Indice generale

Introduzione ..... **xiii**

Capitolo 1 La sicurezza nel mondo delle applicazioni web **1**

La sicurezza delle informazioni in sintesi 1
- Primi approcci con le soluzioni formali 2
- Introduzione alla gestione del rischio 4
- La luce della tassonomia 6
- Verso approcci più pratici 7

Breve storia del Web 8
- L'età della pietra: dal 1945 al 1994 8
- La prima guerra dei browser: dal 1995 al 1999 10
- Il periodo della noia: dal 2000 al 2003 11
- Il Web 2.0 e la seconda guerra dei browser: dal 2004 in avanti 12

L'evoluzione di una minaccia 14
- L'utente è un potenziale problema per la sicurezza 14
- Il cloud, o le gioie della vita in comunità 15
- Visioni non convergenti 16
- Interazioni tra browser: sinergia del fallimento 16
- La rottura del confine client-server 17

Parte I Anatomia del Web **21**

Capitolo 2 Tutto comincia con un URL **23**

La struttura degli Uniform Resource Locator 24
- Schema/nome del protocollo 24
- Indicatore di URL gerarchico 25
- Credenziali di accesso alla risorsa 26
- Indirizzo del server 26
- Porta del server 27
- Percorso gerarchico del file 27
- Stringa di query 28
- Frammento 28
- Mettiamo insieme il tutto 29

Caratteri riservati e percent encoding 31
- Gestione dei caratteri non US-ASCII 33

I principali schemi e la loro funzione 36

Protocolli per il prelevamento di documenti supportati dal browser 36
Protocolli richiesti da applicazioni e plug-in di produttori esterni 37
Pseudo protocolli non incapsulanti 37
Pseudo protocolli incapsulanti 38
Conclusioni sugli schemi 38
Risoluzione di URL relativi 38

Capitolo 3 Il protocollo HTTP 43

Sintassi di base del traffico HTTP 44
Le conseguenze del supporto di HTTP/0.9 45
Trucchi con gli avanzamenti riga 46
Richieste tramite proxy 47
Risoluzione di header duplicati o in conflitto 49
Valori separati da punti e virgola negli header 50
Set di caratteri e schemi di codifica negli header 51
Comportamento dell'header Referer 52
Tipi di richieste HTTP 53
GET 53
POST 54
HEAD 54
OPTIONS 54
PUT 54
DELETE 55
TRACE 55
CONNECT 55
Altri metodi HTTP 55
Codici di risposta del server 55
200–299: successo 56
300–399: reindirizzamento e altri messaggi di stato 56
400–499: errori lato client 57
500–599: errore lato server 57
Coerenza dei codici d'errore HTTP 57
Sessioni keepalive 58
Trasferimenti di dati a blocchi 59
Comportamento della cache 60
Semantica dei cookie HTTP 62
Autenticazione HTTP 64
Crittografia a livello di protocollo e certificati client 65
Certificati EV SSL 66
Regole di gestione degli errori 67

Capitolo 4 Il linguaggio HTML 69

I concetti alla base dei documenti HTML 70
Modalità di parsing del documento 71
La battaglia sulla semantica 72
Il comportamento del parser HTML 73
Interazioni fra più tag 74
Condizionali espliciti e impliciti 75
Suggerimenti per sopravvivere al parsing di codice HTML 76
Codifica delle entità 76
Semantica di integrazione HTTP/HTML 78
Collegamenti ipertestuali e inserimento di contenuti 79
Collegamenti normali 79

Moduli e richieste generate da moduli ... 80
Frame ... 82
Inclusione di tipi di contenuti specifici ... 82
Nota sul CSRF (Cross-Site Request Forgery) ... 84

Capitolo 5 I fogli di stile CSS ... 87

Sintassi CSS di base ... 88
Definizione delle proprietà ... 89
Direttive @ e binding XBL ... 89
Interazioni con HTML ... 90
Rischi di risincronizzazione del parser ... 90
Codifica dei caratteri ... 91

Capitolo 6 Gli script lato browser ... 95

Caratteristiche di base di JavaScript ... 96
Il modello di elaborazione degli script ... 97
Controllo dell'ordine di esecuzione ... 100
Possibilità di ispezione del codice e degli oggetti ... 101
Modifiche all'ambiente di runtime ... 102
JSON e serializzazioni dei dati ... 104
E4X e altre estensioni della sintassi ... 106
Gerarchia di oggetti standard ... 107
Il Document Object Model ... 109
Accesso ad altri documenti ... 111
Codifica dei caratteri di script ... 112
Modalità di inclusione del codice e rischi dell'annidamento ... 113
Il morto vivente: Visual Basic ... 115

Capitolo 7 Tipi di documento diversi da HTML ... 117

File di testo ... 117
Immagini bitmap ... 118
Audio e video ... 119
Documenti basati su XML ... 119
La vista XML generica ... 120
SVG ... 121
MathML ... 122
XUL ... 122
WML ... 123
Feed RSS e Atom ... 124
Nota sui tipi di file non visualizzabili ... 124

