

[Misc] fly

# 目次

- ・自己紹介
- ・問題概要
- ・問題解説
- ・まとめ

# 自己紹介

- ・kmrr
- ・にわかセキュリティエンジニア
- ・最近買ったもの: サメ映画大全



# 問題概要

SECCON for beginners 2021で出題されたMisc問題。

Miscとは、先ほども説明したが雑多なその他問題が出題される。

今回はwolf editorで作られたゲームをチートしてフラグを取得する問題。

以下のURLからファイルをDL

[https://github.com/satoki/ctf4b\\_2021\\_satoki\\_writeups/tree/main/misc/fly](https://github.com/satoki/ctf4b_2021_satoki_writeups/tree/main/misc/fly)

解凍とかは適宜やってくだしあ。

展開すると、Game.exeやら必要そうなファイルが現れる。

Game.exeを起動する。

←

→

⌵

⬆

⬅ << ctf4b\_2021\_satoki\_writeups-main > misc > fly > files > fly ⌵ ↺

🔍 flyの検索

名前

更新日時

種類

サイズ

📄

Config.exe

2021/08/05 10:21

アプリケーション

292 KB

📄

Data.wolf

2021/08/05 10:21

WOLF ファイル

7,245 KB

📄

Game.exe

2021/08/05 10:21

アプリケーション

6,668 KB

📄

Game.ini

2021/08/05 10:22

構成設定

1 KB

📄

GuruguruSMF4.dll

2021/08/05 10:21

アプリケーション拡張

144 KB



2、3マスしか動けないゲーム  
が起動する。



横にいるハニワに話しかけると煽られる。











横に階段がある。  
通常はいけませんがチートして  
階段を降りられないか試す。

## 問題解説

ゲームのチートと言ったらうさみみハリケーンが思いつくので、うさみみハリケーンを使って解いてみる。DLして、「UsaMimi64.exe」を起動する。


※うさみみハリケーンは、プロセスにアタッチしてメモリを参照したり書き換えたりできるツール

	UsaMimi.exe	2021/07/06 6:26	アプリケーション	1,152 KB
	UsaMimi32.exe	2021/07/06 7:50	アプリケーション	2,775 KB
	UsaMimi64.exe	2021/07/06 8:00	アプリケーション	3,563 KB
	UsaSpeed.dll	2011/07/06 15:52	アプリケーション拡張	64 KB
	UsaSpeed32.dll	2019/11/01 10:48	アプリケーション拡張	66 KB
	UsaSpeed64.dll	2015/07/02 16:14	アプリケーション拡張	70 KB












注意点として、必ず「UsaMimi64.exe」を起動してください。

この後利用する簡易数値検索機能は「UsaMimi64.exe」にしか実装されておきませんので、この後の手順が追えなくなります。

Game.exeを選択して、「選択」を押下する。

 プロセスを選択してください - 非管理者権限での起動により一部のプロセスが列挙できません

リスト更新
リスト更新(PID総当り)
実行ファイルを起動
**選択**
キャンセル

プロセス名	Bit	PID(Hex/Dec)	ユーザー	優先度	モジュールパス
 Game.exe	32	0000F57C(62844)	developer@DESKTOP-UVK5KUL	通常	C:\Users\developer\Down
 svchost.exe	64	000091B4(37300)	developer@DESKTOP-UVK5KUL	通常	C:\WINDOWS\system32\svch
 chrome.exe	64	0001B974(113...	developer@DESKTOP-UVK5KUL	通常	C:\Program Files (x86)\C
 chrome.exe	64	0000941C(37916)	developer@DESKTOP-UVK5KUL	低	C:\Program Files (x86)\C
 chrome.exe	64	00017AAC(96940)	developer@DESKTOP-UVK5KUL	通常	C:\Program Files (x86)\C
 chrome.exe	64	0000F248(62024)	developer@DESKTOP-UVK5KUL	低	C:\Program Files (x86)\C
 chrome.exe	64	00005878(22648)	developer@DESKTOP-UVK5KUL	通常	C:\Program Files (x86)\C
 chrome.exe	64	00010360(66400)	developer@DESKTOP-UVK5KUL	通常	C:\Program Files (x86)\C
 chrome.exe	64	000125B8(75192)	developer@DESKTOP-UVK5KUL	通常	C:\Program Files (x86)\C
 chrome.exe	64	00012D5C(77148)	developer@DESKTOP-UVK5KUL	通常	C:\Program Files (x86)\C
 chrome.exe	64	00007CBC(31932)	developer@DESKTOP-UVK5KUL	通常	C:\Program Files (x86)\C

