

STRUČNÝ OBSAH

ČÁST 1 PŘEDBĚŽNÁ PROHLÍDKA

1	Úvod do bezpečnosti webových aplikací	3
2	Profilování	23
3	Hacking webových serverů	37

ČÁST 2 ÚTOK

5	Ověřování	113
6	Autorizace	139
7	Útok na správu stavu relace	153
8	Útoky na validaci vstupu	173
9	Útoky na webová úložiště dat	193
10	Útoky na webové služby	207
11	Hacking správy webových aplikací	223
12	Hacking webových klientů	239
13	Případové studie	259

ČÁST 3 PŘÍLOHY

A	Seznam úkonů při kontrole bezpečnosti webového serveru	269
B	Tahák s nástroji a postupy pro webový hacking	273
C	Použití programu libwhisker	285
D	Instalace a konfigurace nástroje UrlScan	295
E	O doprovodných webových stránkách	317

SOUHRN	315
ODKAZY A DALŠÍ LITERATURA	315
E O doprovodných webových stránkách	317
Rejstřík	319

Učební texty a přílohy jsou na portálu www.cerch.cz dostupné v digitální podobě. Další informace o tom, jak používat tento portál, najdete v příloze 1.

— Mladá Boleslav —

VĚNOVÁNÍ ČESKÝM ČTENÁŘŮM

Čtení je základem naší práce s MČL a klíčová jevová rovina. Každá polovina čtenářského ročníku představuje pro programování v úvodu semestrálního ročníku je určeno určité množství, které je určeno podle potřeb učiva. Čtení je základem naší práce s MČL a klíčová jevová rovina. Každá polovina čtenářského ročníku představuje pro programování v úvodu semestrálního ročníku je určeno určité množství, které je určeno podle potřeb učiva. Čtení je základem naší práce s MČL a klíčová jevová rovina. Každá polovina čtenářského ročníku představuje pro programování v úvodu semestrálního ročníku je určeno určité množství, které je určeno podle potřeb učiva.

— Mladá Boleslav, listopad 2014 —

OBSAH

VĚNOVÁNÍ	xix
VĚNOVÁNÍ ČESKÝM ČTENÁŘŮM	xix
O AUTORECH	xxi
O PŘÍSPÍVAJÍCÍCH AUTORECH	xxii
PŘEDMLUVA	xxiii
PODĚKOVÁNÍ	xxiv
Úvod	xxv
ZAMOTANÁ PAVUČINA, KTEROU JSME UTKALI	xxv
JAK JE TATO KNIHA USPOŘÁDÁNA	xxvi
ČÁSTI	xxvi
Kapitoly: metodologie webového hackingu bez tajemství	xxvi
Modularita, organizace a usnadnění	xxvii
ZÁKLADNÍ STAVEBNÍ KAMENY: ÚTOK A OBRANA	xxvii
Další vizuální nápovědy	xxviii
ON-LINE ZDROJE A NÁSTROJE	xxviii
VŠEM NAŠIM ČTENÁŘŮM	xxix

PŘEDBĚŽNÁ PROHLÍDKA

1	Úvod do bezpečnosti webových aplikací	3
	ARCHITEKTURA WEBOVÝCH APLIKACÍ	5
	Několik slov o jazyce HTML	5
	Transportní protokol: HTTP	7
	Další protokoly	9
	Webový klient	10
	Webový server	11
	Webové servery versus webové aplikace	11
	Webová aplikace	12
	Databáze	15
	Různé komplikace a prostředníci	15
	Nový model: webové služby	16
	POTENCIÁLNÍ SLABÁ MÍSTA	17
	METODY PRONIKÁNÍ DO WEBŮ	18
	Profilování infrastruktury	18
	Útok na webové servery	18
	Zmapování aplikace	18
	Útok na mechanismus ověřování	19
	Útok na schéma autorizace	19
	Provedení funkční analýzy	19
	Zneužití datové konektivity	19
	Útok na rozhraní pro správu	19
	Útok na klienta	20
	Naplánování útoku odmítnutí služby	20
	SOUHRN	20
	ODKAZY A DALŠÍ LITERATURA	20
2	Profilování	23
	OBJEVOVÁNÍ SERVERU	24
	Intuice	24
	Internet footprinting	24
	Dotazy DNS	28
	Ping	28
	Objevování prostřednictvím skenování portů	29
	Práce s virtuálními servery	30
	OBJEVOVÁNÍ SLUŽEB	31
	IDENTIFIKACE SERVERU	33
	Práce se SSL	34

