

Indice generale

Prefazione	xv	
Introduzione	xvii	
A chi è rivolto questo libro	xvii	
Che cosa troverete in questo libro	xviii	
Buon Hacking!	xix	
L'autrice	xix	
Il revisore tecnico	xx	
Parte I	Il settore della caccia ai bug	1
Capitolo 1	Scegliere un programma di caccia ai bug	3
Lo stato delle cose	3	
Tipi di asset	4	
Siti e applicazioni social	4	
Applicazioni web in generale	5	
Applicazioni per dispositivi mobili (Android, iOS e Windows)	6	
API	6	
Codice sorgente ed eseguibili	7	
Hardware e IoT	7	
Piattaforme di caccia ai bug	7	
I pro	8	
... e i contro	9	
Ambiti, pagamenti e tempi di risposta	9	
Ambiti del programma	9	
Importi dei premi	10	
Tempi di risposta	11	
Programmi privati	11	
Scegliere il programma giusto	12	
Un rapido confronto dei programmi più noti	13	

Capitolo 2 Come operare in un programma di caccia ai bug.....15

Scrivere un buon report.....	15
Passaggio 1 – Create un titolo descrittivo	16
Passaggio 2 – Fornite un riassunto chiaro	16
Passaggio 3 – Includete una valutazione della gravità.....	16
Passaggio 4 – Fornite passaggi chiari per la riproduzione	18
Passaggio 5 – Fornite una prova di concetto.....	18
Passaggio 6 – Descrivete gli scenari di impatto e di attacco.....	19
Passaggio 7 – Consigliare possibili soluzioni	19
Passaggio 8 – Verificate il report	20
Ulteriori suggerimenti per scrivere report migliori.....	20
Costruire una relazione con il team di sviluppo	21
Lo stato del report	21
Affrontare i conflitti	23
Costruire una partnership	23
Perché state fallendo?	24
Perché non trovate bug?.....	24
Perché i vostri report vengono respinti?	26
Che cosa fare quando vi trovate in un vicolo cieco.....	27
Passaggio 1 – Prendetevi una pausa	28
Passaggio 2 – Costruitevi il vostro set di competenze.....	28
Passaggio 3 – Cercate una nuova prospettiva	28
Infine, qualche parola per esperienza	29

Parte II Le basi31**Capitolo 3 Come funziona Internet33**

Il modello client-server	33
Il sistema dei nomi di dominio: DNS	34
Porte Internet	35
Richieste e risposte HTTP	36
Controlli di sicurezza Internet.....	38
Codifica dei contenuti	38
Gestione delle sessioni e cookie HTTP.....	39
Autenticazione basata su token.....	40
Token web JSON	41
La politica same-origin	43
Imparate a programmare	44

Capitolo 4 Configurare l'ambiente e intercettare il traffico45

Scegliere un sistema operativo	45
Configurare gli elementi essenziali: un browser e un proxy	46
Aprire il browser embedded.....	47
Configurare Firefox	47

Configurare Burp	49
Usare Burp	51
Il proxy	52
L'intruder	54
Il repeater	56
Il decoder	56
Il comparer	57
Salvare le richieste in Burp	57
Un appunto finale sul... prendere appunti	57

Capitolo 5 Hacking web: ricognizione.....59

Procedere manualmente attraverso il target	60
Google dorking	60
Esplorare l'ambito	63
WHOIS e Reverse WHOIS	63
Indirizzi IP	64
Analizzare i certificati.....	65
Enumerare i sottodomini	66
Enumerare i servizi	67
Attacchi a forza bruta sulle directory	68
Spidering nel sito.....	69
Hosting di terze parti.....	72
Ricognizione GitHub.....	74
Altre subdole tecniche OSINT	75
Le "impronte digitali" dello stack di tecnologie	76
Realizzare gli script di ricognizione.....	78
Le basi dello scripting bash.....	79
Salvare l'output dello strumento in un file.....	81
Aggiungere la data della scansione all'output	82
Aggiungere opzioni per scegliere gli strumenti da eseguire	83
Eseguire altri strumenti	84
Parsing dei risultati	87
Creare un master report.....	89
Eseguire la scansione di più domini.....	90
Scrivere una libreria di funzioni	95
Creare programmi interattivi.....	96
Uso di variabili e caratteri speciali.....	99
Scheduling di scansioni automatiche	101
Una nota sulle API Recon	103
Ora dedicatevi all'hacking.....	103
Strumenti menzionati in questo capitolo	104
Scoperta dell'ambito	104
Tecniche OSINT.....	105
Impronte digitali dello stack di tecnologie.....	105
Automazione.....	106

Parte III Vulnerabilità web.....107**Capitolo 6 XSS, Cross Site Scripting.....109**