うさみハリケン 32Bit 新型改良版 - [Game.exe (PID: 0000F57C/62844)]

プロセス(P) 移動(M) 編集(E) 検索(S) デバッグ(D) プラグイン(X) 表示(V) ウィンドウ(W) その他(A) ヘルプ(H)



Address	:	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	
00400E20	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0123456789ABCDEF
00400E30	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400E40	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400E50	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400E60	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400E70	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400E80	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400E90	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400EA0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400EB0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400EC0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400ED0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400EE0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400EF0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F00	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F10	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F20	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F30	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F40	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F50	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F60	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F70	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F80	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400F90	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400FA0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400FB0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400FC0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400FD0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400FE0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00400FF0	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00401000	:	55	8B	FC	6A	FF	68	FB	A3	7D	00	64	A1	00	00	00	00	リソースファイル...

メモリエディタが起動される。





操作できるキャラクターを柵の外に出せないかを試す。

キャラクターは横に移動できるので、X軸方向の増減を検索し、チートできないかを調べる。





簡易数値検索 (空き物理メモリが少ない状況では使用しないでください)

縮小表示

☐ 最前面表示

検索結果(最大記録件数は空き)

1. 検索する数値の形式とオプションを選択:

整数: ☒ Byte ☒ Word ☒ DWord ☒ QWord ☐ 符号付き

浮動小数点数: ☒ float ☒ double ☒ ±1範囲で検索

2. 検索対象領域と比較方法の設定:

領域の属性: 読/書/実行 MAPPED以外

アドレス範囲: 00010000 7FFFFFFF

比較方法: 入力値と同じ

3. 検索する数値を半

※整数は先頭0x

※整数は先頭0+

①

- 入力値と同じ
- 入力値以上
- 入力値以下
- 入力値とは異なる
- 2つの入力値の間
- 現在値は不明な値 (符号なし)
- 現在値は不明な値 (符号付き)

初回検索(2回目以降は絞り込み検索)

②

4. 検索結果の操作と表示の設定:

アドレス



問題解説

x軸が減少したと推定

## 2. 検索対象領域と比較方法の設定:

領域の属性: 読/書/実行    MAPPED以外

アドレス範囲: 00010000    7FFEFFFF

比較方法 ① 減少した

## 3. 検索する数値を半角の10進数か16進数で入力して検索実行:

※整数は先頭「0x」または値にabcdefABCDEFありで16進数扱い

※整数は先頭に+か-で符号付き整数扱い

絞り込み検索

②

## 4. 検索結果の操作と表示の設定:



x軸が増加したと推定

## 2. 検索対象領域と比較方法の設定:

領域の属性:	読/書/実行	MAPPED以外
アドレス範囲:	00010000	7FFEFFFF
比較方法	① 増加した	

## 3. 検索する数値を半角の10進数か16進数で入力して検索実行:

※整数は先頭「0x」または値にabcdefABCDEFありで16進数扱い

※整数は先頭に+か-で符号付き整数扱い

絞り込み検索	

②

検索結果(最大記録件数は空きメモリに依存):

34

連続検索回数:

