

Obsah

| | |
|--|-----------|
| Předmluva | 15 |
| Úvod | 17 |
| „Jsme za vodou, máme přece firewall“ | 18 |
| Chybovat je lidské | 18 |
| Nápis na zdi | 18 |
| Rozvržení knihy | 19 |
| Části | 19 |
| Kapitoly | 20 |
| Závěrečné slovo | 21 |
| Poděkování | 21 |
| Příspěvovatel | 22 |
| Část I Aréna pro elektronický obchod | 23 |
| Případová studie: Acme Art, Inc. napadena! | 24 |
| Kapitola 1 Jazyky pavučiny: Babylón 21. století | 33 |
| Úvod | 34 |
| Jazyky pavučiny | 34 |
| HTML | 35 |
| Dynamické HTML (DHTML) | 38 |
| XML | 38 |
| XHTML | 39 |
| Perl | 39 |
| PHP | 43 |
| ColdFusion | 45 |
| ColdFusion Application Server | 45 |
| ColdFusion Markup Language | 46 |
| ColdFusion Studio | 47 |
| ASP | 47 |
| Propojení s databázemi | 49 |
| CGI | 53 |
| Java | 57 |
| Shrnutí | 67 |

| | |
|---|-----|
| Kapitola 2 Webové a databázové servery | 69 |
| Úvod | 70 |
| Web servery..... | 70 |
| Apache..... | 70 |
| Internet Information Server (IIS) | 75 |
| Databázové servery..... | 85 |
| Microsoft SQL Server | 87 |
| Oracle | 93 |
| Shrnutí | 102 |
| Kapitola 3 Nákupní košíky a platební portály | 103 |
| Úvod | 104 |
| Vývoj prodejny | 105 |
| Elektronické nakupování..... | 107 |
| Nákupní košíky | 109 |
| Životní cyklus elektronického košíku | 109 |
| Sbírání, zkoumání a porovnávání vybraného zboží | 109 |
| Sledování celkové ceny..... | 109 |
| Změny ve výběru..... | 109 |
| Provedení nákupu..... | 110 |
| Implementace nákupního košíku | 111 |
| Katalog zboží | 112 |
| Správa relace | 112 |
| Komunikace s databázemi | 112 |
| Spolupráce s platebním portálem | 113 |
| Ukázky špatných implementací nákupních košíků | 113 |
| Nákupní košík Carello..... | 113 |
| Nákupní košík DCShop..... | 113 |
| Nákupní košík Hassan Consulting | 114 |
| Cart32 a další nákupní košíky | 114 |
| Provedení platby..... | 114 |
| Dokončení objednávky..... | 114 |
| Způsob platby..... | 114 |
| Ověřování a ochrana před podvody | 115 |
| Provedení objednávky a vystavení stvrzenky | 115 |
| Přehled systému pro zpracování plateb..... | 115 |
| Stránka s potvrzením objednávky | 117 |
| Rozhraní k platebnímu portálu..... | 117 |
| Rozhraní k databázi transakcí | 118 |
| Spolupráce s platebním portálem – ukázka | 118 |

| | |
|--|------------|
| Problémy spojené s implementací platebních systémů | 121 |
| Propojení | 122 |
| Dočasné informace | 122 |
| SSL | 122 |
| Ukládání uživatelských profilů | 122 |
| PayPal – elektronické platby pro jednotlivce | 123 |
| Shrnutí | 124 |
| Kapitola 4 HTTP a HTTPS: Hackerská latina | 125 |
| Úvod | 126 |
| Webové protokoly | 126 |
| HTTP | 127 |
| HTTPS (HTTP přes SSL) | 134 |
| Shrnutí | 136 |
| Kapitola 5 URL: Hackerův meč | 137 |
| Úvod | 138 |
| Struktura URL | 139 |
| URL a předávání parametrů | 141 |
| Zápis URL | 143 |
| Metaznaky | 144 |
| Vkládání zvláštních znaků do URL | 145 |
| Kódování Unicode | 146 |
| Zneužívání kódování URL | 147 |
| Díra v Unicode | 148 |
| Díra ve dvojitém dekódování | 149 |
| HTML formuláře | 151 |
| Anatomie HTML formuláře | 152 |
| Vstupní prvky | 153 |
| Předávání parametrů metodami GET a POST | 155 |
| Shrnutí | 159 |
| Část II URL tajemství zbavená | 161 |
| Případová studie: Průzkum odhalil výši aktiv | 162 |
| Kapitola 6 Rozplétání pavučiny | 165 |
| Úvod | 166 |
| Součásti webové aplikace | 166 |
| Vnější web server | 168 |
| Prováděcí prostředí pro webové aplikace | 169 |
| Databázový server | 170 |

