Steffen Schneckenburger

Uwe Dittmann, Alfred Schätter (Eds.)

Optimization of Web Application Security

Analysis of Common Threats, Countermeasures and Impact on the Software Development Lifecycle

Steinbeis-Transferzentrum
Marketing, Logistik und
Unternehmensführung an der
Hochschule Pforzheim

Steinbeis-Edition

Steffen Schneckenburger

Uwe Dittmann, Alfred Schätter (Eds.)

Optimization of Web Application Security

Analysis of Common Threats, Countermeasures and Impact on the Software Development Lifecycle

**Steinbeis-Transferzentrum
Marketing, Logistik und
Unternehmensführung an der
Hochschule Pforzheim**

Imprint

Steffen Schneckenburger | Uwe Dittmann, Alfred Schätter (Eds.)
Optimization of Web Application Security
Analysis of Common Threats, Countermeasures and Impact on the Software Development Lifecycle

1st edition 2011 | Steinbeis-Edition, Stuttgart
ISBN 978-3-941417-69-4

Layout: Steinbeis-Edition
Cover: ©iStockphoto.com/Baris Simsek
Production: Frick Werbeagentur / Frick Digitaldruck, Krumbach

Steinbeis is an international service provider in knowledge and technology transfer. The Steinbeis Transfer Network is made up of about 800 Steinbeis Enterprises and project partners in 50 countries. Specialized in chosen areas, Steinbeis Enterprises' portfolio of services covers consulting; research and development; training and employee development as well as evaluation and expert reports for every sector of technology and management. Steinbeis Enterprises are frequently attached to research establishments, universities, universities of applied sciences and universities of cooperative education.

Founded in 1971, the Steinbeis-Stiftung is the umbrella organization of the Steinbeis Transfer Network. It is headquartered in Stuttgart, Germany. Steinbeis-Edition publishes selected works mirroring the scope of the Steinbeis Network expertise.

146956-2011-06 | www.steinbeis-edition.de

Foreword

The intention of the book is all about creating awareness in terms of web application security and to support the reader with several examples as well as best practices through the development of secure web applications. Software developers and their customers often do not realize the importance of these requirements within a contract or at least define them superficially. For this reason the objective of the book is to develop an annex comprising common threats and countermeasures as well as necessary adjustments of the software development lifecycle in terms of security to establish a common basis of security understanding between developers, managers, customers and other stakeholders. As a result this book is directed to anyone from developer to decision-maker who wants to get an overview of current web application security flaws and corresponding countermeasures.

The book introduces current web application security threats and elaborates countermeasures in order to avoid or at least to reduce the impact of these flaws. In addition the security software development lifecycle of Microsoft is evaluated in order to avoid flaws in the first place.

Several critical web application vulnerabilities are identified based on intensive research. They were individually ranked according to the related risks. The top five risks elaborated are the following:

- Social Engineering
- (Blind) SQL Injection
- Brute Force
- Insecure Direct Object Reference
- Security Misconfiguration

Management summary

This book introduces current web application security threats based on literature research. Countermeasures are elaborated in order to avoid or at least to reduce the impact of these flaws. In addition the security software development lifecycle of Microsoft is evaluated in order to avoid flaws in the first place. The intention of this book is all about creating awareness in terms of web application security and to support the reader with several examples as well as best practices through the development of secure web applications.

Table of Contents

List of Abbreviations

AJAX	Asynchronous JavaScript and XML
API	Application Programming Interface
AS / NZS	Australian / New Zealand Standard
ASCII	American Standard Code for Information Interchange
CEO	Chief Executive Officer
CGI	Common Gateway Interface
CIA	Confidentiality, Integrity and Availability
CMS	Content Management System
COM	Component Object Model
CSI	Computer Security Institute
CSRF	Cross-site Request Forgery
CSS	Cascading Style Sheets
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DBMS	Database Management System
DMZ	Demilitarized Zone
EJB	Enterprise Java Beans
FBI	Federal Bureau of Investigation
FSR	Final Security Review
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Information Technology

JAAS	Java Authentication and Authorization Service
JDBC	Java Database Connectivity
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MS	Microsoft®
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PHP	Hypertext Preprocessor
RFI	Remote File Include
SANS	SysAdmin, Networking and Security Institute
SDL	Security Software Development Lifecycle
SMB	Server Message Block
SQL	Structured Query Language
SSL	Secure Sockets Layer
SW	Software
TLS	Transport Layer Security
UML	Unified Modeling Language
URL	Uniform Resource Locator
US	United States
WASC	Web Application Security Consortium
WWW	World Wide Web
XSS	Cross-site Scripting

List of Illustrations

1 Introduction

1.1 Problem Statement

"Information is the currency of the new millennium."
(Crowell 2001)

William P. Crowell, former president and chief executive officer (CEO) of the Cylink Corporation, already identified information as the currency of the millennium in 2001. This fact tightens now nine years later by the increasing popularity of social networks and other web 2.0 developments where people divulge a large quantity of private information to the service provider whereof the related business model depends. On the one hand trust will be the critical success factor in the web 2.0 environment (McClure 2008, 36). On the other hand attacks against web applications have expanded and become even worse with the recent trends towards richer web 2.0 applications (Mehta 2008, 26). The focus has moved to application layer vulnerabilities because of the increasing security level of operating systems (NSA 2007, 1). Furthermore security weaknesses in web applications are often easy to exploit and not just feasible for professional hackers. The National Institute of Standards and Technology (NIST) recorded over 6,600 vulnerabilities with an upward trend already in 2006 (NSA 2007, 1).

The attackers' motives have changed over time from personal prestige to financial fraud today. The possible impact on the e-commerce is remarkable according to a survey conducted in the United States (US) which discovered that over 60 percent of clients would neglect doing business with a company if their personal data were at risk due to unsecure web applications (Clusif 2010, 6).

There are numerous reasons for the necessity of web application security. Web applications offer new and valuable ways to interact with customers but they also expose organizations to significant risks. 50 percent of all web applications have major vulnerabilities according to the SysAdmin, Networking and Security (SANS) Institute and 80 percent of successful attacks against organizations are caused by the exploitation of these flaws (Mehta 2008, 27). The extent of the problem is hard to measure. The parties involved are often even unaware when such attacks occur until the financial