8

問題解説

アドレス	数値形式	今回検索	前回検索
0019B668	Byte	64	72
0019B668	Word	64	72
0019B668	DWord	64	72
0019B668	QWord	68719476800	68719476808
0019B668	float	8.9683102e-044	1.0089349e-043
0019B668	double	3.395193268706455...	3.395193269101708...
00A861B8	Byte	27	28
00A861B8	Word	27	28
00A861B8	DWord	27	28
00A861B8	QWord	103079215131	103079215132
00A861B8	float	3.7835059e-044	3.9236357e-044
00A861B8	double	5.0927898998650630...	5.092789899700037...
00A861C8	Word	864	896
00A861C8	DWord	864	896
00A861C8	QWord	3298534884192	3298534884224
00A861C8	float	1.2107219e-042	1.2555634e-042
00A861C8	double	1.629692767888201...	1.629692767904012...
00A8A098	QWord	1099511627776	1236950581248
00A8A098	double	5.432309224871097...	6.111347877979984...
00A8A09C	Byte	0	32
00A8A09C	Word	256	288
00A8A09C	DWord	256	288
00A8A09C	float	3.5873241e-043	4.0357396e-043
02E2BC10	Byte	27	28
02E2BC10	Word	27	28
02E2BC10	DWord	27	28
02E2BC10	QWord	103079215131	103079215132
02E2BC10	float	3.7835059e-044	3.9236357e-044
02E2BC10	double	5.0927898998650630...	5.092789899700037...
02E2BC20	Word	864	896
02E2BC20	DWord	864	896

最終的に34件くらいに絞られる。  
赤枠がキャラクターのx軸と推測できる



The screenshot shows the WinDBG memory dump window. The address 0019B6D0 is selected, and the context menu is open. The option '選択アドレスへの直接書き込み・選択範囲の一括書き換え(I)... (中クリック)' is highlighted with a red rectangle.

ddress	:	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
0A861B0	:	2F	00	00	00	FE	FF	FF	FF	1E	00	00	00	18	00	00	00	/.....
0A861C0	:	CC	CC	CC	CC	CC	CC	CC	CC	00	03	00	00	00	03	00	00	????????タ.....

