Datum:	Freitag, 22. März 2024, 11:00 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/rooms/rfy-mjv-xdx-scg/join