



Nutzbar für
alle SQL-Daten-
banken. Spezial-
wissen zu Oracle,
MS SQL Server,
MySQL und
PostgreSQL.

Justin Clarke

SQL Hacking

SQL-Injektion auf relationale Datenbanken im
Detail verstehen und abwehren.

- Anfälligkeit für SQL-Injektion erkennen, ausnutzen und Schäden beseitigen
- Angriffe auf Datenbanken detailliert im Quellcode nachvollziehen
- Tools kennen und nutzen: Automatisierte Quellcodeprüfung, Automatisierung der blinden SQL-Injektion und mehr

Justin Clarke
SQL-Hacking

Justin Clarke

SQL Hacking

SQL-Injektion auf relationale Datenbanken im Detail verstehen und abwehren.

- Anfälligkeit für SQL-Injektion erkennen, ausnutzen und Schäden beseitigen
- Angriffe auf Datenbanken detailliert im Quellcode nachvollziehen
- Tools kennen und nutzen: Automatisierte Quellcodeprüfung, Automatisierung der blinden SQL-Injektion und mehr

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Alle Angaben in diesem Buch wurden vom Autor mit größter Sorgfalt erarbeitet bzw. zusammengestellt und unter Einschaltung wirksamer Kontrollmaßnahmen reproduziert. Trotzdem sind Fehler nicht ganz auszuschließen. Der Verlag und der Autor sehen sich deshalb gezwungen, darauf hinzuweisen, dass sie weder eine Garantie noch die juristische Verantwortung oder irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernehmen können. Für die Mitteilung etwaiger Fehler sind Verlag und Autor jederzeit dankbar. Internetadressen oder Versionsnummern stellen den bei Redaktionsschluss verfügbaren Informationsstand dar. Verlag und Autor übernehmen keinerlei Verantwortung oder Haftung für Veränderungen, die sich aus nicht von ihnen zu vertretenden Umständen ergeben. Evtl. beigefügte oder zum Download angebotene Dateien und Informationen dienen ausschließlich der nicht gewerblichen Nutzung. Eine gewerbliche Nutzung ist nur mit Zustimmung des Lizenzinhabers möglich.

This edition of **SQL Injections Attacks and Defense** by Justin Clarke is published by arrangement with **ELSEVIER INC.**, a Delaware corporation having its principal place of business at 360 Park Avenue South, New York, NY 10010, USA

ISBN der englischen Originalausgabe: 978-1597499637

© 2016 Franzis Verlag GmbH, 85540 Haar bei München

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Das Erstellen und Verbreiten von Kopien auf Papier, auf Datenträgern oder im Internet, insbesondere als PDF, ist nur mit ausdrücklicher Genehmigung des Verlags gestattet und wird widrigenfalls strafrechtlich verfolgt.

Die meisten Produktbezeichnungen von Hard- und Software sowie Firmennamen und Firmenlogos, die in diesem Werk genannt werden, sind in der Regel gleichzeitig auch eingetragene Warenzeichen und sollten als solche betrachtet werden. Der Verlag folgt bei den Produktbezeichnungen im Wesentlichen den Schreibweisen der Hersteller.

Autor: Justin Clarke

Programmleitung: Dr. Markus Stäuble

Satz und Übersetzung: G&U Language & Publishing Services GmbH

art & design: www.ideehoch2.de

ISBN 978-3-645-20466-8

Inhaltsverzeichnis

Danksagung.....	21
Die Autoren der Beiträge	23
Chefautor und Fachgutachter.....	26
1. Was ist SQL-Injection?.....	27
1.1 Einführung	27
1.2 Wie funktionieren Webanwendungen?.....	28
1.2.1 Eine einfache Anwendungsarchitektur	30
1.2.2 Eine kompliziertere Architektur.....	31
1.3 Wie funktioniert SQL-Injection?	32
1.3.1 Aufsehenerregende Beispiele	36
1.4 Wie kann das passieren?.....	40
1.4.1 Dynamische Stringerstellung	40
1.4.2 Falsche Behandlung von numerischen Typen.....	43
1.4.3 Falsche Behandlung von Mehrfachübertragungen.....	48
1.4.4 Unsichere Datenbankkonfiguration	50
1.5 Zusammenfassung.....	52
1.6 Schneller Überblick.....	53
1.6.1 Wie funktionieren Webanwendungen?.....	53
1.6.2 Wie funktioniert SQL-Injection?	53
1.6.3 Wie kann das passieren?.....	54
1.7 Häufig gestellte Fragen	54