選択アドレスへの直接書き込み・選択範囲の一括書き換え

書き込み範囲/書き込みデータ/オプション指定

書き込み範囲アドレス

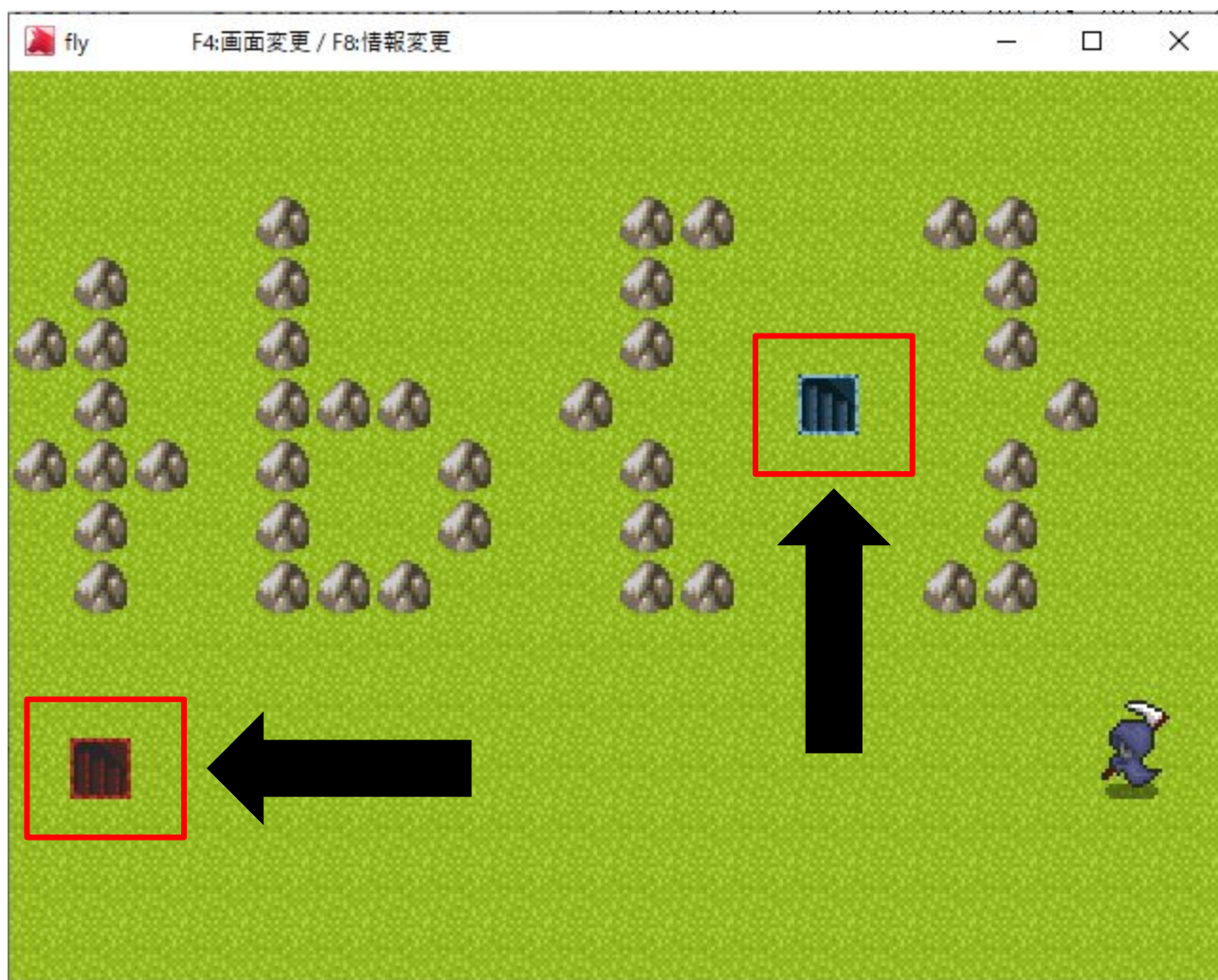
開始:  終端:  ☒ 範囲終端を入力データで決定

書き込むデータを入力

書き込み

キャンセル





問題解説



fly

F4:画面変更 / F8:情報変更



問題解説



R. I. P. Flag



問題解説

青い階段には入れない。。。

## ここで

wolf editorでは、階段を触ってマップを移動する、という流れを作る際以下のように作りこむ。

1. 階段の先を表示する際には、マップファイルを用意する
2. プレイヤーが階段に触れると、用意されたマップファイルに移動するようイベントを設定する

青い階段の先にマップが準備されている場合、そこにフラグが隠されていると推測できる。

しかし青い階段にはマップ遷移イベントがないため、赤い階段の遷移先を青い階段のマップに改ざんできないか考えてみる。

メモリ検索により、マップファイル名である「mps」を検索するため、参照先を一番上に変更する。

うさみみハリケーン 32Bit 新型改良版 - [Game.exe (PID: 0000F57C/62844)]

① 移動(M) 編集(E) 検索(S) デバッグ(D) プラグイン(X) 表示(V) ウィンドウ(W) その他(A) ヘルプ(H)

表示アドレスを16進数で指定

縮小表示

02E52508

アドレス変更

キャンセル

メモリアリアマップ・モジュールリスト/PEヘッダ情報/セクションリスト

マップ更新

エリアダンプ

前のモジュール

次のモジュール

☒ PEヘッダ/セクション情報を表示

アドレス	属性	サイズ	モジュール/情報	バー
00400000	-R--	00001000	Game.exe	ver2
00401000	ER--	003E5000	Game.exe	
007E6000	-R--	0009C000	Game.exe	
00882000	-RW-	00002000	Game.exe	
00884000	---C	00014000	Game.exe	
00898000	-RW-	00001000	Game.exe	
00899000	---C	00001000	Game.exe	
0089A000	-RW-	0000A000	Game.exe	
008A4000	---C	00002000	Game.exe	

