Web Security: A WhiteHat Perspective

Security of Browser

In late 2013, approximately 40 million customer debit and credit cards were leaked in a data breach at Target. This catastrophic event, deemed one of the biggest data breaches ever, clearly showed that many companies need to significantly improve their information security strategies. **Web Security: A White Hat Perspective** presents a comprehensive guide to web security technology and explains how companies can build a highly effective and sustainable security system.

In this book, web security expert Wu Hanqing reveals how hackers work and explains why companies of different scale require different security methodologies. With in-depth analysis of the reasons behind the choices, the book covers client script security, server applications security, and Internet company security operations. It also includes coverage of browser security, cross-sites script attacks, click jacking, HTML5/PHP security, injection attacks, authentication, session management, access control, web frame security, DDOS, leaks, Internet transactions security, and the security development lifecycle.

This excerpt from chapter 2 focuses on major browser security issues, including same-origin policy, sandboxing, malicious URL intercepts, and the continuing rapid development of security.

Excerpted with permission from the publisher, Auerbach Publications, from "**Web Security: A WhiteHat Perspective**" by Hanqing Wu and Liz Zhao. Copyright ©2015.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- Browser Security.pdf

This excerpt examines program leadership and the role it plays as a critical success factor for facilitating work integration, stakeholder engagement, objective alignment, organizational change readiness, and benefits realization.