

# Indice generale

<b>Prefazione</b>	.....	<b>xi</b>
<b>Premessa</b>	.....	<b>xiii</b>
<b>Ringraziamenti</b>	.....	<b>xv</b>
<b>Introduzione</b>	.....	<b>xvii</b>
A chi è rivolto questo libro	.....	xvii
Come è organizzato il libro: una roadmap	.....	xvii
Parliamo del codice	.....	xvii
L'autore	.....	xviii
<b>Parte I</b>	<b>Principi di Web Security</b>	<b>1</b>
<b>Capitolo 1</b>	<b>Conosci il tuo nemico</b>	<b>3</b>
Capire come gli hacker vi attaccano e perché	.....	4
Sopravvivere alle conseguenze di un hacking	.....	8
Quanto dovremmo essere paranoici?	.....	10
Da dove iniziare a proteggersi?	.....	11
Tenete traccia delle nuove vulnerabilità	.....	11
Scoprite quale codice state distribuendo	.....	12
Registrate e monitorate l'attività	.....	12
Trasformate i membri del vostro team in esperti di sicurezza	....	13
Rallentate	.....	14
Riepilogo	.....	14
<b>Capitolo 2</b>	<b>Sicurezza del browser</b>	<b>15</b>
Le varie parti di un browser	.....	16
La sandbox JavaScript	.....	17

Policy di sicurezza dei contenuti .....	19
La policy same-origin .....	21
Richieste multiorigine (cross-origin) .....	23
Controlli di integrità delle risorse secondarie .....	25
Accesso al disco .....	27
L'API File .....	27
WebStorage .....	28
IndexedDB .....	30
Cookie .....	31
Cookie sicuri .....	33
Cookie HttpOnly .....	34
L'attributo SameSite .....	35
Cookie con scadenza .....	36
Invalidazione dei cookie .....	37
Monitoraggio inter-sito (cross-site) .....	37
Riepilogo .....	39

### **Capitolo 3 Crittografia .....41**

I principi della crittografia .....	42
Le chiavi di crittografia .....	42
Crittografia dei dati in transito .....	45
Adottare misure pratiche .....	48
Reindirizzamento a HTTPS .....	48
Chiedere al browser di utilizzare sempre il protocollo HTTPS .....	49
Crittografia dei dati inattivi .....	49
Hashing della password .....	50
Salting .....	52
Controllo dell'integrità .....	53
Riepilogo .....	55

### **Capitolo 4 Sicurezza del server web .....57**

Convalida dell'input .....	57
Allow list .....	57
Block list .....	58
Corrispondenza di pattern .....	59
Ulteriore convalida .....	61
Convalida degli indirizzi e-mail .....	61
Convalida dei file inviati .....	63
Escaping dell'output .....	64
Escaping dell'output nella risposta HTTP .....	65
Escaping dell'output nei comandi del database .....	67
Escaping dell'output nelle stringhe dei comandi .....	70
Gestione delle risorse .....	73
REST (Representation State Transfer) .....	75

