1. Record Nr. UNINA9910971306703321

Autore	Huseby Sverre H
Titolo	Innocent code : a security wake-up call for Web programmers / / Sverre H. Huseby
Pubbl/distr/stampa	New York, : John Wiley & Sons, c2004
ISBN	9786610270736 9781280270734 128027073X 9780470857472 0470857471
Edizione	[1st ed.]
Descrizione fisica	1 online resource (248 p.)
Disciplina	005.8
Soggetti	Computer security Computer networks - Security measures World Wide Web - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references (p. 209-219) and index.
Nota di contenuto	Contents; Foreword; Acknowledgments; Introduction; 0.1 The Rules; 0.2 The Examples; 0.3 The Chapters; 0.4 What is Not in This Book?; 0.5 A Note from the Author; 0.6 Feedback; 1 The Basics; 1.1 HTTP; 1.1.1 Requests and responses; 1.1.2 The Referer header; 1.1.3 Caching; 1.1.4 Cookies; 1.2 Sessions; 1.2.1 Session hijacking; 1.3 HTTPS; 1.4 Summary; 1.5 Do You Want to Know More?; 2 Passing Data to Subsystems; 2.1 SQL Injection; 2.1.1 Examples, examples and then some; 2.1.2 Using error messages to fetch information; 2.1.3 Avoiding SQL injection; 2.2 Shell Command Injection; 2.2.1 Examples 2.2.2 Avoiding shell command injection2.3 Talking to Programs Written in C/C++; 2.3.1 Example; 2.4 The Evil Eval; 2.5 Solving Metacharacter Problems; 2.5.1 Multi-level interpretation; 2.5.2 Architecture; 2.5.3 Defense in depth; 2.6 Summary; 3 User Input; 3.1 What is Input Anyway?; 3.1.1 The invisible security barrier; 3.1.2 Language peculiarities: totally unexpected input; 3.2 Validating Input; 3.2.1 Whitelisting vs. blacklisting; 3.3 Handling Invalid Input; 3.3.1 Logging; 3.4 The Dangers of Client-side Validation; 3.5 Authorization Problems;

3.5.1 Indirect access to data
3.5.2 Passing too much to the client3.5.3 Missing authorization tests; 3.5.4 Authorization by obscurity; 3.6 Protecting server-generated input; 3.7 Summary; 4 Output Handling: The Cross-site Scripting Problem; 4.1 Examples; 4.1.1 Session hijacking; 4.1.2 Text modification; 4.1.3 Socially engineered Cross-site Scripting; 4.1.4 Theft of passwords; 4.1.5 Too short for scripts?; 4.2 The Problem; 4.3 The Solution; 4.3.1 HTML encoding; 4.3.2 Selective tag filtering; 4.3.3 Program design; 4.4 Browser Character Sets; 4.5 Summary; 4.6 Do You Want to Know More?; 5 Web Trojans; 5.1 Examples
5.2 The Problem5.3 A Solution; 5.4 Summary; 6 Passwords and Other Secrets; 6.1 Crypto-Stuff; 6.1.1 Symmetric encryption; 6.1.2 Asymmetric encryption; 6.1.3 Message digests; 6.1.4 Digital signatures; 6.1.5 Public key certificates; 6.2 Password-based Authentication; 6.2.1 On clear-text passwords; 6.2.2 Lost passwords; 6.2.3 Cracking hashed passwords; 6.2.4 Remember me?; 6.3 Secret Identifiers; 6.4 Secret Leakage; 6.4.1 GET request leakage; 6.4.2 Missing encryption; 6.5 Availability of Server-side Code; 6.5.1 Insecure file names; 6.5.2 System software bugs; 6.6 Summary
6.7 Do You Want to Know More?7 Enemies of Secure Code; 7.1 Ignorance; 7.2 Mess; 7.3 Deadlines; 7.4 Salesmen; 7.5 Closing Remarks; 7.6 Do You Want to Know More?; 8 Summary of Rules for Secure Coding; Appendix A: Bugs in the Web Server; Appendix B: Packet Sniffing; B.1 Teach Yourself TCP/IP in Four Minutes; B.2 Sniffing the Packets; B.3 Man-In-The-Middle Attacks; B.4 MITM with HTTPS; B.5 Summary; B.6 Do You Want to Know More?; Appendix C: Sending HTML Formatted E-mails with a Forged Sender Address; Appendix D: More Information; D.1 Mailing Lists; D.2 OWASP; Acronyms; References; Index; A; B; C
D

Sommario/riassunto

This concise and practical book shows where code vulnerabilities lie-without delving into the specifics of each system architecture, programming or scripting language, or application-and how best to fix themBased on real-world situations taken from the author's experiences of tracking coding mistakes at major financial institutionsCovers SQL injection attacks, cross-site scripting, data manipulation in order to bypass authorization, and other attacks that work because of missing pieces of codeShows developers how to change their mindset from Web site construction to Web sit