1. Record Nr. UNINA9910457721103321

Autore	Stuttard Dafydd <1972->
Titolo	The web application hacker's handbook : finding and exploiting security flaws / / Dafydd Stuttard, Marcus Pinto
Pubbl/distr/stampa	Indianapolis, IN : , : John Wiley & Sons, Inc., , [2011] ©2011
ISBN	9781118175224 1118175220 9781283258210 1283258218 9786613258212
Edizione	[Second edition.]
Descrizione fisica	1 online resource (xxxiii, 878 pages) : illustrations
Altri autori (Persone)	PintoMarcus <1978->
Disciplina	004 005.8
Soggetti	Internet - Security measures Computer security Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record. Includes index.
Nota di contenuto	The Web Application Hacker's Handbook; Contents; Introduction; Chapter 1 Web Application (In)security; The Evolution of Web Applications; Common Web Application Functions; Benefits of Web Applications; Web Application Security; ""This Site Is Secure""; The Core Security Problem: Users Can Submit Arbitrary Input; Key Problem Factors; The New Security Perimeter; The Future of Web Application Security; Summary; Chapter 2 Core Defense Mechanisms; Handling User Access; Authentication; Session Management; Access Control; Handling User Input; Varieties of Input; Approaches to Input Handling Boundary ValidationMultistep Validation and Canonicalization; Handling Attackers; Handling Errors; Maintaining Audit Logs; Alerting Administrators; Reacting to Attacks; Managing the Application; Summary; Questions; Chapter 3 Web Application Technologies; The HTTP Protocol; HTTP Requests; HTTP Responses; HTTP Methods; URLs;

REST; HTTP Headers; Cookies; Status Codes; HTTPS; HTTP Proxies; HTTP Authentication; Web Functionality; Server-Side Functionality; Client-Side Functionality; State and Sessions; Encoding Schemes; URL Encoding; Unicode Encoding; HTML Encoding; Base64 Encoding; Hex Encoding
Remoting and Serialization FrameworksNext Steps; Questions; Chapter 4 Mapping the Application; Enumerating Content and Functionality; Web Spidering; User-Directed Spidering; Discovering Hidden Content; Application Pages Versus Functional Paths; Discovering Hidden Parameters; Analyzing the Application; Identifying Entry Points for User Input; Identifying Server-Side Technologies; Identifying Server-Side Functionality; Mapping the Attack Surface; Summary; Questions; Chapter 5 Bypassing Client-Side Controls; Transmitting Data Via the Client; Hidden Form Fields; HTTP Cookies; URL Parameters
The Referer HeaderOpaque Data; The ASP.NET ViewState; Capturing User Data: HTML Forms; Length Limits; Script-Based Validation; Disabled Elements; Capturing User Data: Browser Extensions; Common Browser Extension Technologies; Approaches to Browser Extensions; Intercepting Traffic from Browser Extensions; Decompiling Browser Extensions; Attaching a Debugger; Native Client Components; Handling Client-Side Data Securely; Transmitting Data Via the Client; Validating Client-Generated Data; Logging and Alerting; Summary; Questions; Chapter 6 Attacking Authentication; Authentication Technologies
Design Flaws in Authentication MechanismsBad Passwords; Brute-Forcible Login; Verbose Failure Messages; Vulnerable Transmission of Credentials; Password Change Functionality; Forgotten Password Functionality; ""Remember Me"" Functionality; User Impersonation Functionality; Incomplete Validation of Credentials; Nonunique Usernames; Predictable Usernames; Predictable Initial Passwords; Insecure Distribution of Credentials; Implementation Flaws in Authentication; Fail-Open Login Mechanisms; Defects in Multistage Login Mechanisms; Insecure Storage of Credentials; Securing Authentication
Use Strong Credentials

Sommario/riassunto

The highly successful security book returns with a new edition, completely updated Web applications are the front door to most organizations, exposing them to attacks that may disclose personal information, execute fraudulent transactions, or compromise ordinary users. This practical book has been completely updated and revised to discuss the latest step-by-step techniques for attacking and defending the range of ever-evolving web applications. You'll explore the various new technologies employed in web applications that have appeared since the first edition and review the new attack