La difesa a livelli.....	76
Il principio del privilegio minimo.....	77
Riepilogo.....	78
<b>Capitolo 5 La sicurezza è un processo.....</b>	<b>81</b>
Il principio dei “quattro occhi”.....	82
Applicazione del principio del privilegio minimo ai processi.....	83
Automatizzare tutto il possibile.....	84
Non reinventare la ruota.....	86
Gestione degli audit trail.....	87
Scrittura del codice in modo sicuro.....	89
Controllo del codice sorgente.....	89
Gestione delle dipendenze.....	90
Progettazione di un processo di sviluppo.....	90
Scrittura di unit test.....	92
Esecuzione di revisioni del codice.....	94
Automazione dei processi di rilascio.....	94
Distribuzione in ambienti di produzione.....	96
Rollback del codice.....	97
Uso di strumenti di protezione.....	97
Analisi delle dipendenze.....	97
Analisi statica.....	98
Penetration testing automatizzati.....	98
Firewall.....	99
Sistemi di rilevamento delle intrusioni.....	100
Programma antivirus.....	101
Gestire gli errori.....	101
Riepilogo.....	103
<b>Parte II Vulnerabilità.....</b>	<b>105</b>
<b>Capitolo 6 Vulnerabilità del browser.....</b>	<b>107</b>
Attacchi Cross Site Scripting.....	108
Attacchi Stored Cross-Site Scripting.....	108
Attacco Reflected Cross-Site Scripting.....	111
Cross-Site Scripting basato sul DOM.....	112
Proteggersi dal Cross-Site Scripting tramite l’escaping.....	114
Escaping nei template lato-client.....	117
Policy di sicurezza dei contenuti.....	117
Attacchi Cross-Site Request Forgery.....	118
Rendere le vostre richieste GET prive di effetti collaterali.....	120
Token anti-CSRF.....	121
Garantire che i cookie vengano inviati con l’attributo SameSite.....	124
Clickjacking.....	125

Protezione dal clickjacking .....	127
X-Frame-Options .....	128
Attacchi Cross-Site Script Inclusion .....	128
Protezione dagli attacchi XSSI .....	130
Impostazione di una policy CSP per le risorse multiorigine ...	131
Riepilogo .....	131

## **Capitolo 7 Vulnerabilità di rete.....133**

Vulnerabilità Monster-in-the-Middle .....	133
Intercettare il traffico su una rete .....	134
Sfruttare i protocolli misti .....	137
Attacchi a downgrade .....	138
Vulnerabilità a deviazione.....	139
Domini “sosia”.....	140
DNS Poisoning .....	142
Occupazione (squatting) dei sottodomini .....	146
Violazione dei certificati .....	149
Revoca dei certificati .....	150
Trasparenza dei certificati.....	151
Sottrazione delle chiavi .....	152
Riepilogo .....	153

## **Capitolo 8 Vulnerabilità dell’autenticazione .....155**

Attacchi a forza bruta.....	155
Single Sign-On.....	157
OpenID Connect e OAuth.....	157
Il linguaggio SAML.....	159
Rafforzare la vostra autenticazione .....	160
Regole sulla complessità della password.....	160
CAPTCHA.....	163
Limitazioni basate sulla frequenza.....	165
Autenticazione a più fattori.....	166
Autenticazione biometrica .....	168
Memorizzazione delle credenziali d’accesso.....	170
Hashing, salting e peppering delle password.....	171
Credenziali sicure per i login in uscita.....	172
Enumerazione degli utenti .....	174
Nomi utente pubblici .....	177
Attacchi basati sui tempi .....	179
Riepilogo .....	180

## **Capitolo 9 Vulnerabilità della sessione .....181**

Come funzionano le sessioni.....	181
Sessioni lato-server .....	182
Sessioni lato-client.....	185

Token web JSON .....	186
Dirottamento della sessione .....	187
Dirottamento della sessione sulla rete .....	187
Dirottamento della sessione tramite Cross-Site Scripting .....	188
Identificatori di sessione deboli .....	188
Fissazione della sessione .....	190
Manomissione della sessione .....	192
Riepilogo .....	192

## **Capitolo 10 Vulnerabilità delle autorizzazioni .....195**

Modellazione delle autorizzazioni .....	196
Caso 1: il forum web .....	197
Caso 2: la piattaforma di contenuti .....	197
Caso 3: lo strumento di messaggistica .....	198
Progettazione delle autorizzazioni .....	199
Implementazione del controllo degli accessi .....	199
Restrizioni di accesso all'URL .....	201
Tabelle di routing dinamiche .....	201
Decoratori .....	202
Hook .....	202
Dichiarazioni if .....	204
Errori di autorizzazione vs. reindirizzamenti .....	204
Organizzazione dello schema degli URL .....	205
Modello-Vista-Controller .....	206
Autorizzazioni lato-client .....	207
Autorizzazioni a tempo determinato .....	208
Controllo delle autorizzazioni .....	208
Unit test .....	209
Librerie di mocking .....	209
Individuazione dei più comuni difetti nelle attività di autorizzazione .....	210
Manca il controllo degli accessi .....	211
Confusione su quali componenti del codice applicano il controllo degli accessi .....	211
Violazione dei confini di sicurezza .....	211
Decisioni di controllo degli accessi basate su input non fidati .....	212
Riepilogo .....	212