| | |
|--|------------|
| Propojení komponent..... | 170 |
| Domácí zpracovávací prostředí..... | 171 |
| API a plug-iny web serveru | 171 |
| Přesměrování URL a vnitřní zastoupení | 171 |
| Zastoupení vnitřním aplikačním serverem..... | 171 |
| Příklady | 172 |
| Propojení s databází | 177 |
| Použití API konkrétní databáze..... | 177 |
| Příklady | 177 |
| Použití ODBC | 178 |
| Použití JDBC..... | 179 |
| Specializované webové aplikační servery | 180 |
| Rozpoznávání součástí webové aplikace podle URL | 180 |
| Základy rozpoznávání technologií | 181 |
| Příklady | 182 |
| Další příklady | 184 |
| Pokročilé techniky rozpoznávání technologií..... | 186 |
| Příklady | 187 |
| Rozpoznávání databázových serverů..... | 188 |
| Protiopatření | 190 |
| Pravidlo 1: HTTP hlavička musí prozradit co nejméně..... | 191 |
| Pravidlo 2: Prohlížeči nesmí být zaslány chybová hlášení | 191 |
| Shrnutí | 191 |
| Kapitola 7 Mezi řádky | 193 |
| Úvod | 194 |
| Únik informací přes HTML | 195 |
| Co vám prohlížeč neukáže | 195 |
| Netscape Navigator – View Page Source..... | 196 |
| Internet Explorer – Zobrazit Zdrojový kód..... | 197 |
| Stopy, které hledat..... | 198 |
| HTML komentáře | 198 |
| Průběh úprav | 199 |
| Podrobnosti o vývojáři nebo autorovi..... | 199 |
| Odkazy na další části webové aplikace..... | 200 |
| Popisky a poznámky | 200 |
| Komentáře vložené webovým aplikačním serverem | 201 |
| Starý „zakomentovaný“ kód | 201 |
| Vnitřní a vnější odkazy..... | 202 |
| E-mailové adresy a uživatelská jména..... | 202 |

| | |
|--|------------|
| Spam, spam, spam..... | 203 |
| Klíčová slova a značky meta..... | 203 |
| Skrytá pole..... | 204 |
| Klientské skripty..... | 205 |
| Techniky automatizace prosívání zdrojových textů..... | 206 |
| Použití programu wget..... | 206 |
| Použití programu grep..... | 209 |
| Sam Spade, Black Widow a Teleport Pro..... | 210 |
| Shrnutí..... | 211 |
| Kapitola 8 Rozbor struktury webu | 213 |
| Úvod..... | 214 |
| HTML a rozbor struktury webu..... | 214 |
| Metodika rozboru struktury webu..... | 215 |
| Krok 1: Prolezení webu..... | 216 |
| Ruční prolezení webu..... | 216 |
| Bližší pohled na HTTP hlavičku..... | 216 |
| Oblíbené nástroje pro rozbor struktury webu..... | 217 |
| Závěr kroku 1..... | 221 |
| Krok 2: Rozdělení struktury aplikace na logické celky..... | 223 |
| Závěr kroku 2..... | 226 |
| Krok 3: Rozbor jednotlivých webových zdrojů..... | 226 |
| 1. Rozbor přípon..... | 226 |
| 2. Rozbor cest v URL..... | 226 |
| 3. Rozbor relace..... | 227 |
| 4. Účel formulářů..... | 228 |
| 5. Účel appletů a objektů..... | 228 |
| 6. Vyhodnocení klientských skriptů..... | 229 |
| 7. Rozbor komentářů a e-mailových adres..... | 229 |
| Závěr kroku 3..... | 229 |
| Krok 4: Inventarizace webových zdrojů..... | 230 |
| Shrnutí..... | 231 |
| Část III Jak na to jdou? | 233 |
| Případová studie: Kterak Boris Anně ke štěstí pomohl..... | 234 |
| Kapitola 9 Kybergraffiti | 237 |
| Úvod..... | 238 |
| Znetvoření webu Acme Travel, Inc..... | 238 |
| Mapování cílové sítě..... | 241 |

| | |
|---|------------|
| Proplížení přes proxy | 242 |
| Prolomení HTTP autentizace | 245 |
| Procházení adresářů | 248 |
| Nahrání znetvořených stránek..... | 252 |
| Kde byla chyba? | 255 |
| Kladiva na HTTP autentizaci..... | 256 |
| Brutus | 257 |
| WebCracker 4.0..... | 258 |
| Protiopatření proti útoku na Acme Travel, Inc..... | 260 |
| Znepřístupnění proxy | 260 |
| Použití silnějších hesel pro HTTP autentizaci | 260 |
| Zakázání procházení adresářů | 261 |
| Shrnutí | 262 |
| Kapitola 10 Elektroničtí zloději | 263 |
| <hr/> | |
| Úvod | 264 |
| Výstavba elektronického obchodu | 265 |
| Vlastní obchod | 266 |
| Nákupní košík | 266 |
| Pokladna..... | 266 |
| Databáze | 266 |
| Propojení | 267 |
| Vývoj elektronických prodejen | 267 |
| Vykradení Acme Fashions, Inc. | 268 |
| Výstavba elektronické prodejny Acme Fashion | 269 |
| Hledání jádra problému..... | 270 |
| Přestavba www.acme-fashions.com..... | 282 |
| Nové problémy opraveného systému..... | 282 |
| Posmrtná a další protiopatření..... | 289 |
| Shrnutí | 291 |
| Kapitola 11 Přístup k databázím | 293 |
| <hr/> | |
| Úvod | 294 |
| Napadení autobazaru | 297 |
| Kontrola vstupu..... | 297 |
| Protiopatření | 302 |
| Shrnutí | 303 |