SOUHRN	35
ODKAZY A DALŠÍ LITERATURA	35
3 Hacking webových serverů	37
NEJČASTĚJŠÍ SLABÁ MÍSTA PODLE PLATFORMEM	38
Apache	38
Microsoft Internet Information Server (IIS)	41
Útoky proti komponentám IIS	42
Útoky proti IIS	50
Získání vyšších oprávnění na IIS	57
Netscape Enterprise Server	63
Slabá místa dalších webových serverů	66
Různé techniky hackingu webových serverů	68
SOFTWARE PRO AUTOMATICKÉ SKENOVÁNÍ SLABÝCH MÍST	70
Whisker	70
Nikto	73
twwwscan/arirang	73
Stealth HTTP Scanner	74
Typhon	75
WebInspect	77
AppScan	78
FoundScan WebModule	79
ODEPŘENÍ SLUŽEB WEBOVÝCH SERVERŮ	79
SOUHRN	82
ODKAZY A DALŠÍ LITERATURA	82
4 Mapování aplikace	86
DOKUMENTOVÁNÍ STRUKTURY APLIKACE	86
RUČNÍ INSPEKCE APLIKACE	88
Staticky a dynamicky generované stránky	88
Adresářová struktura	90
Pomocné soubory	93
Třídy a aplety jazyka Java	94
Komentáře HTML a obsah	95
Formuláře	97
Řetězce s dotazy	98
Dataázová spojení	100
NÁSTROJE PRO AUTOMATICKÝ PRŮZKUM	101
lynx	101
wget	103
Teleport Pro	104

Black Widow	105
WebSleuth	105
BĚŽNÁ OBRANA	107
Upozornění	107
Ochrana adresářů	108
Ochrana souborů include	108
Různé rady	109
SOUHRN	109
ODKAZY A DALŠÍ LITERATURA	110

ČÁST 2**ÚTOK**

5	Ověřování	113
	OVĚŘOVACÍ MECHANISMY	114
	Ověřování HTTP: Basic a Digest	114
	Integrated Windows (NTLM)	117
	Negotiate	121
	Certifikáty	122
	Vicenásobné ověřovací metody	122
	Formulářové ověřování	123
	Microsoft Passport	125
	ÚTOKY NA WEBOVÉ OVĚŘOVÁNÍ	128
	Hádání hesel	128
	Hádání ID relací a hrubá síla	133
	Podvracení (subverting) cookie	134
	Obejití přihlašovacích formulářů nad SQL	135
	OBEJÍTÍ OVĚŘOVÁNÍ	136
	SOUHRN	137
	ODKAZY A DALŠÍ LITERATURA	137
6	Autorizace	139
	ÚTOKY	140
	Maticí rolí	141
	Metodika	141
	Dotazový řetězec	142
	Data POST	142
	Skryté tagy	143
	URI	143
	Hlavičky protokolu HTTP	144

Soubory cookie	144
Závěrečné poznámky	144
Případová studie: Použití nástroje CURL pro mapování oprávnění	146
Obrana	149
Autorizace serveru Apache	150
Autorizace na serveru IIS	151
SOUHRN	152
ODKAZY A DALŠÍ LITERATURA	152
7 Útok na správu stavu relace	153
METODY NA STRANĚ KLIENTA	155
Skrutá pole	156
URL	157
Hlavičky HTTP a soubory cookie	157
METODY NA STRANĚ SERVERU	158
Identifikátory relací generované serverem	159
Databáze relací	159
ANALÝZA IDENTIFIKÁTORU RELACE	160
Analýza obsahu	160
Časová okna	170
SOUHRN	172
ODKAZY A DALŠÍ LITERATURA	172
8 Útoky na validaci vstupu	173
OČEKÁVÁNÍ NEOČEKÁVATELNÉHO	174
CÍLE ÚTOKŮ NA VALIDACI VSTUPU	175
KDE NAJÍT POTENCIÁLNÍ TERČE	175
OBEJÍT PROCEDUR OVĚŘOVÁNÍ NA STRANĚ KLIENTA	175
BĚŽNÉ ÚTOKY NA VALIDACI VSTUPU	176
Přeplnění vyrovnávací paměti	177
Kanonizace (tečka-tečka-lomítko)	179
Útoky pomocí skriptů	183
Zmanipulování aplikace	187
Útoky vložení kódu SQL a na úložiště dat	187
Spuštění příkazu	188
Běžné vedlejší efekty	188
BĚŽNÁ OBRANA	189
SOUHRN	190
ODKAZY A DALŠÍ LITERATURA	191

