Obsah

Předmluva 7

Úvod 9

Pravidla 10
Příklady 11
Kapitoly 12
Co v této knize nenaleznete? 13
Poznámka autora 13
Odezva 14

KAPITOLA 1 15

Počátky 15

HTTP 15
Požadavky a odpovědi 16
Hlavička Referer 19
Ukládání do mezipaměti (cache) 20
Soubory cookie 21
Relace 22
Krádež relace 23
HTTPS 26
Závěr 29
Chcete se dozvědět více? 29

KAPITOLA 2 31

Přenos dat do subsystémů 31

SQL Injection 32
Příklady, příklady a zase příklady 32
Využívání chybových hlášení k získávání informací 39
Jak se vyhnout útoku typu SQL Injection 41
Shell Command Injection 46

Příklady 47
Ochrana před útokem Shell Command Injection 49
Povídání k programům napsaným v jazycích C/C++ 54
Příklad 54
Proradná funkce Eval 56
Řešení problémů s metaznaky 56
Interpretace metaznaků na více úrovních 57
Architektura 58
Strategie defense in depth
– současné zabezpečení prostřednictvím několika mechanismů 59
Shrnutí 60

KAPITOLA 3 63
Vstup uživatele 63

Co se vlastně skrývá za slovem vstup? 63
Neviditelná bezpečnostní bariéra 68
Zvláštnosti programovacích jazyků: zcela neočekávaný vstup dat 70
Kontrola vstupu 72
Bílá listina oproti černé listině 76
Ošetření neplatného vstupu 78
Zaznamenávání událostí do protokolu 80
Rizika kontroly vstupu na straně klienta 83
Problémy s přístupovými oprávněními 86
Nepřímý přístup k datům 87
Když se klientovi předává příliš mnoho dat 89
Když chybí kontrola oprávnění 93
Ověření přístupu utajením 94
Ochrana vstupu vytvořeného serverem 95
Shrnutí 98

KAPITOLA 4 99
Ošetření výstupu: útok Cross-site Scripting 99

Příklady 100
Krádež relace 101
Úprava textu 104
Útok Cross-site Scripting vedený metodou sociálního inženýrství 105
Krádež hesel 108
Příliš málo znaků pro skripty? 110
Problém 111
Řešení 112
Kódování HTML 113
Výběrové filtrování značek 114
Návrh programu 119
Znakové sady používané v prohlížečích 120

Shrnutí 121
Chcete se dozvědět více? 121

KAPITOLA 5 123
Trojské koně 123

Příklady 123
Problém 128
Řešení 128
Shrnutí 130

KAPITOLA 6 131
Hesla a další tajné informace 131

Šifrování 131
Symetrické šifrování 132
Asymetrické šifrování 133
Hašovací funkce 134
Digitální podpisy 135
Certifikáty 136
Ověřování uživatelů pomocí hesel 137
O nešifrovaných heslech 137
Zapomenutá hesla 139
Prolomení hašů hesel 140
Pamatujete si na mě? 143
Utajené identifikátory 145
Únik tajných informací 147
Únik informací v požadavcích přenášených metodou GET 148
Chybějící šifrování 150
Dostupnost kódu na straně serveru 150
Problematické názvy souborů 151
Chyby v systémových aplikacích 152
Shrnutí 153
Chcete se dozvědět více? 154

KAPITOLA 7 155
Nepřátelé bezpečného kódu 155

Nedostatek informací 155
Nepořádnost 157
Uzávěrka 163
Prodejci 164
Poznámky na závěr 165
Chcete se dozvědět více? 165

KAPITOLA 8 167
Přehled pravidel pro vytváření bezpečného kódu 167

PŘÍLOHA A 175
Chyby ve webovém serveru 175

PŘÍLOHA B 179
Zachytávání paketů (Packet Sniffing) 179

Naučte se základy protokolu TCP/IP během čtyř minut 179
Zachytávání paketů 181
Útok man in the middle 182
MITM ve spojení s protokolem HTTPS 183
Shrnutí 183
Chcete se dozvědět více? 184

PŘÍLOHA C 185
Odesílání e-mailů ve formátu HTML s falešnou adresou odesílatele 185

PŘÍLOHA D 187
Další informace 187

Diskusní fóra 187
OWASP 188

Odkazy 191

Zkratky 199