[モジュール先頭アドレス]  
左クリック:  
該当モジュール情報を表示  
右クリック:  
ポップアップメニューを表示

②

wolfeditorのマップ情報の拡張子は「.mps」っぽいことが公式ドキュメントからわかる

マップの新規作成

マップの保存フォルダとファイル名を入力してください

MapData / .mps

マップサイズ

横 20 縦 15

タイルセット

0: 街・ダンジョン

登録先(システムDBタイプ0) ☒ 登録する

登録先 04: マップのループ設定

登録名 <マップ名を入力> ループ無し

再生するBGM ☐ 使用する ☐ 前MAPのまま

ファイル File ☒ ファイル名指定

音量[%] 100 周波数[%] 100 ループ位置[ms] 0

再生するBGS ☐ 使用する ☐ 前MAPのまま

ファイル File ☒ ファイル名指定

#### 【マップの保存フォルダとファイル名】

保存したいフォルダを左のプルダウンメニューから選び、保存したいファイル名を右の文字入力欄に入力します。

#### 【マップサイズ】

マップの大きさを指定します。単位はチップ数です。

#### 【タイルセット】

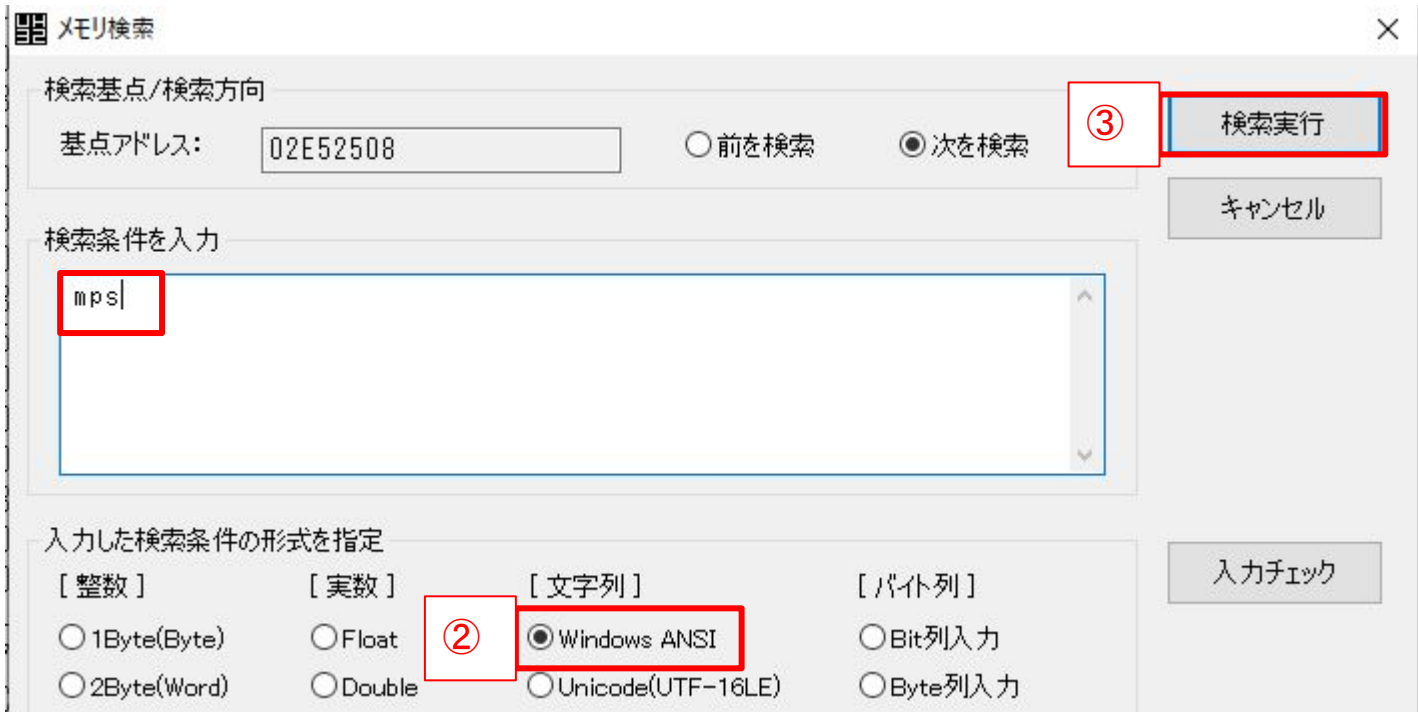
マップの描画に使用するタイルセットを選択します。

#### 【登録先】

マップファイル(.mpsファイル)は通常、システムDBタイプ0番のデータベースにファイル名を書き込まないとゲームで使うことができません。しかし、ここで登録先を指定することで、簡単にシステムDBタイプ0番にそれらを書き込むことができます。

デフォルトで「登録する」のチェックが押されているので、あとは「登録先」を選択し、登録名、ループ設定、BGM、BGS、遠景設定を指定してください。

なお、この「登録名」はゲーム的には意味はありません、あなたがエディットする際に区別するための名前ですので、自由に設定してください。





うさみみハリケーン 32Bit 新型改良版 - [Game.exe (PID: 0000F57C/62844)]

プロセス(P) 移動(M) 編集(E) 検索(S) デバッグ(D) プラグイン(X) 表示(V) ウィンドウ(W) その他(A) ヘルプ(H)

Address	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	
0123456789ABCDEF																	
02E52500	4D	61	70	44	61	74	61	2F	66	6C	61	67	31	2E	3D	70	MapData/flag1.mps
02E52510	73	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	s.....
02E52520	13	B3	F0	04	00	2B	00	88	31	30	30	25	5B	91	95	94	ワ...+.100%[装備
