9 August 2019 Study · Mobile Security · Web & Cloud

Detection of Code Injection Vulnerabilities in HTML5 Apps

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Version 2019-08-09
Source https://technology2.a-sit.at/en/publications/detection-of-code-injection-vulnerabilities-in-html5-apps/

In order to develop mobile cross-platform applications, frameworks based on JavaScript and HTML5 are often used. Unfortunately, such applications do not only bring the advantage of platform independence, but also the vulnerabilities of browser applications, especially the ability to inject potentially malicious code. This report presents a tool that can detect and evaluate the use of Content Security Policy (CSP), a browser feature that can protect against code injection. It also shows how to determine whether an application that does not use CSP or uses it in an insecure manner is vulnerable to code injection via Apache Cordova plug-ins.