

Spis treści

WSTĘP	11
O tej książce	12
Kto powinien przeczytać tę książkę	12
Krótką historią internetu	12
Skrypty w przeglądarkach	13
Na scenę wkracza nowy rywal	14
Maszyny do pisania kodu HTML-a	14
Metafora systemu rur	15
Czym należy się martwić najbardziej	15
Zawartość książki	15
 1	
HAKOWANIE STRONY INTERNETOWEJ	19
Ataki na oprogramowanie i ukryta sieć	19
Jak zhakować stronę internetową	21
 CZĘŚĆ I. PODSTAWY	23
 2	
JAK DZIAŁA INTERNET	25
Zbiór protokołów internetowych	25
Adresy protokołu internetowego	26
System nazw domen	27
Protokoły warstwy aplikacji	27
HyperText Transfer Protocol	28
Połączenia stanowe	32
Szyfrowanie	33
Podsumowanie	33
 3	
JAK DZIAŁAJĄ PRZEGLĄDARKI	35
Renderowanie strony internetowej	35
Ogólne informacje o silniku renderowania	36
Document Object Model	37
Informacje o stylach	37

JavaScript	38
Przed renderowaniem i po renderowaniu: co jeszcze robi przeglądarka	40
Podsumowanie	41

4

JAK DZIAŁAJĄ SERWERY WWW	43
Zasoby statyczne i dynamiczne	44
Zasoby statyczne	44
Rozwiązywanie adresów URL	44
Systemy dostarczania treści	46
Systemy zarządzania treścią	46
Zasoby dynamiczne	47
Szablony	48
Bazy danych	48
Rozproszona pamięć podręczna	51
Języki wykorzystywane w programowaniu serwisów WWW	51
Podsumowanie	55

5

JAK PRACUJĄ PROGRAMIŚCI	57
Etap 1. Projekt i analiza	58
Etap 2. Pisanie kodu	59
Rozproszone i scentralizowane systemy kontroli wersji	59
Tworzenie gałęzi i scalanie kodu	60
Etap 3. Testowanie przed publikacją	61
Pokrycie testami i ciągła integracja	61
Środowiska testowe	62
Etap 4. Proces publikacji	63
Opcje standaryzacji wdrażania podczas publikacji	63
Proces budowania	65
Skrypty do migracji bazy danych	66
Etap 5. Testowanie i obserwacje po publikacji	66
Testy penetracyjne	66
Rejestrowanie zdarzeń, monitorowanie i raportowanie błędów	67
Zarządzanie zależnościami	68
Podsumowanie	68

CZĘŚĆ II. ZAGROŻENIA 71

6

ATAKI PRZEZ WSTRZYKIWANIE	73
Wstrzykiwanie SQL-a	74
Czym jest SQL?	74
Anatomia ataku wstrzykiwania SQL-a	75
Pierwsza metoda obrony: użycie instrukcji parametryzowanych	77
Druga metoda obrony: użycie mapowania obiektowo-relacyjnego	78
Dodatkowa metoda obrony: obrona w głąb	79
Wstrzykiwanie polecenia	81
Anatomia ataku przez wstrzykiwanie polecenia	81
Metoda obrony: stosowanie sekwencji ucieczki dla znaków kontrolnych	83

Zdalne wykonywanie kodu	84
Anatomia ataku przez zdalne wykonywanie kodu	84
Metoda obrony: zablokowanie wykonywania kodu podczas deserializacji	84
Luki związane z przysyłaniem plików	85
Anatomia ataku przez przestanie pliku	86
Metody obrony	87
Podsumowanie	89

7

ATAKI CROSS-SITE SCRIPTING	91
Zapisane ataki cross-site scripting	92
Pierwsza metoda obrony: stosowanie sekwencji ucieczki dla znaków HTML-a	94
Druga metoda obrony: implementacja zasad Content Security Policy	95
Odbite ataki cross-site scripting	97
Metoda ochrony: stosowanie sekwencji ucieczki w dynamicznej zawartości żądań HTTP	98
Ataki cross-site scripting oparte na hierarchii DOM	98
Metoda obrony: stosowanie sekwencji ucieczki w dynamicznej treści z fragmentów URI	100
Podsumowanie	101

8

ATAKI CROSS-SITE REQUEST FORGERY	103
Anatomia ataku CSRF	104
Pierwsza metoda obrony: przestrzeganie zasad REST	105
Druga metoda obrony: implementacja cookie z tokenami CSRF	105
Trzecia metoda obrony: użycie atrybutu cookie SameSite	107
Dodatkowa metoda obrony: wymagaj ponownego uwierzytelnienia w przypadku wrażliwych operacji	108
Podsumowanie	108

9

NARUSZANIE UWIERZYTELNIANIA	109
Implementacja uwierzytelniania	110
Natywne uwierzytelnianie HTTP	110
Nienatywne uwierzytelnianie	111
Ataki brute-force	111
Pierwsza metoda obrony: uwierzytelnianie zewnętrzne	112
Druga metoda obrony: integracja pojedynczego logowania	113
Trzecia metoda obrony: zabezpieczenie własnego systemu uwierzytelniania	113
Konieczność podania nazwy użytkownika, adresu e-mail lub obydwu	113
Konieczność tworzenia skomplikowanych haseł	116
Bezpieczne przechowywanie haseł	117
Wymaganie uwierzytelniania wieloskładnikowego	118
Implementowanie i zabezpieczanie funkcji wylogowania	119
Zapobieganie enumeracji użytkowników	120
Podsumowanie	121