Capitolo 8 Visualizzazione del contenuto con i plug-in del browser ... 127

Attivazione di un plug-in ... 128
I pericoli della gestione del Content-Type dei plug-in ... 129
Applicazioni esterne per la visualizzazione dei documenti ... 130
Framework applicativi basati su plug-in ... 131
Adobe Flash ... 132
Microsoft Silverlight ... 134
Sun Java ... 134
XBAP ... 135
I controlli ActiveX ... 136
Convivere con gli altri plug-in ... 137

Parte II Funzionalità di sicurezza dei browser ...139

Capitolo 9 La logica dell'isolamento del contenuto 141

La regola della stessa origine per il Document Object Model 142
document.domain 143
postMessage(...) 144
Interazioni con le credenziali del browser 146
La regola della stessa origine per XMLHttpRequest 146
La regola della stessa origine per il Web Storage 149
Le regole di sicurezza per i cookie 149
Impatto dei cookie sulla regola della stessa origine 151
Problemi con le restrizioni sul dominio 152
L'inconsueto pericolo di "localhost" 153
Cookie e hijacking "legittimo" del DNS 154
Regole di sicurezza per i plug-in 154
Adobe Flash 155
Microsoft Silverlight 158
Java 158
Origini ambigue o inattese 159
Indirizzi IP 159
Nomi di host con punti extra 159
Nomi di host non completamente qualificati 160
File locali 160
Pseudo URL 161
Estensioni del browser e interfacce utente 162
Altri utilizzi delle origini 162

Capitolo 10 Ereditarietà dell'origine 165

Ereditarietà dell'origine per about:blank 166
Ereditarietà per URL con schema data: 167
Ereditarietà per URL javascript: e vbscript: 169
Nota sugli pseudo URL non accettati 170

Capitolo 11 Oltre le regole della stessa origine 173

Interazioni tra finestre e frame 174
Modifica della posizione di documenti esistenti 174
Utilizzo di frame non richiesto 178
Inclusione di contenuti di domini diversi 181
Nota sulle sottorisorse provenienti da origini diverse 183
Canali laterali legati alla privacy 184
Altre falle della regola della stessa origine 186

Capitolo 12 Altri confini della sicurezza 187

Navigazione su schemi sensibili 187
Accesso alle reti interne 188
Porte vietate 190
Limitazioni sui cookie di terzi 192

Capitolo 13 Meccanismi di riconoscimento del contenuto 195
La logica di rilevazione del tipo di documento 196
Tipi MIME malformati 197
Valori speciali di Content-Type 197
Tipo di contenuto non riconosciuto 199
Uso di Content-Disposition a scopo di difesa 201
Direttive di contenuto su sottorisorse 202
File scaricati e altri contenuti non HTTP 202
Gestione del set di caratteri 204
BOM (Byte Order Mark) 206
Ereditarietà e ridefinizione del set di caratteri 207
Set di caratteri o sottorisorse controllate dal codice di markup 207
Rilevamento di file non HTTP 208

Capitolo 14 Affrontare gli script ostili 211
Attacchi Denial-of-Service 212
Limiti al tempo di esecuzione e all'uso della memoria 213
Limiti alla connessione 214
Filtro delle finestre pop-up 215
Restrizioni sull'uso di finestre di dialogo 216
Problemi di posizionamento e di aspetto delle finestre 218
Attacchi temporizzati all'interfaccia utente 220

Capitolo 15 Privilegi di sito estrinseci 223
Permessi di sito gestiti da browser e plug-in 224
Domini codificati internamente 225
Gestori di password basati su moduli 225
Il modello ad aree di Internet Explorer 227
MotW e Zone.Identifier 229

Parte III Uno sguardo su ciò che verrà 231

Capitolo 16 Funzionalità di sicurezza nuove e future 233
Framework di estensione del modello di sicurezza 234
Richieste da domini diversi 234
XDomainRequest 237
Altri usi dell'header Origin 238
Framework di restrizione del modello di sicurezza 239
CSP (Content Security Policy) 239
Frame in sandbox 243
Strict Transport Security 245
Modalità di navigazione privata 247
Altri sviluppi 247
Sistemi di pulizia del codice HTML interni al browser 247
Filtro di XSS 249

Capitolo 17 Altri meccanismi dei browser degni di nota 253
Proposte a livello di URL e di protocollo 253
Caratteristiche a livello dei contenuti 256
Interfacce di I/O 257

Capitolo 18 Vulnerabilità web comuni 259
Vulnerabilità specifiche di applicazioni web 259
Problemi da considerare nella progettazione di applicazioni web 261
Problemi comuni che interessano solo il codice lato server 263

Epilogo 265

Note bibliografiche 267

Indice analitico 279