

1. Record Nr.	UNIORUON00199067
Autore	ARTHUR, Ribeiro
Titolo	A Legiao Potugueza ao serviço de Napoleao (1808-1813) : Illustrado com quatro aguarellas do auctor e trz photogravuras / Ribeiro Arthur
Pubbl/distr/stampa	Lisboa, : Livraria Ferin, 1901. VIII, 151 p. ; 22 cm.
Lingua di pubblicazione	Portoghes
Formato	Materiale a stampa
Livello bibliografico	Monografia
2. Record Nr.	UNINA9910807159803321
Autore	Alcorn Wade
Titolo	The browser hacker's handbook / / Wade Alcorn, Christian Frichot, Michele Orru
Pubbl/distr/stampa	Indianapolis, Indiana : , : Wiley, , 2014 ©2014
ISBN	1-118-91435-X 1-118-66210-5
Edizione	[1st edition]
Descrizione fisica	1 online resource (650 p.)
Altri autori (Persone)	FrichotChristian OrruMichele
Disciplina	005.8
Soggetti	Computer hackers
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Copyright; About the Authors; About the Contributing Authors; About the Technical Editor; Credits; Acknowledgments; Contents; Introduction; Chapter 1: Web Browser Security; A Principal Principle; Exploring the Browser; Symbiosis with the Web Application; Same Origin Policy; HTTP Headers; Markup Languages; HTML; XML; Cascading Style Sheets; Scripting; JavaScript; VBScript; Document Object Model; Rendering Engines; WebKit; Trident; Gecko; Presto; Blink; Geolocation; Web Storage; Cross-origin Resource Sharing; HTML5;

WebSocket; Web Workers; History Manipulation; WebRTC;  
Vulnerabilities  
Evolutionary PressuresHTTP Headers; Content Security Policy; Secure  
Cookie Flag; HttpOnly Cookie Flag; X-Content-Type-Options; Strict-  
Transport-Security; X-Frame-Options; Reflected XSS Filtering;  
Sandboxing; Browser Sandboxing; IFrame Sandboxing; Anti-phishing  
and Anti-malware; Mixed Content; Core Security Problems; Attack  
Surface; Rate of Change; Silent Updating; Extensions; Plugins;  
Surrendering Control; TCP Protocol Control; Encrypted Communication;  
Same Origin Policy; Fallacies; Robustness Principle Fallacy; External  
Security Perimeter Fallacy; Browser Hacking Methodology; Initiating  
RetainingAttacking; Summary; Questions; Notes; Chapter 2: Initiating  
Control; Understanding Control Initiation; Control Initiation Techniques;  
Using Cross-site Scripting Attacks; Reflected Cross-site Scripting;  
Stored Cross-site Scripting; DOM Cross-site Scripting; Universal Cross-  
site Scripting; XSS Viruses; Bypassing XSS Controls; Using Compromised  
Web Applications; Using Advertising Networks; Using Social Engineering  
Attacks; Phishing Attacks; Baiting; Anti-Phishing Controls; Using Man-  
in-the-Middle Attacks; Man-in-the-Browser; Wireless Attacks; ARP  
Spoofing; DNS Poisoning  
Exploiting CachingSummary; Questions; Notes; Chapter 3: Retaining  
Control; Understanding Control Retention; Exploring Communication  
Techniques; Using XMLHttpRequest Polling; Using Cross-origin  
Resource Sharing; Using WebSocket Communication; Using Messaging  
Communication; Using DNS Tunnel Communication; Exploring  
Persistence Techniques; Using IFrames; Using Full Browser Frame  
Overlay; Using Browser Events; Using Pop-Under Windows; Using Man-  
in-the-Browser Attacks; Hijacking AJAX Calls; Hijacking Non-AJAX  
Requests; Evading Detection; Evasion using Encoding; Base64 Encoding;  
Whitespace Encoding  
Non-alphanumeric JavaScriptEvasion using Obfuscation; Random  
Variables and Methods; Mixing Object Notations; Time Delays; Mixing  
Content from Another Context; Using the callee Property; Evasion using  
JavaScript Engines Quirks; Summary; Questions; Notes; Chapter 4:  
Bypassing the Same; Understanding the Same Origin Policy;  
Understanding the SOP with the DOM; Understanding the SOP with  
CORS; Understanding the SOP with Plugins; Understanding the SOP with  
UI Redressing; Understanding the SOP with Browser History; Exploring  
SOP Bypasses; Bypassing SOP in Java; Bypassing SOP in Adobe Reader  
Bypassing SOP in Adobe Flash

---

#### Sommario/riassunto

Hackers exploit browser vulnerabilities to attack deep within networks  
The Browser Hacker's Handbook gives a practical understanding of  
hacking the everyday web browser and using it as a beachhead to  
launch further attacks deep into corporate networks. Written by a team  
of highly experienced computer security experts, the handbook  
provides hands-on tutorials exploring a range of current attack  
methods. The web browser has become the most popular and widely  
used computer ""program"" in the world. As the gateway to the Internet,  
it is part of the storefront to any business that

---

3. Record Nr.	UNISANNIONAP0400690
Autore	LaLonde, Wilf R. <1947- >
Titolo	Smalltalk 5. : practice and experience / Wilf LaLonde, John Pugh
Pubbl/distr/stampa	Englewood Cliffs (NJ), : Prentice Hall, c1994
ISBN	0138140391
Descrizione fisica	VI, 185 p. : ill. ; 24 cm + 1 floppy disk
Altri autori (Persone)	Pugh, John <1950- >
Disciplina	005.13 005.133
Soggetti	Elaboratori elettronici - Programmazione - Linguaggio Smalltalk V
Collocazione	SALA DING 005.13      LAL.sm
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Sul front.: Smalltalk V is based on articles originally appearing in the Journal of Object-Oriented Programming.