Zurich University
of Applied Sciences

School of
Engineering

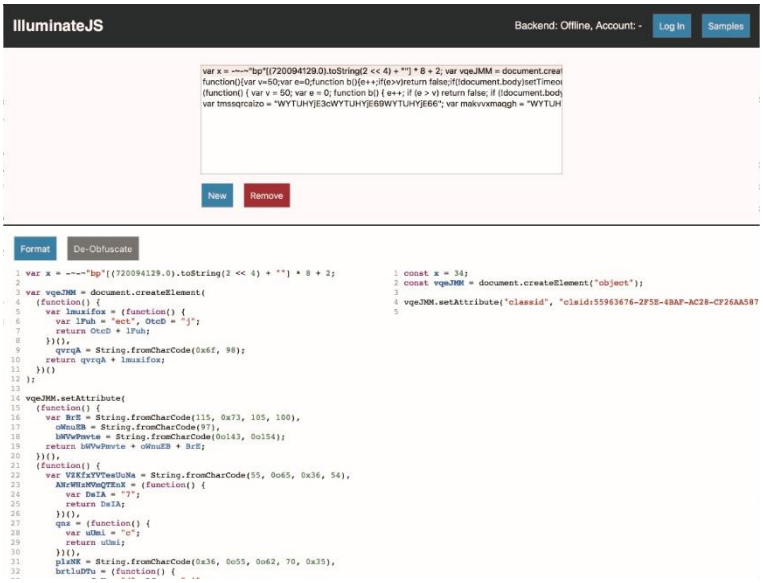
InIT Institute of Applied
Information Technology

De-Obfuscating JavaScript Using Static Analysis

Diplomand
Lucas Neiva

Dozent
Bernhard Tellenbach

Obfuscation is a method of transforming source code into equivalent code that is harder to read, classify, and analyse. Use cases include evading signature based malware scanners and intellectual property protection. In the case of malware, automated de-obfuscation could allow for improved detection and analysis. De-Obfuscation is the opposite transformation. It aims to partially reverse the process in order to ease analysis of obfuscated code.
This bachelor thesis analyzes JSDetox, a well-known JavaScript de-obfuscation tool, and proposes nine de-obfuscation features that go beyond the capabilities of JSDetox. To evaluate these features, a custom de-obfuscation tool has been developed. The tool implements them as abstract syntax tree (AST) transformations, which partially evaluate and simplify code statically. Results show that it allows for more information to be extracted from malware samples than with JSDetox.



Web-based application that can de-obfuscate malicious JavaScript code for analysis.