Meccanismi	109
Tipi di vulnerabilità XSS.....	113
Stored XSS.....	113
Blind XSS	115
Reflected XSS.....	115
DOM-based XSS	115
Self-XSS.....	117
Contromisure	117
A caccia di vulnerabilità XSS	118
Passaggio 1 – Cercare le opportunità di input.....	119
Passaggio 2 – Inserire il payload	120
Passaggio 3 – Confermare l'impatto	124
Bypass delle protezioni anti-XSS.....	124
Sintassi JavaScript alternativa	124
Maiuscole e codifica	125
Errori logici del filtro.....	126
Ampliare l'attacco	126
Automatizzare la caccia alle vulnerabilità XSS	127
Alla ricerca della vostra prima vulnerabilità XSS.....	128

Capitolo 7 Open Redirects.....129

Meccanismi	129
Contromisure	131
A caccia di vulnerabilità Open Redirects.....	131
Passaggio 1 – Cercare i parametri di reindirizzamento	131
Passaggio 2 – Google Dorking per trovare altri parametri di reindirizzamento.....	132
Passaggio 3 –Verificare le vulnerabilità Open Redirects basate su parametri.....	133
Passaggio 4 –Verificare le vulnerabilità Referer-based Open Redirects	134
Bypass delle protezioni anti-Open Redirects	134
Utilizzare la correzione automatica del browser.....	134
Sfruttare una logica difettosa del validatore.....	135
Utilizzare i dati URL.....	136
Sfruttare la decodifica degli URL.....	137
Combinazione di più tecniche di exploit	138
Ampliare l'attacco	139
Alla ricerca della vostra prima vulnerabilità Open Redirects	140

Capitolo 8	Clickjacking	141
	Meccanismi	141
	Contromisure	147
	A caccia di vulnerabilità Clickjacking.....	148
	Passaggio 1 – Ricerca delle azioni di alterazione dello stato	148
	Passaggio 2 – Controllo delle intestazioni della risposta	149
	Passaggio 3 – Conferma della vulnerabilità.....	149
	Bypass delle protezioni anti-Clickjacking	150
	Ampliare l'attacco	151
	Una nota sull'invio del payload di Clickjacking	152
	Alla ricerca della vostra prima vulnerabilità Clickjacking	152
Capitolo 9	CSRF, Cross-Site Request Forgery	155
	Meccanismi	155
	Contromisure	159
	A caccia di vulnerabilità CSRF	161
	Passaggio 1 – Individuare le azioni di alterazione dello stato ...	161
	Passaggio 2 – Cercare una assenza di protezioni anti-CSRF....	161
	Passaggio 3 – Confermare la vulnerabilità	162
	Bypass delle protezioni anti-CSRF.....	163
	Sfruttare il Clickjacking	164
	Modificare il metodo della richiesta	164
	Ignorare i token CSRF archiviati sul server	165
	Ignorare i token CSRF a doppio invio.....	167
	Bypass del controllo dell'intestazione CSRF referer.....	168
	Aggirare la protezione anti-CSRF utilizzando un attacco XSS.....	170
	Ampliare l'attacco	170
	Sottrarre informazioni all'utente tramite un attacco CSRF	170
	Preparare un attacco Stored Self-XSS utilizzando un attacco CSRF.....	171
	Acquisire l'account utente utilizzando un attacco CSRF	172
	Consegnare il payload CSRF	173
	Alla ricerca della vostra prima vulnerabilità CSRF.....	175
Capitolo 10	IDOR, Insecure Direct Object References.....	177
	Meccanismi	177
	Contromisure	179
	A caccia di vulnerabilità IDOR.....	180
	Passaggio 1 – Creare due account	180
	Passaggio 2 – Scoprire le funzionalità	180
	Passaggio 3 – Acquisire le richieste	181
	Passaggio 4 – Cambiare gli ID	181

Bypass delle protezioni anti-IDOR	183
ID codificati e ID hash	183
ID-leaks	184
Offrire all'applicazione un ID, anche se non lo richiede.....	184
Controllare i riferimenti IDOR ciechi.....	185
Modificare il metodo della richiesta	185
Modificare il tipo di file richiesto.....	186
Ampliare l'attacco	187
Automatizzare l'attacco	187
Alla ricerca della vostra prima vulnerabilità IDOR	187

Capitolo 11 SQL Injection189

Meccanismi	190
Iniettare del codice nelle query SQL.....	190
SQL Injection di secondo ordine	193
Contromisure	194
A caccia di vulnerabilità SQL Injection	197
Passaggio 1 – Cercare vulnerabilità SQL Injection classiche....	197
Passaggio 2 – Cercare vulnerabilità Blind SQL Injection	198
Passaggio 3 – Ottenere informazioni utilizzando attacchi SQL Injection	200
Passaggio 4 – Cercare vulnerabilità NoSQL	201
Ampliare l'attacco	203
Raccogliete informazioni sul database	203
Ottenete una web shell	204
Automatizzare le SQL Injection	205
Alla ricerca della vostra prima vulnerabilità SQL Injection.....	205

