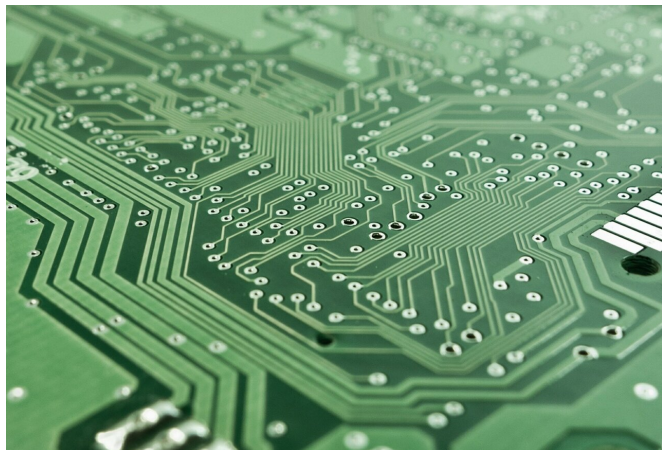


High-performance detection tool for ReDoS-vulnerability

16 August 2021, by Zhang Nannan



Credit: Pixabay/CC0 Public Domain

Regular expressions (regexes) are widely used in different fields of computer science. However, the Regular expression Denial of Service (ReDoS) vulnerability forms a class of common and serious algorithmic complexity attacks.

The existing ReDoS-vulnerability detection tools have defects of low precision or low recall rate due to the lacking of formal and comprehensive detection conditions of ReDoS-vulnerabilities.

A research team led by Prof. Chen Haiming from the Institute of Software of the Chinese Academy of Sciences developed high-performance detection tool for ReDoS-vulnerability.

Their study was issued at USENIX Security Symposium 2021.

Through examining massive ReDoS-vulnerable regexes, Chen's team proposed the ReDoS-vulnerability detection conditions, namely the ReDoS-vulnerability patterns, and gave the necessary conditions for triggering these patterns

formally.

Based on this, they developed a static and dynamic combined ReDoS-vulnerability detection [algorithm](#), and designed ReDoSHunter, the ReDoS-vulnerability detection tool.

ReDoSHunter can pinpoint multiple root causes in a vulnerable regex, prescribe the degree of the vulnerability and generate attack-triggering strings, etc. It has achieved 100% precision and recall ratio on datasets of Corpus, RegExLib and Snort with 37,651 regexes.

In detecting the publicly-confirmed practical vulnerabilities in Common Vulnerabilities and Exposure (CVE), ReDoSHunter can detect 100% ReDoS-related CVEs.

In their previous study, Chen's team proposed a programming-by-example framework, FlashRegex, for generating anti-ReDoS regexes by either synthesizing or repairing from given examples. It is the first framework that integrates regex synthesis and repair with the awareness of ReDoS-vulnerabilities.

FlashRegex can efficiently generate or repair regexes without ReDoS-vulnerabilities, and there're 0 ReDoS-vulnerabilities in repaired regexes.

The study, titled "FlashRegex: deducing anti-ReDoS regexes from examples," was issued at ASE 2020.

More information: Yeting Li et al, FlashRegex, *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering* (2021). [DOI: 10.1145/3324884.3416556](https://doi.org/10.1145/3324884.3416556)

Provided by Chinese Academy of Sciences

APA citation: High-performance detection tool for ReDoS-vulnerability (2021, August 16) retrieved 16 October 2021 from <https://techxplore.com/news/2021-08-high-performance-tool-redos-vulnerability.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.