

```
handle_connection (sockfd=9, client_addr_ptr=0xbffff810, logf
nywebd.c:86
```

JON ERICKSON

```
0x08048fb7 in main () at tinywebd.c:72
db) print client_addr_ptr
= (struct sockaddr_in *) 0xbffff810
db) print *client_addr_ptr
= (sin_family = 2, sin_port = 15284, sin_addr = {s_addr = 16
n_zero = "\000\000\000\000\000\000\000"}
db) x/x %client_addr_ptr
bffff7e4: 0xbffff810
db) x/24x request + 500
bffff7b4: 0xbffff624 0xbffff624 0xbffff624 0xbffff624
bffff7c4: 0xbffff624 0xbffff624 0xbffff624 0xbffff624
bffff7d4: 0xbffff624 0xbffff624 0xbffff624 0xbffff624
bffff7e4: 0xbffff624 0xbffff624 0xbffff624 0xbffff624
bffff7f4: 0xbffff624 0xbffff624 0xbffff624 0xbffff624
bffff804: 0x0804a8c0 0xbffff818 0x00000010 0x3bb40002
```

HAKINGAS

PROGRAMŲ KODO NARSTYMO MENAS

2-ASIS PATAISYTAS IR PAPILDYTAS LEIDIMAS

```
 breakpoint 2, handle_connection (sockfd=-1073744433, client_addr
gfd=2560)
```

```
 tinywebd.c:90
ptr = strstr(request, " HTTP/"); // Search for valid-looking
```

```
db) x/24x request + 500
bffff7b4: 0xbffff624 0xbffff624 0xbffff624 0xbffff624
bffff7c4: 0xbffff624 0xbffff624 0xbffff624 0xbffff624
bffff7d4: 0xbffff624 0xbffff624 0xbffff624 0xbffff5cf
bffff7e4: 0xbffff5cf 0x00000a00 0xbffff838 0x00000004
bffff7f4: 0x00000000 0x00000000 0x08048a30 0x00000000
bffff804: 0x0804a8c0 0xbffff818 0x00000010 0x3bb40002
```

```
db) print client_addr_ptr
= (struct sockaddr_in *) 0xbffff5cf
```

```
db) print client_addr_ptr
= (struct sockaddr_in *) 0xbffff5cf
```

```
db) print *cli
= (sin_family = 2, sin_port = 15284, sin_addr = {s_addr = 16
n_zero = "\000\000\000\000\000\000\000"}
db) x/s log buffer
```



TURINYS

PRATARMĖ	1
0X100 ĮVADAS	3
0X200 PROGRAMAVIMAS	7
0x210 Kas yra programavimas?	8
0x220 Pseudokodas	9
0x230 Valdymo struktūros	9
0x231 Sąlygos operatorius If-Then-Else	9
0x232 While/Until ciklai	11
0x233 For ciklai	12
0x240 Svarbesnės programavimo sąvokos	13
0x241 Kintamieji	13
0x242 Aritmetiniai operatoriai	14
0x243 Lyginimo operatoriai	16
0x244 Funkcijos	17
0x250 Imkimės darbo	20
0x251 Aiškesnis vaizdas	22
0x252 x86 šeimos procesorius	25
0x253 Asemblerio kalba	27
0x260 Grįžkime prie pagrindų	39
0x261 Eilutės	39
0x262 Su ženklu, be ženklo, ilgos ir trumpos	43
0x263 Rodyklės	45
0x264 Formato eilutės	49
0x265 Tipų priskyrimas	53
0x266 Komandų eilutės argumentai	60
0x267 Kintamojo kontekstas	63
0x270 Atmintinės paskirstymas programoms	70
0x271 Atmintinės segmentai C kalboje	77
0x272 Krūvos naudojimas	79
0x273 Patikrinta malloc() funkcija	81
0x280 Tolesnis darbas su pagrindais	83
0x281 Failų prieiga	83
0x282 Failų prieigos leidimai	88
0x283 Naudotojo identifikatoriai	90
0x284 Struktūros	98
0x285 Funkcijos rodyklės	102
0x286 Pseudoatsitiktiniai skaičiai	103
0x287 Azartinis žaidimas	104

