SOFTWARE TESTING, VERIFICATION AND RELIABILITY
Softw. Test. Verif. Reliab. 2021; **00**:1–37
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/stvr

Combinatorial Methods for Dynamic Gray-Box SQL Injection Testing

Bernhard Garn
bgarn@sba-research.org
Jovan Zivanovic
jzivanovic@sba-research.org
Manuel Leithner
mleithner@sba-research.org
Dimitris E. Simos
dsimos@sba-research.org

SBA Research, 1040 Vienna, Austria

SUMMARY

This work presents an extended and enhanced gray-box combinatorial security testing methodology for *SQL* injection vulnerabilities in web applications. We propose multiple new attack grammars modelling SQLi attacks against MySQL-compatible databases, each one targeting a different injection context. Additionally, these grammars are also dynamically refined at the beginning of each attack against an endpoint of a web application, as a further optimization of the used attack model by taking into account the specifics of the generated query of that endpoint. Our goal is to enhance existing combinatorial approaches for detecting SQL injection vulnerabilities. The newly developed methodology is implemented in a prototype security testing tool called *SQLInjector+*, which is an extension of an earlier prototype developed by us in prior work. This improved tool can attack (i.e., test) any web application that uses a MySQL-compatible database management system. We evaluate our revised approach and improved prototype tool in a case study comprising of different kinds of web applications to which SQLi is a potential security threat. The case study contains the well-known verification framework WAVSEP among other five real-world web applications and one web application firewall. Our generated attack vectors, constructed via combinatorial methods applied to our improved and dynamically optimized attack grammars, are capable of injecting every known vulnerable endpoint in WAVSEP and also of finding new vulnerable parameters in some of the real-world applications investigated in this paper. Our approach performs equally well or better when compared to existing state-of-art of *SQL* injection security testing tools (sqlmap, w3af, wapiti and fuzzdb) across all tested web applications in the case study. Copyright © 2021 John Wiley & Sons, Ltd.

Received . . .

KEY WORDS: Combinatorial testing, security testing, gray-box testing, SQL injection, web applications

1. INTRODUCTION

SQL injection (*SQLi*) is a well-known type of command injection attack, where an attacker attempts to insert additional content into SQL queries produced by an application that uses databases (DBs) to store and retrieve information. *SQLi*s are some of the most common and most critical vulnerabilities found in web applications according to the most recent OWASP Top 10 report [47] published in 2017 and prior releases [45, 46]. This is despite the fact that there exists a large body of work dedicated to this topic, both in terms of detecting and defending against such flaws.

[*] Correspondence to: Dimitris E. Simos, dsimos@sba-research.org, SBA Research, 1040 Vienna, Austria