



活動報告

CTF for GIRLS

■CTF for GIRLS 発起人

■NTTセキュアプラットフォーム研究所

中島明日香 [Asuka Nakajima]

CTF for GIRLS ?



情報セキュリティ技術に興味がある / 学んでいる /
携わっている女性コミュニティを作ること

Why woman only ?

■ 個人の体験 & 周りの話から・・・

興味はあるけど・・・

目立って
居心地が悪い

私（女性には）
向いてないのでは・・・

➡ 女性限定にする事でハードルを下げ触れる機会を増やす

■ 海外でも・・・

[韓国] The Power of XX (POC)

[台湾] HITCON GIRLS

Activities of the CTF for GIRLS

第一回ワークショップ

開催日: 2014年6月28日 (土)

参加者: 約80名

- バイナリ解析
- パケット解析
- フォレンジック
- Webセキュリティ
- (暗号)

第二回ワークショップ

開催日: 2014年10月17日 (金)

参加者: 約50人

- パケット解析



講師も全員女性のセキュリティエンジニア

Contents

バイナリ解析

➡ 16進数/Win32API/アセンブリ基礎/デバッガの使い方

パケット解析

➡ TCP/IP基礎 /パケットの構造について/Wiresharkの使い方

フォレンジック

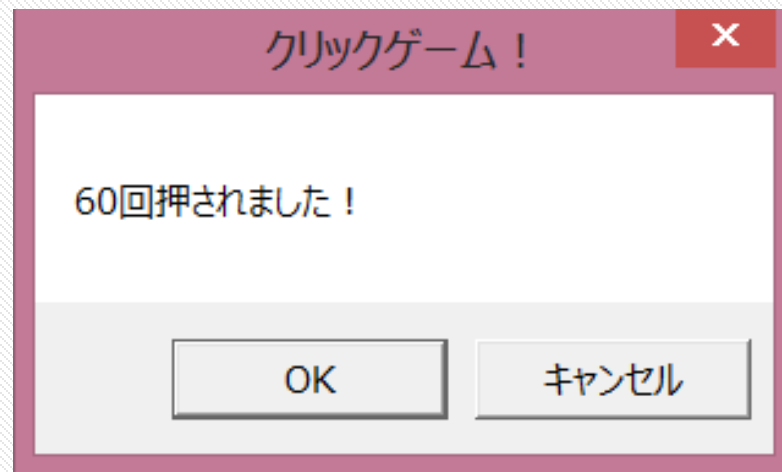
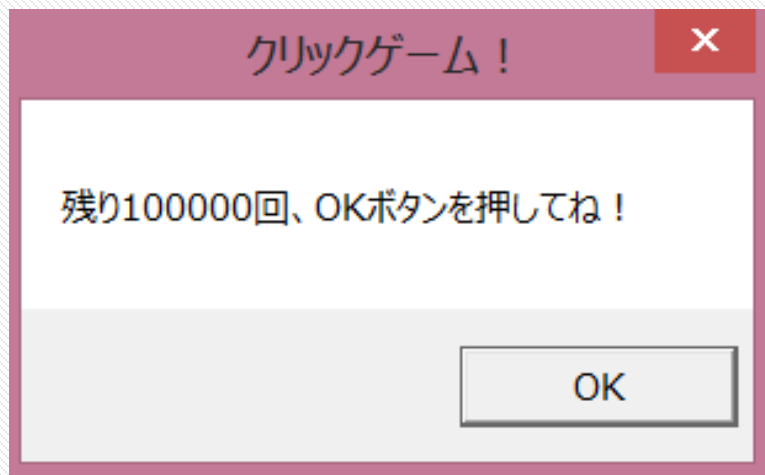
➡ ディスク解析基礎/
レジストリの構造について/
Autopsy・FTK Imagerの使い方