## **Capitolo 11 Vulnerabilità a payload .....213**

Attacchi a deserializzazione .....	214
Vulnerabilità JSON .....	217
Inquinamento dei prototipi .....	218
Vulnerabilità XML .....	221
Convalida XML .....	221
Bombardamento XML .....	222

Attacchi a entità esterne XML .....	224
Mitigazione degli attacchi XML .....	226
Vulnerabilità nell'upload di file .....	227
Convalidare i file caricati .....	227
Rinominare i file dopo l'upload .....	228
Scrivere su disco senza le autorizzazioni appropriate .....	229
Utilizzare l'archiviazione sicura dei file .....	230
Attraversamento dei percorsi .....	231
Assegnamenti in massa .....	233
Riepilogo .....	235

## **Capitolo 12 Vulnerabilità a iniezione .....237**

Esecuzione di codice da remoto .....	238
Linguaggi specifici del dominio .....	239
Include lato-server .....	242
SQL Injection.....	243
Istruzioni parametrizzate .....	246
Framework ORM .....	248
NoSQL Injection.....	251
MongoDB.....	251
Couchbase.....	252
Cassandra .....	252
HBase.....	252
LDAP Injection .....	252
Iniezione di comandi .....	253
Iniezione di CRLF .....	256
Iniezione di espressioni regolari.....	258
Riepilogo .....	260

## **Capitolo 13 Vulnerabilità nel codice fornito da terze parti .....261**

Le dipendenze .....	263
Versioni delle dipendenze .....	264
Studio delle vulnerabilità .....	265
Distribuzione delle patch .....	267
Più in basso nello stack .....	268
Non divulgare informazioni.....	270
Rimozione delle intestazioni del server .....	270
Modifica del nome del cookie della sessione .....	270
Utilizzo di URL "puliti".....	270
Scrubbing delle voci DNS .....	271
Sanificazione dei file template .....	272
Impronta digitale del server.....	273
Configurazione non sicura .....	273
Configurazione della directory root del Web .....	273
Disabilitazione della segnalazione degli errori lato-client .....	274

---

Modifica delle password di default.....	274
Riepilogo .....	275
<b>Capitolo 14 Diventare inconsapevolmente complici .....</b>	<b>277</b>
Falsificazione delle richieste lato-server .....	277
Limitazione dei domini cui si ha accesso .....	279
Limitazione delle richieste HTTP ai soli utenti reali.....	280
Convalida degli URL cui si accede .....	280
Utilizzo di una block list di domini.....	281
Spoofing della posta elettronica .....	281
Il Sender Policy Framework.....	282
DomainKeys Identified Mail.....	282
Autenticazione, reporting e conformità dei messaggi basati sul dominio .....	283
Passaggi pratici.....	283
Reindirizzamenti aperti .....	283
Non consentire reindirizzamenti extra-sito .....	284
Controllare il Referer quando eseguite i reindirizzamenti.....	285
Riepilogo .....	285
<b>Capitolo 15 Che cosa fare dopo aver subito un attacco .....</b>	<b>287</b>
Scoprire la violazione.....	288
Fermare un attacco in corso .....	288
Capire che cosa è andato storto .....	290
Evitare che l'attacco si ripeta .....	291
Comunicazione dei dettagli sull'incidente agli utenti.....	291
Mitigazione degli attacchi futuri.....	292
Riepilogo .....	292
<b>Indice analitico.....</b>	<b>295</b>