TU Clausthal

Abschlussvortrag Masterarbeit Abdul Moiz Ahmed

„Mining Mass Assignment Vulnerabilities“

The security of Application Programming Interface (APIs) has become critical in today's software landscape because of its crucial role in modern web applications. Securing APIs or a complete web application is a major priority for companies due to the growing concerns about data privacy. To mitigate such risks, the Open Web Application Security Project (OWASP) has released a guide known as the OWASP Top 10 API Security Risks. They outline the most critical vulnerabilities that pose the greatest security threats; however, there is no detailed method of attack and it is countermeasures. Among the most critical API security risks is Mass Assignment Vulnerability (MAV), ranked sixth in the OWASP Top 10 in 2019, which is difficult to detect. Mass Assignment Vulnerabilities (MAVs) occur when user-supplied input bound to model attributes improperly, this allows attackers to change sensitive fields that should not be accessible by users, leading to unauthorized actions or privilege escalation. Therefore, this research presents a comprehensive evaluation of existing open source tools designed to detect MAV in either APIs or complete web applications with a specific focus on Ruby on Rails projects. A test set was developed using a diverse set of publicly available APIs and applications, and each tool was extensively tested to evaluate its effectiveness. This study identifies the strengths and limitations of these tools, provides valuable information on their performance, and contributes to ongoing efforts to improve security for APIs and web applications by helping developers and businesses choose the most effective tools for detecting and mitigating MAVs, leading to a safer online experience for everyone. It also highlights the need for detection technologies that can work across various frameworks and programming languages.

This research highlights the need for the continued development and refinement of these tools to fully address the challenges caused by MAVs. In addition, through systematic testing, we developed patterns to find MAV symptoms, particularly in Ruby on Rails applications. Using more prevalent patterns we mined GitHub using GitHub's Code Search REST API to find the repositories that have these symptoms of MAV and verify how effective are these patterns.

Betreuer der Arbeit:	Prof. Dr. Mohammad Ghafari, PD Dr. Christoph Knieke
Datum:	Montag, 30. September 2024, 14:00 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/rooms/p6f-ppi-v17-lwe/join