0X300	SPRAGŲ IŠNAUDOJIMAS	117
0x310	Pagrindiniai spragų išnaudojimo metodai	120
0x320	Buferio perpildymas	120
0x321	Dėklo tipo buferio perpildymo spragos	124
0x330	Eksperimentai su BASH apvalkalu	135
0x331	Aplinkos panaudojimas	143
0x340	Perpildymai kituose segmentuose	151
0x341	Nesudėtingas krūvos perpildymas	152
0x342	Funkcijų rodyklės perpildymas	157
0x350	Formato eilutės	168
0x351	Formato parametrai	169
0x352	Formato eilutės spraga	171
0x353	Skaitymas iš pasirenkamųjų atmintinės adresų	173
0x354	Rašymas į pasirenkamuosius atmintinės adresus	174
0x355	Tiesioginė prieiga prie parametru	181
0x356	Trumpųjų įrašų naudojimas	183
0x357	Apėjimas per <code>.ctors</code>	185
0x358	Dar viena <code>noteserch</code> programos spraga	190
0x359	Globaliojo poslinkio lentelės perrašymas	191
0X400	DARBAS TINKLE	195
0x410	OSI modelis	196
0x420	Programinės jungtys	198
0x421	Programinių jungčių funkcijos	199
0x422	Programinių jungčių adresai	200
0x423	Tinklo baitų eiliškumas	202
0x424	Interneto adreso konvertavimas	203
0x425	Nesudėtingo serverio pavyzdys	203
0x426	Žiniatinklio kliento pavyzdys	207
0x427	Tinyweb serveris	213
0x430	Išsamiau apie žemesnius lygmenis	217
0x431	Duomenų kanalų lygmuo	217
0x432	Tinklo lygmuo	219
0x433	Transportavimo lygmuo	221
0x440	Šnipinėjimas tinkle	223
0x441	Tiesioginės prieigos jungčių šnipinėjimo programa	226
0x442	<code>libpcap</code> šnipinėjimo programa	227
0x443	Lygmenų dekodavimas	229
0x444	Aktyvus šnipinėjimas	239
0x450	Paslaugos blokavimas	251

0x451	Užtvindymas SYN paketais	252
0x452	„Mirtina“ užklausa	256
0x453	Paskutinis lašas	256
0x454	Užtvindymas ryšio patikrinimo užklausomis	257
0x455	Srauto didinimo atakos	257
0x456	Paskirstytas DoS užtvindymas	258
0x460	TCP/IP ryšio užvaldymas	258
0x461	RST užvaldymas	259
0x462	Išžėstinis ryšio užvaldymas	264
0x470	Prievadų nuskaitymas	264
0x471	Slaptasis SYN nuskaitymas	265
0x472	FIN, X-mas ir NULL nuskaitymas	265
0x473	Ryšių imitavimas	266
0x474	Neaktyvus nuskaitymas	266
0x475	Išankstinė apsauga (uždanga)	268
0x480	Savarankiškas mėginimas įsilaužti į sistemą	273
0x481	Analizė naudojant GDB derintuvę	274
0x482	Beveik nesiskaito	276
0x483	Su prievadu saistantis apvalkalo kodas	279
0X500	APVALKALO KODAS	283
0x510	Asemblerio ir C kalbų palyginimas	283
0x511	Linux sisteminiai kreipiniai assembleriu	286
0x520	Kelias iki apvalkalo kodo	289
0x521	Dėklą naudojančios assemblerio komandos	289
0x522	Analizė pasitelkus GDB derintuvę	291
0x523	Nulinių baitų pašalinimas	292
0x530	Apvalkalą užvaldantis apvalkalo kodas	298
0x531	Privilegijos	302
0x532	Dar mažesnis apvalkalo kodas	304
0x540	Su prievadu saistantis apvalkalo kodas	306
0x541	Standartinių failų deskriptorių dubliavimas	310
0x542	Valdymo struktūrų nukreipimas	312
0x550	Atgalinio ryšio apvalkalo kodas	316
0X600	ATSAKOMOSIOS PRIEMONĖS	323
0x610	Aptinkančiosios atsakomosios priemonės	324
0x620	Sistemos demonai	324
0x621	Glaustai apie signalus	326
0x622	tinyweb demonas	328