Webセキュリティ

➡ Webセキュリティ基礎/
SQLインジェクション/
ディレクトリトラバーサル



ゲーム風のプログラム



100000回 OKボタンを押すとクリア

Example

バイナリ解析

00401000	\$ 55	PUSH EBP	
00401001	. 89E5	MOV EBP,ESP	
00401003	. 6A 00	PUSH 0	
00401005	. 68 00204000	PUSH binary-l.00402000	[Style = MB_OK!MB_APPLMODAL Title = "ãNãëãbãNãQüCãÇüI"
0040100A	. 68 11204000	PUSH binary-l.00402011	Text = "ãcëç100000ë:üAOKãçã^ãõë=ëfëçë-ëçüI"
0040100F	. 6A 00	PUSH 0	hOwner = NULL
00401011	. E8 EA2F0000	CALL <JMP.&user32.MessageBoxA>	MessageBoxA
00401016	. 3E:C705 003041	MOV DWORD PTR DS:[403000],0	
00401021	> 3E:FF35 003041	PUSH DWORD PTR DS:[403000]	[<%d> = 0
00401028	. 68 34204000	PUSH binary-l.00402034	Format = "%zdë:ëfë ëçëëëçüI"
0040102D	. 68 04304000	PUSH binary-l.00403004	s = binary-l.00403004
00401032	. E8 CF2F0000	CALL <JMP.&user32.wsprintfA>	wsprintfA
00401037	. 6A 01	PUSH 1	[Style = MB_OKCANCEL!MB_APPLMODAL
00401039	. 68 00204000	PUSH binary-l.00402000	Title = "ãNãëãbãNãQüCãÇüI"
0040103E	. 68 04304000	PUSH binary-l.00403004	Text = ""
00401043	. 6A 00	PUSH 0	hOwner = NULL
00401045	. E8 B62F0000	CALL <JMP.&user32.MessageBoxA>	MessageBoxA
0040104A	. 83F8 02	CMP EAX,2	
0040104D	√74 63	JE SHORT binary-l.004010B2	
0040104F	. 3E:FF05 003041	INC DWORD PTR DS:[403000]	
00401056	. 3E:813D 003041	CMP DWORD PTR DS:[403000],186A0	
00401061	^7E BE	JLE SHORT binary-l.00401021	
00401063	. B9 00000000	MOV ECX,0	
00401068	> B8 FF000000	MOV EAX,0FF	
0040106D	. 3E:33048D 6921	XOR EAX,DWORD PTR DS:[ECX*4+402069]	
00401075	. 8981 84304000	MOV DWORD PTR DS:[ECX+403084],EAX	
0040107B	. 41	INC ECX	
0040107C	. 83F9 0B	CMP ECX,0B	
0040107F	^7E E7	JLE SHORT binary-l.00401068	
00401081	. C781 85304000	MOV DWORD PTR DS:[ECX+403085],0	
00401088	. 68 84304000	PUSH binary-l.00403084	
00401090	. 68 58204000	PUSH binary-l.00402058	[<%s> = ""
00401095	. 68 44304000	PUSH binary-l.00403044	Format = "The flag is (%s)"
0040109A	. E8 672F0000	CALL <JMP.&user32.wsprintfA>	s = binary-l.00403044
0040109F	. 6A 00	PUSH 0	wsprintfA
004010A1	. 68 47204000	PUSH binary-l.00402047	[Style = MB_OK!MB_APPLMODAL
004010A6	. 68 44304000	PUSH binary-l.00403044	Title = "Congratulations!"
004010AB	. 6A 00	PUSH 0	Text = ""
004010AD	. E8 4E2F0000	CALL <JMP.&user32.MessageBoxA>	hOwner = NULL
004010B2	> 6A 00	PUSH 0	MessageBoxA
004010B4	. E8 532F0000	CALL <JMP.&kernel32.ExitProcess>	ExitCode = 0
			ExitProcess

デバッガで開く

Example

バイナリ解析

DWORD PTR DS:[403000] と10万を比較している

0040104A	. 83F8 02	CMP EAX,2
0040104D	. 74 63	JE SHORT binary-L.004010B2
0040104F	. 3E:FF05 003040	INC DWORD PTR DS:[403000]
00401056	. 3E:813D 003040	CMP DWORD PTR DS:[403000],186A0
00401061	. 7F BF	JLE SHORT binary-L.00401021

DS:[00403000]=00000001



dword の 00403000 ...

16進

符号あり

符号なし

OK キャンセル

修正



dword の 00403000 ...

16進

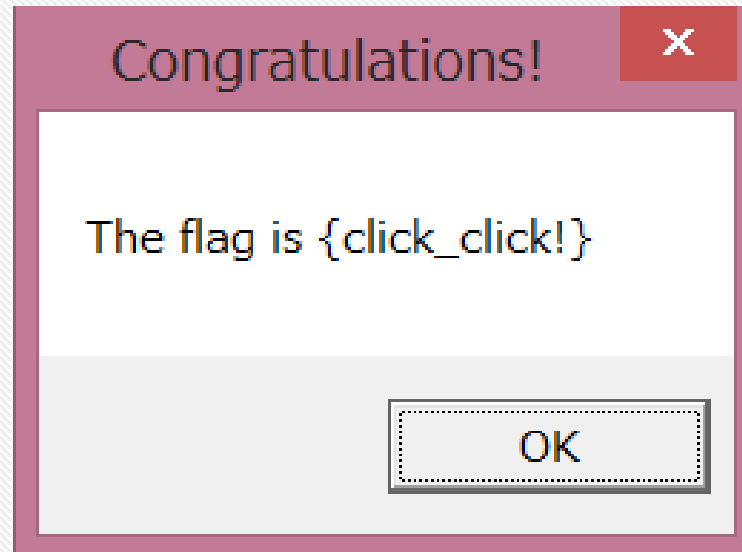
符号あり

符号なし

OK キャンセル

Example

バイナリ解析



Flag : “click_click!”

Statistics

■参加者が面白かったと感じた分野 [複数回答可・第一回]

順位	分野	回答数
1位	パケット解析	46
2位	フォレンジック	40
3位	バイナリ解析	33
4位	WEB	28
5位	暗号	22
6位	その他	1

■参加者コメント (一部抜粋)

今後情報セキュリティをどのように学べばよいか、方向性が見えました。

講師も参加者も全員女性だったので、相談も質問もしやすく、本当に楽しく過ごす事が出来ました。

同世代の女子大生のみなさんと、大学で学んでいることやエピソードを聞いたり、分からない問題を教えあったりする事が出来ました。

■ 参加者を運営側に勧誘する

- ➡ スキルアップの場・機会を提供
- ➡ コミュニティ拡大のサイクルを形成する

■ ハイレベルな女性人材の輩出

- ➡ ロールモデルとなるような女性を輩出
- ➡ (セキュリティ女子)という括りがなくなる位

第三回ワークショップを現在開催検討中！