

Michał Zalewski

Tangled Web

Der Security-Leitfaden für Webentwickler

Deutsche Ausgabe – Aktualisiert und erweitert von Mario Heiderich



dpunkt.verlag

Lektorat: René Schönfeldt
Copy Editing: Ursula Zimpfer, Herrenberg
Übersetzung und Satz: G&U Language & Publishing Services, Flensburg
Herstellung: Nadine Thiele
Umschlaggestaltung: Helmut Kraus, www.exclam.de
basierend auf einem Entwurf von Hugh D'Andrade
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-86490-002-0

1. Auflage 2013
German-language edition copyright © 2013 dpunkt.verlag GmbH
Ringstraße 19 B
69115 Heidelberg



Copyright © 2012 by Michał Zalewski.
Title of the English-language original: The Tangled Web, ISBN 978-1-59327-388-0,
published by No Starch Press. All rights reserved.

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

Für meinen Sohn

Inhaltsübersicht

1	Sicherheit in einer Welt der Webanwendungen	1
---	---	---

Teil I: Anatomie des Web

2	Am Anfang war die URL	29
3	HTTP	53
4	HTML	87
5	CSS	109
6	JavaScript im Browser	119
7	Nicht-HTML-Dokumente	145
8	Inhalte mit Browser-Plug-ins darstellen	157

Teil II: Sicherheitsfeatures von Browsern

9	Inhalte isolieren	177
10	Ursprungsvererbung	207
11	Die Welt außerhalb von SOPs	217
12	Sonstige Schlupflöcher	235
13	Mechanismen zur Inhaltserkennung	245
14	Umgang mit schädlichen Skripten	267
15	Webseiten mit speziellen Berechtigungen	283

Teil III: Ein Blick in die Zukunft

16	Neue und zukünftige Sicherheitsfunktionen	297
17	Weitere wichtige Browsermechanismen	323
18	Allgemeine Schwachstellen im Web	329
	Epilog	337