Institut für Theoretische Informatik
Arbeitsgruppe Kryptographie und Sicherheit

Prof. Dr. Jörn Müller-Quade
Prof. Dr. Dennis Hofheinz

Karlsruher Institut für Technologie

Application Security

Investigating and Validation of NoSQL Injection Vulnerabilites

Master Thesis

of Computer Science

by

Patrick Spiegel

Date:	May 11, 2016
Period of processing:	01. April - 30. September 2016
Matriculation number:	1854488
Primary Reviewer:	Prof. Dr. Jörn Müller-Quade
Secondary Reviewer:	Prof. Dr. Dennis Hofheinz
Company Supervisor:	Dr. Martin Johns

Statement of Authorship

I declare that I have developed and written the enclosed thesis completely by myself, and have not used sources or means without declaration in the text.

Karlsruhe, May 11, 2016

Abstract

Contents

Statement of Authorship I

List of Figures V

List of Tables VI

List of Listings VII

List of Abbreviations VIII

1 Introduction 1
- 1.1 Motivation . . . 1
- 1.2 Objective . . . 1
- 1.3 Structure . . . 1

2 Technical Background 2
- 2.1 SQL Databases . . . 2
  - 2.1.1 General Approach . . . 2
  - 2.1.2 SQL Injection . . . 2
- 2.2 NoSQL Databases . . . 2
  - 2.2.1 General Approach . . . 2
  - 2.2.2 Types of NoSQL Databases . . . 2
  - 2.2.3 NoSQL Technologie Stack . . . 2
- 2.3 NoSQL Underlying Technologies . . . 2
  - 2.3.1 HTTP . . . 2
  - 2.3.2 REST . . . 2
  - 2.3.3 JavaScript . . . 2

3 Conception 3
- 3.1 Paradim Shift for NoSQL Queries . . . 3
- 3.2 Approaches for Injection Attacks . . . 3
  - 3.2.1 Altered Object Type Injection . . . 3
  - 3.2.2 Function Injection . . . 3

4 NoSQL Injection Attacks 4
- 4.1 Selected Databases . . . 4
- 4.2 Altered Object Type Injection . . . 4
  - 4.2.1 MongoDB - Node.js Attack . . . 4
  - 4.2.2 MongoDB - PHP Attack . . . 4
  - 4.2.3 Redis - Node.js Attack . . . 4
  - 4.2.4 Redis - PHP Attack . . . 4
- 4.3 Function Injection . . . 4
  - 4.3.1 CouchDB MapReduce Attack . . . 4

5 NoSQL Injection Detection 5

6 Evaluation **6**

7 Related Work **7**

8 Conclusion **8**

List of Figures

List of Tables

List of Listings

List of Abbreviations

HTTP	Hypertext Transfer Protocol
NoSQL	Not only Structured Query Language
SQL	Structured Query Language

1 Introduction

1.1 Motivation

1.2 Objective

1.3 Structure

2 Technical Background

2.1 SQL Databases

2.1.1 General Approach

2.1.2 SQL Injection

2.2 NoSQL Databases

2.2.1 General Approach

2.2.2 Types of NoSQL Databases

2.2.3 NoSQL Technologie Stack

2.3 NoSQL Underlying Technologies

2.3.1 HTTP

2.3.2 REST

2.3.3 JavaScript

3 Conception

3.1 Paradim Shift for NoSQL Queries

3.2 Approaches for Injection Attacks

3.2.1 Altered Object Type Injection

3.2.2 Function Injection

4 NoSQL Injection Attacks

4.1 Selected Databases

4.2 Altered Object Type Injection

4.2.1 MongoDB - Node.js Attack

4.2.2 MongoDB - PHP Attack

4.2.3 Redis - Node.js Attack

4.2.4 Redis - PHP Attack

4.3 Function Injection

4.3.1 CouchDB MapReduce Attack

5 NoSQL Injection Detection

6 Evaluation

7 Related Work

8 Conclusion