

Roman Kümmel

XSS

Cross-Site Scripting v praxi

o reálných zranitelnostech ve virtuálním světě

2011

Cross-Site Scripting v praxi

Autor: Roman Kümmel (ccuminn@soom.cz, www.soom.cz)

Vydal, vytiskl: Tigris spol. s r o. Zlín, www.TiskovyExpress.cz

Rok vydání: 2011

ISBN 978-80-86062-34-1

Obsah

Obsah	3
Předmluva	7
Úvod	9
Kapitola 1	10
Skriptování	10
JavaScript	11
DOM	24
AJAX	36
Same Origin Policy	40
Kapitola 2	42
Nástroje, které pomohou	42
Nástroje pro psaní a ladění kódu	43
Lokální proxy servery	47
Kódování/dekódování znaků a kódů	50
Kapitola 3	52
Úvod do XSS a souvisejících zranitelností	52
Perzistentní XSS	54
Non-perzistentní (reflected) XSS	62
DOM-based XSS	74
CSRF	76
Clickjacking	85
HTML injection	91
Kapitola 4	92
Pokročilé metody injektáže skriptů	92
Skripty v externích souborech	92
In-line skripty	93
Self-contained JavaScript	95

Bypassing	98
Přesměrování.....	112
HTTP Response Splitting.....	116
Skripty v grafických souborech	120
Injektáž skriptu skrz Flash	122
Injektáž skriptu skrz plug-in Acrobat Reader	137
Injektáž skriptu skrz PDF soubory.....	138
Vstup přes QuickTime	139
Spuštění skriptu přes RSS	140
SIXSS.....	141
XSS s využitím RFI a LFI.....	144
Nakažené cookies.....	146
Vstup přes HTTP hlavičky.....	147
Stránka 404	148
Vložení skriptu skrz CSS (XSSTC)	150
Spuštění skriptu ve vlastním profilu	153
Kapitola 5	158
Průstup bezpečnostními filtry	158
Obcházení bezpečnostních filtrů.....	158
Kódování.....	162
Znakové sady	180
Řetězce jako regulární výrazy.....	183
Obfuskace JavaScriptu.....	184
Kapitola 6.....	188
Komunikační kanál mezi obětí a útočníkem.....	188
Parametry GET požadavku	189
XMLHttpRequest.....	191
Generovaný Form	193
Kapitola 7	194
Hledání zranitelností	194
Manuální nástroje.....	195
Poloautomatické nástroje	196

Automatické nástroje	197
Kapitola 8	200
Skrývání útoku	200
Neviditelná akce	200
Odložení akce	200
Jednou spustit stačí	201
Schování útočníka za webovou proxy	202
Kapitola 9	203
Útoky XSS	203
Krádeže session	203
Změna přihlašovacího formuláře	214
Změna obsahu webové stránky	215
Přesměrování uživatelů	216
Keylogger v JavaScriptu	216
Zjištění navštívených stránek	217
Seznam vyhledávaných frází	218
Zjištění, kde je uživatel přihlášen	220
Password cracker	222
Útok na Intranet	224
XSS worms	231
XSS proxy / backdoor	234
Instalace malware	244
Kapitola 10	245
Obrana	245
Na straně webové aplikace	245
Na straně uživatele / webového prohlížeče	249
Content Security Policy	258
Příloha A	264
Použití speciálních znaků	264
Příloha B	274
Vektory injekce kódu	274
Injekce využívající možností HTML5	274

Injekce fungující v HTML4 a starších	278
Injekce založená na CSS	286
Injekce prostého JavaScriptu	293
Injekce založené na E4X v prohlížečích s jádrem Gecko	295
Injekce skrz vlastnosti a metody DOM.....	297
Injekce založené na JSON.....	298
Injekce ukryté v SVG.....	298
Injekce svázané s X(HT)ML.....	305
Injekce založené na UTF-7 a dalších exotických znakových sadách	311
Útoky DoS zaměřené na klienta.....	313
Injekce využívající HTML behavior a binding....	314
Příloha C	319
IT zákony	319
Rejstřík.....	326