0x630	Rinkoje siūlomos priemonės	332
0x631	tinywebd išnaudojimo priemonė	332
0x640	Žurnalo failai	337
0x641	Susilieti su minia	338
0x650	Akivaizdūs nepastebimi dalykai	340
0x651	Žingsnis po žingsnio	340
0x652	Išnarstyti elementų surinkimas	344
0x653	Antrinis procesas	350
0x660	Papildomas maskavimas	351
0x661	[žurnalą rašomo IP adreso klastojimas	352
0x662	Išnaudojimas be registracijos žurnale	356
0x670	Visa infrastruktūra	358
0x671	Pakartotinis programinės jungties panaudojimas	359
0x680	Naudingosios informacijos „kontrabanda“	363
0x681	Eilutės kodavimas	364
0x682	Kaip paslėpti masyvą	367
0x690	Buferio apribojimai	367
0x691	Polimorfinis spausdinamasis ASCII apvalkalo kodas	370
0x6a0	Atsakomųjų priemonių tobulinimas	380
0x6b0	Nevykdomasis dėklas	380
0x6b1	Grąžinimas į libc biblioteką	381
0x6b2	Grąžinimas į funkciją system()	381
0x6c0	Atsitiktinės dėklo vietos parinkimas	383
0x6c1	Analizė naudojant BASH skriptą ir GDB derintuvę	385
0x6c2	Atspirtis nuo linux-gate	389
0x6c3	Taikomosios žinios	392
0x6c4	Pirmasis bandymas	392
0x6c5	Pamėginkime pasiekti norimą rezultatą	394
0X700	KRIPTOLOGIJA	397
0x710	Informacijos teorija	398
0x711	Absolūtus saugumas	398
0x712	Vienartiniai užpildai	398
0x713	Kvantinio šifro rakto persiuntimas	399
0x714	Praktiškai nepažeidžiamas saugumas	400
0x720	Algoritmo vykdymo trukmė	400
0x721	Asimptotinė išraiška	401
0x730	Simetrinis šifravimas	402
0x731	Lovo Groverio kvantinis paieškos algoritmas	403

0x740	Asimetrinis šifravimas	404
0x741	RSA algoritmas	404
0x742	Piterio Šoro kvantinio skaidymo dauginamaisiais algoritmas ..	408
0x750	Mišrieji šifrai	409
0x751	Pusiaukelės pažeidimai	410
0x752	Skirtingi SSH protokolo kompiuterių kontroliniai kodai	414
0x753	Panašūs kontroliniai kodai	417
0x760	Slaptažodžių atskleidimas	421
0x761	Slaptažodžio atskleidimas naudojant žodyną	423
0x762	Kruopštus slaptažodžio parinkimas	425
0x763	Maišos kodo paieškos lentelė	427
0x764	Slaptažodžio tikimybės matrica	427
0x770	Belaidžio 802.11b ryšio užšifravimas	437
0x771	Laidinį ryšį atitinkantis slaptumas (WEP)	437
0x772	Srauto šifras RC4	438
0x780	WEP pažeidimai	439
0x781	Šifro parinkimas atsijungus nuo tinklo	439
0x782	Daugkartinis šifro rakto srauto naudojimas	440
0x783	Inicijavimo vektoriaus iššifravimo žodynų lentelės	441
0x784	IP peradresavimas	441
0x785	Flurerio, Mantino ir Šamiro pažeidimas	443
0x800	IŠVADOS	453
0x810	Nuorodos	454
0x820	Šaltiniai	455