Capitolo 12 Race Condition207

Meccanismi	207
Quando una Race Condition diventa una vulnerabilità	209
Contromisure	211
A caccia di vulnerabilità Race Condition	212
Passaggio 1 – Trovare le funzionalità soggette a Race Condition.....	212
Passaggio 2 – Inviare richieste simultanee.....	212
Passaggio 3 – Controllare i risultati	213
Passaggio 4 – Creare una prova di concetto	213
Ampliare l'attacco	213
Alla ricerca della vostra prima vulnerabilità Race Condition.....	214

Capitolo 13 SSRF, Server-Side Request Forgery215

Meccanismi	215
Contromisure	216
A caccia di vulnerabilità SSRF	217

Passaggio 1 – Individuare le funzionalità soggette a vulnerabilità SSRF	217
Passaggio 2 – Fornire URL interni agli endpoint potenzialmente vulnerabili	219
Passaggio 3 – Controllare i risultati	220
Bypass delle protezioni anti-SSRF.....	222
Bypassare le allowlist	222
Bypassare le blocklist.....	223
Ampliare l'attacco	226
Eseguire la scansione della rete	226
Estrarre i metadati dell'istanza	228
Sfruttare le vulnerabilità Blind SSRF.....	229
Attaccare la rete	230
Alla ricerca della vostra prima vulnerabilità SSRF.....	231
Capitolo 14 Insecure Deserialization.....	233
Meccanismi	233
PHP	234
Java.....	243
Contromisure	245
A caccia di vulnerabilità Insecure Deserialization.....	246
Ampliare l'attacco	247
Alla ricerca della vostra prima vulnerabilità Insecure Deserialization	247
Capitolo 15 XXE, XML External Entity.....	249
Meccanismi	249
Contromisure	251
A caccia di vulnerabilità XXE	252
Passaggio 1 – Trovare i punti di ingresso dei dati XML	252
Passaggio 2 – Test della vulnerabilità Classic XXE	253
Passaggio 3 – Test della vulnerabilità Blind XXE	254
Passaggio 4 – Incorporare payload XXE in diversi tipi di file.....	254
Passaggio 5 – Test della vulnerabilità XInclude	255
Ampliare l'attacco	256
Leggere file protetti	256
Lanciare un attacco SSRF.....	256
Utilizzare un attacco Blind XXE.....	257
Eseguire attacchi Denial-of-Service.....	259
Ulteriori informazioni sulla sottrazione di dati tramite attacchi XXE.....	260
Alla ricerca della vostra prima vulnerabilità XXE.....	262

Capitolo 16 Template Injection263

Meccanismi	263
Motori di template	264
Iniezione del codice nel template	265
Contromisure	267
A caccia di vulnerabilità Template Injection	268
Passaggio 1 – Cercare l’uso dell’input dell’utente	268
Passaggio 2 – Rilevare la vulnerabilità Template Injection inviando payload di test	268
Passaggio 3 – Determinare il motore di template in uso	269
Ampliare l’attacco	270
Ricerca un accesso al sistema tramite codice Python	271
Uscire dalla sandbox utilizzando le funzioni built-in di Python	271
Inviare il payload di test	274
Automatizzare gli attacchi Template Injection	275
Alla ricerca della vostra prima vulnerabilità Template Injection	275

Capitolo 17 Errori nella logica dell’applicazione e nel controllo degli accessi.....277

Errori nella logica dell’applicazione	278
Errori nel controllo degli accessi	280
Pannelli di amministrazione esposti	280
Vulnerabilità directory traversal	281
Contromisure	281
A caccia di errori nella logica dell’applicazione e nel controllo degli accessi	282
Passaggio 1 – Studiare il target	282
Passaggio 2 – Intercettare le richieste durante la navigazione	282
Passaggio 3 – Pensare fuori dagli schemi	282
Ampliare l’attacco	283
Alla ricerca degli errori nella logica dell’applicazione o nel controllo degli accessi	283

Capitolo 18 RCE, Remote Code Execution285

Meccanismi	285
Code Injection	286
File Inclusion	287
Contromisure	289
A caccia di vulnerabilità RCE	290
Passaggio 1 – Raccogliere informazioni sull’obiettivo	290
Passaggio 2 – Identificare le posizioni sospette di input dell’utente	291