9	Útoky na webová úložiště dat	193
	ÚVOD DO SQL	194
	VLOŽENÍ KÓDU SQL	194
	OR 1=1	204
	UNION	205
	INSERT	205
	Běžná obrana	205
	SOUHRN	206
	ODKAZY A DALŠÍ LITERATURA	206
10	Útoky na webové služby	207
	CO JE WEBOVÁ SLUŽBA?	208
	Přenos: SOAP prostřednictvím HTTP(S)	209
	WSDL	211
	Adresářové služby: UDDI a DISCO	213
	UKÁZKY HACKINGU WEBOVÝCH SLUŽEB	215
	ZÁKLADY ZABEZPEČENÍ WEBOVÉ SLUŽBY	217
	Podobnosti se zabezpečením webových aplikací	217
	Opatření pro zabezpečení webových služeb	217
	SOUHRN	220
	ODKAZY A DALŠÍ LITERATURA	221
11	Hacking správy webových aplikací	223
	ADMINISTRACE WEBOVÉHO SERVERU	224
	Telnet	224
	SSH	224
	Speciální porty pro správu	225
	Další služby pro administraci	225
	SPRÁVA WEBOVÉHO OBSAHU	226
	FTP	227
	SSH/SCP	227
	FRONTPAGE	227
	WebDAV	231
	WEBOVÁ SPRÁVA SÍTÍ A SYSTÉMŮ	232
	Další webové nástroje pro správu	235
	SOUHRN	236
	ODKAZY A DALŠÍ LITERATURA	236

12	Hacking webových klientů	239
	PROBLÉM S BEZPEČNOSTÍ NA STRANĚ KLIENTA	240
	Metodologie útoku	241
	ÚTOKY S AKTIVNÍM OBSAHEM	241
	Java a JavaScript	241
	ActiveX	243
	Opatření na straně serveru	249
	Cross-site scripting	249
	KRÁDEŽ SOUBORU COOKIE (COOKIE HIJACKING)	252
	SOUHRN	256
	ODKAZY A DALŠÍ LITERATURA	257
13	Případové studie	259
	PŘÍPADOVÁ STUDIE Č. 1: OD URL K PŘÍKAZOVÉ ŘÁDCE A ZASE ZPÁTKY	260
	Obrana v případové studii č. 1	262
	PŘÍPADOVÁ STUDIE Č. 2: XOR SE NEROVNÁ BEZPEČNOST	262
	Obrana v případové studii č. 2	263
	PŘÍPADOVÁ STUDIE Č. 3: KALENDÁŘ A CROSS-SITE SCRIPTING	264
	Opatření v případové studii č. 3	265
	SOUHRN	265
	ODKAZY A DALŠÍ LITERATURA	266

ČÁST 3

PŘÍLOHY

A	Seznam úkonů při kontrole bezpečnosti webového serveru	269
B	Tahák s nástroji a postupy pro webový hacking	273
	Víceúčelové nástroje	274
	Profilování	274
	Whois	275
	Běžné porty používané při profilování	275
	Útoky na webové servery	276
	Skenery slabých míst webových aplikačních serverů	277
	Průzkum aplikace	278
	Ověřování	278
	Správa stavů	279
	Validace vstupů	279
	Oblíbené znaky pro testování validace vstupů	279
	Formátovací znaky SQL	280

Základní syntaxe pro vkládání SQL	280
Užitečné proměnné MS SQL Serveru	281
Uložené procedury pro průzkum SQL Serveru	281
Parametrisované rozšířené uložené procedury MS SQL	281
Rozšířené uložené procedury bez parametrů	282
Objekty systémových tabulek SQL	282
Standardní tabulky databáze Master v SQL	282
Běžné porty používané pro webovou správu	283
Potenciálně škodlivé metody protokolu WebDAV	284
Běžná hesla	284
Analýza na straně klienta	284

C Použití programu libwhisker 285

LIBWHISKER PODROBNĚ	286
Funkce crawl	288
Funkce utils_randstr	290
Vytváření skriptu pomocí nástroje libwhisker	291
Sinjection.pl	291

D Instalace a konfigurace nástroje UrlScan 295

PŘEHLED NÁSTROJE URLSCAN	296
ZÍSKÁNÍ NÁSTROJE URLSCAN	296
Instalace aktualizací nástroje UrlScan	297
AKTUALIZACE PROGRAMŮ RODINY WINDOWS	297
hfnetchk	297
Nástroje nezávislých firem	299
ZÁKLADNÍ INSTALACE NÁSTROJE URLSCAN	300
Odstranění nástroje IISLockdown	304
Bezobslužná instalace nástroje IISLockdown	305
INSTALACE NÁSTROJE URLSCAN PRO POKROČILÉ	306
Rozbalení UrlScan.dll	306
Konfigurace UrlScan.ini	306
Instalace filtru UrlScan s rozhraním ISAPI pod IIS	308
Odstranění filtru UrlScan	311
Popis příkazů v souboru UrlScan.ini	311
Oddíl Options	311
Oddíl AllowVerbs	313
Oddíl DenyVerbs	313
Oddíl DenyHeaders	314
Oddíl AllowExtensions	314
Oddíl DenyExtensions	314