10

PRZECHWYTYWANIE SESJI	123
Jak działają sesje	124
Sesje po stronie serwera	124
Sesje po stronie klienta	126

Jak hakerzy przechwytują sesje	127
Kradzież cookie	127
Fiksacja sesji	129
Wykorzystanie słabych identyfikatorów sesji	130
Podsumowanie	131
11	
UPRAWNIENIA	133
Eskalacja uprawnień	134
Kontrola dostępu	134
Opracowanie modelu autoryzacji	135
Implementacja kontroli dostępu	136
Testowanie kontroli dostępu	137
Dodawanie ścieżek audytu	138
Unikanie typowych niedopatrzeń	138
Directory traversal	139
Ścieżki do plików i ścieżki względne	139
Anatomia ataku directory traversal	140
Pierwsza metoda obrony: zaufaj serwerowi WWW	141
Druga metoda obrony: skorzystaj z usługi hostingowej	141
Trzecia metoda obrony: użycie niebezpośrednich odwołań do plików	142
Czwarta metoda obrony: czyszczenie odwołań do plików	142
Podsumowanie	143
12	
WYCIĘKI INFORMACJI	145
Pierwsza metoda obrony: usunięcie wymownych nagłówków serwera	146
Druga metoda obrony: użycie czystych adresów URL	146
Trzecia metoda obrony: użycie ogólnych parametrów cookie	146
Czwarta metoda obrony: wyłączenie raportowania błędów po stronie klienta	147
Piąta metoda obrony: minifikacja lub obfuskacja plików JavaScriptu	148
Szósta metoda obrony: czyszczenie plików po stronie klienta	148
Śledź informacje o lukach w zabezpieczeniach	149
Podsumowanie	149
13	
SZYFROWANIE	151
Szyfrowanie w protokole internetowym	152
Algorytmy szyfrowania, funkcje skrótu i kody uwierzytelniania wiadomości	152
TLS handshake	155
Włączanie HTTPS	157
Certyfikaty cyfrowe	157
Uzyskiwanie certyfikatu cyfrowego	158
Instalowanie certyfikatu cyfrowego	160
Atakowanie HTTP (i HTTPS)	163
Routery bezprzewodowe	163
Hotspoty wi-fi	163
Dostawcy usług internetowych	164
Agencje rządowe	164
Podsumowanie	164

ZEWNĘTRZNE BIBLIOTEKI	167
Zabezpieczanie zależności	168
Z jakiego kodu korzystasz	168
Możliwość szybkiego wdrażania nowych wersji	171
Śledź doniesienia o problemach z bezpieczeństwem	171
Kiedy aktualizować	172
Zabezpieczanie konfiguracji	173
Wyłączanie domyślnych danych dostępowych	173
Wyłączanie otwartych indeksów katalogów	173
Chroń swoją konfigurację	174
Utwadzanie środowisk testowych	175
Zabezpieczanie interfejsu administratora	175
Zabezpieczanie używanych usług	175
Chroń swoje klucze do API	176
Zabezpieczanie mechanizmów webhook	176
Zabezpieczanie treści dostarczanych przez zewnętrzne podmioty	177
Usługi jako wektor ataku	177
Uważaj na malvertising	178
Unikanie dostarczania złośliwego oprogramowania	179
Korzystanie z godnych zaufania platform reklamowych	179
Korzystanie ze standardu SafeFrame	180
Dostosowanie preferencji dotyczących reklam	180
Przeprowadzaj inspekcje podejrzanych reklam i raportuj je	180
Podsumowanie	181

ATAKI NA XML-A	183
Użycie XML-a	184
Walidacja XML-a	185
Pliki Document Type Definition	185
Bomby XML-a	186
Ataki XML External Entity	188
Jak hakerzy wykorzystują zewnętrzne encje	188
Zabezpieczanie parsera XML-a	189
Python	189
Ruby	189
Node.js	189
Java	189
.NET	190
Inne uwarunkowania	190
Podsumowanie	191

NIE BĄDŹ NARZĘDIEM	193
Falszowanie poczty elektronicznej	194
Implementacja metody Sender Policy Framework	195
Implementowanie DomainKeys Identified Mail	195
Zabezpieczanie poczty elektronicznej w praktyce	196
Kamufłowanie złośliwych linków w wiadomościach e-mail	196
Otwarte przekierowania	197
Zapobieganie otwartym przekierowaniom	197
Inne uwarunkowania	198

Clickjacking	198
Ochrona przed atakami typu clickjacking	199
Server-side request forgery	200
Ochrona przed atakami server-side forgery	200
Botnety	201
Ochrona przed instalacją szkodliwego oprogramowania	201
Podsumowanie	202

17

ATAKI DENIAL-OF-SERVICE203

Ataki typu denial-of-service	204
Ataki przez protokół Internet Control Message Protocol	204
Ataki przez Transmission Control Protocol	204
Ataki przez warstwę aplikacji	205
Ataki odbite i wzmocnione	205
Ataki distributed denial-of-service	205
Nieumyślne ataki denial-of-service	206
Ochrona przed atakami denial-of-service	206
Zapory sieciowe i systemy zapobiegania włamaniom	206
Usługi chroniące przed atakami distributed denial-of-service	207
Budowanie z myślą o skalowaniu	207
Podsumowanie	209

18

PODSUMOWANIE211