Passaggio 3 – Inviare i payload di test	291
Passaggio 4 – Confermare la vulnerabilità	292
Ampliare l'attacco	292
Bypass delle protezioni anti-RCE	293
Alla ricerca della vostra prima vulnerabilità RCE	295
Capitolo 19 Bypass del blocco SOP, Same Origin Policy	297
Meccanismi	297
Sfruttare la vulnerabilità della CORS	298
Sfruttare postMessage()	300
Sfruttare JSON con Padding	302
Bypassare il blocco SOP utilizzando un attacco XSS	304
A caccia di bypass del blocco SOP	304
Passaggio 1 – Determinare se vengono utilizzate tecniche di rilassamento del blocco SOP	304
Passaggio 2 – Trovare configurazioni errate della tecnica CORS	304
Passaggio 3 – Trovare bug postMessage Bug	306
Passaggio 4 – Trovare difetti JSONP	307
Passaggio 5 – Considerare altri fattori	307
Ampliare l'attacco	307
Alla ricerca della vostra prima vulnerabilità di bypass del blocco SOP	308
Capitolo 20 Sicurezza del meccanismo SSO, Single Sign-On.....	309
Meccanismi	309
Condivisione dei cookie	310
Il linguaggio SAML	311
OAuth	314
A caccia di vulnerabilità di acquisizione di sottodomini	318
Passaggio 1 – Elencare i sottodomini del target	318
Passaggio 2 – Trovare le pagine non registrate	318
Passaggio 3 – Registrare la pagina	319
Monitoraggio delle acquisizioni di sottodomini	320
A caccia di vulnerabilità SAML	321
Passaggio 1 – Individuare la risposta SAML	321
Passaggio 2 – Analizzare i campi della risposta	321
Passaggio 3 – Bypassare la signature	322
Passaggio 4 – Ricodificare il messaggio	322
A caccia di vulnerabilità a furto di token OAuth	322
Ampliare l'attacco	323
Alla ricerca della vostra prima vulnerabilità di bypass del meccanismo SSO	323

Capitolo 21	Fughe di informazioni	325
	Meccanismi	325
	Contromisure	326
	A caccia delle fughe di informazioni	327
	Passaggio 1 – Tentare un attacco di attraversamento del percorso	327
	Passaggio 2 – Cercare in Wayback Machine	328
	Passaggio 3 – Cercare nei siti di paste-dump	329
	Passaggio 4 – Ricostruire il codice sorgente da una directory .git esposta	330
	Passaggio 5 – Trovare informazioni nei file pubblici	333
	Ampliare l'attacco	333
	Alla ricerca della vostra prima vulnerabilità alla fuga di informazioni	334
Parte IV	Tecniche avanzate	335
Capitolo 22	Condurre analisi del codice	337
	Test white-box o black-box?	338
	L'approccio veloce, a colpi di grep	338
	Pattern di programmazione pericolosi	338
	Fughe di segreti e crittografia debole	340
	Nuove patch e dipendenze obsolete	342
	Commenti degli sviluppatori	342
	Funzionalità di debug, file di configurazione ed endpoint	342
	L'approccio dettagliato	343
	Funzioni importanti	343
	Input dell'utente	344
	Esercizio: individuare le vulnerabilità	346
Capitolo 23	Hacking delle app Android	349
	Configurazione di un proxy mobile	350
	Bypassare il pinning dei certificati	351
	Anatomia di un APK	352
	Strumenti disponibili	353
	Android Debug Bridge	353
	Android Studio	354
	Apktool	354
	Frida	355
	Mobile Security Framework	355
	A caccia di vulnerabilità	355

Capitolo 24 Hacking delle API.....357

Che cosa sono le API?.....	357
API REST	359
API SOAP.....	360
API GraphQL	360
Applicazioni API-centriche.....	363
A caccia di vulnerabilità API	364
Eseguire la ricognizione.....	364
Testing di errori nel controllo degli accessi e di fughe di informazioni.....	366
Test di problemi di limiti di velocità.....	367
Test di bug tecnici	368

**Capitolo 25 Individuazione automatica
delle vulnerabilità tramite fuzzer.....371**

Che cos'è il fuzzing?	371
Come funziona un web fuzzer	372
Il processo di fuzzing.....	373
Passaggio 1 – Determinare i punti di iniezione dei dati	373
Passaggio 2 – Decidere l'elenco dei payload	374
Passaggio 3 – Fuzzing	374
Passaggio 4 – Monitorare i risultati	376
Fuzzing con Wfuzz	376
Enumerare i percorsi.....	376
Attaccare a forza bruta l'autenticazione	378
Testing delle vulnerabilità web più comuni	379
Maggiori informazioni su Wfuzz.....	380
Analisi fuzzing vs. statica	380
Le insidie del fuzzing	380
Estendere il kit di strumenti per i test automatizzati.....	381

Indice analitico.....383