| | | |
|--|----------------------------------|-----|
| Kapitola 12 | Java: Vzdálené provádění příkazů | 305 |
| Úvod | | 306 |
| Technologie založené na Javě | | 307 |
| Architektura javových aplikačních serverů | | 308 |
| Útok na javový web server | | 309 |
| Hledání děr v javových aplikačních serverech | | 310 |
| Úkázka: Internetový portál pro obchod s cennými papíry | | 311 |
| Protiopatření | | 322 |
| Opevnění javového serveru | | 322 |
| Další obecná protiopatření | | 323 |
| Shrnutí | | 325 |
| Kapitola 13 | Falšování identity | 327 |
| Úvod | | 328 |
| Únos relace: Ukradená totožnost a zkažená schůzka | | 328 |
| 5. března, 7:00 – Alicin byt | | 328 |
| 8:30 – Alice v práci | | 330 |
| 10:00 – Bobova kancelář | | 331 |
| 11:00 – Bobova kancelář | | 332 |
| 12:30 – Alicina kancelář | | 336 |
| 21:30 – Bertoliniho italská restaurace | | 337 |
| Únosy relací | | 337 |
| Dodatečná analýza únosu relace | | 338 |
| Stavové diagramy aplikace | | 339 |
| HTTP a sledování relace | | 340 |
| Stavové a bezstavové aplikace | | 341 |
| Cookies a skrytá pole | | 344 |
| Cookies | | 344 |
| Skrytá pole | | 344 |
| Implementace relace a její správy | | 345 |
| Identifikátory relací by měly být jedinečné | | 345 |
| Identifikátory relací by neměly být „uhodnutelné“ | | 345 |
| Identifikátory by měly být nezávislé | | 345 |
| Identifikátory by měly být provázány se síťovými spojeními | | 346 |
| Shrnutí | | 346 |
| Kapitola 14 | Přeplnění vyrovnávacích pamětí | 347 |
| Úvod | | 348 |
| Příklad | | 348 |
| Přeplnění vyrovnávacích pamětí | | 349 |

| | |
|---|-----|
| Přeplnění: Nejjednodušší varianta | 349 |
| Přeplnění: ukázka | 355 |
| Dodatečná protiopatření | 360 |
| Shrnutí | 360 |

Část IV Webové hodiny pro pokročilé

| | |
|------------------------|-----|
| Případová studie | 362 |
|------------------------|-----|

Kapitola 15 Web hacking: Automatizované nástroje

| | |
|-------------------------------|-----|
| Úvod | 366 |
| Netcat | 366 |
| Whisker | 368 |
| Hrubá síla | 370 |
| Brutus | 372 |
| Achilles | 375 |
| Cookie Pal | 378 |
| Teleport Pro | 387 |
| Bezpečnostní doporučení | 388 |
| Shrnutí | 389 |

Kapitola 16 Červi

| | |
|--------------------------|-----|
| Úvod | 392 |
| Červ Code Red | 392 |
| 26. ledna 2000 | 392 |
| 18. června 2001 | 392 |
| 12. července 2001 | 393 |
| 19. července 2001 | 394 |
| 4. srpna, 2001 | 395 |
| Červ Nimda | 396 |
| Boj s novými červy | 397 |
| Vždy ve střehu | 398 |
| Shrnutí | 398 |

Kapitola 17 Jak vyzrát na IDS

| | |
|-----------------------------|-----|
| Úvod | 400 |
| Základy detektorů | 400 |
| Síťové detektory | 401 |
| Hostitelské detektory | 401 |
| Přesnost detektorů | 401 |
| Cesta za detektor | 402 |

| | |
|---|-----------|
| Bezpečný hacking – hackování přes SSL..... | 402 |
| Příklad | 403 |
| Tunelování útoků přes SSL..... | 405 |
| Detekce průniku přes SSL..... | 406 |
| Sledování SSL provozu..... | 406 |
| Polymorfní URL | 409 |
| Šestnáctkové kódování..... | 410 |
| Neplatné kódování znaků v Unicode | 411 |
| Doplňování falešných cest | 411 |
| Vkládání „./“ | 411 |
| Použití nestandardních oddělovačů cesty | 412 |
| Použití násobných lomítek | 412 |
| Kombinování různých technik | 412 |
| Vyvolávání planých poplachů | 413 |
| Možná protiopatření..... | 414 |
| Dešifrování SSL..... | 415 |
| Dekódování URL | 415 |
| Shrnutí | 415 |
| <hr/> Dodatek A | <hr/> 417 |
| <hr/> Dodatek B | <hr/> 419 |
| <hr/> Dodatek C | <hr/> 423 |
| <hr/> Dodatek D | <hr/> 427 |
| <hr/> Dodatek E | <hr/> 433 |
| <hr/> Dodatek F | <hr/> 435 |
| <hr/> Rejstřík | <hr/> 437 |