02E52530	F5	82	C8	82	E7	81	7D	30	25	5D	00	00	00	00	00	00	なら±0%].....
02E52540	0F	00	00	00	00	00	00	00	1E	B3	CF	04	00	2C	00	88	.....ウマ.....
02E52550	38	30	25	5B	91	95	94	F5	82	C8	82	E7	2D	32	30	25	80%[装備なら-20%
02E52560	5D	00	6D	69	64	00	64	00	00	00	00	00	00	00	00	00	]mid.d.....
02E52570	1	うさみみハリケーン 32Bit 新型改良版 - [Game.exe (PID: 0000F57C/62844)]															
02E52580	8	プロセス(P) 移動(M) 編集(E) 検索(S) デバッグ(D) プラグイン(X) 表示(V) ウィンドウ(W) その他(A) ヘルプ(H)															
02E52590	6																

マップデータにはflag1.mps、flag2.mpsが確認できる。

Address	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	
0123456789ABCDEF																	
02E526E0	4D	61	70	44	61	74	61	2F	66	6C	61	67	32	2E	3D	70	MapData/flag2.mps
02E526F0	73	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	s.....
02E52700	57	B3	34	05	00	37	00	88	00	00	00	00	00	00	00	00	ワ4../.....
02E52710	00	00	00	00	00	00	00	00	00	00	00	00	18	26	E5	02	.....&..
02E52720	12	52	B3	33	05	00	38	00	88	4&..4&..R03..8..	MapData/ctf4b.mps						
02E52730	4D	61	70	44	61	74	61	2F	66	6C	61	67	32	2E	3D	70	s.....
02E52740	73	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	]ワ...9..90%[装備
02E52750	5D	B3	0E	05	00	39	00	88	39	30	25	5B	91	95	94	F5	なら-10%].....
02E52760	82	C8	82	E7	2D	31	30	25	5D	00	00	00	00	00	00	00	.....
02E52770	0F	00	00	00	00	00	00	00	5B	B3	05	05	00	2A	00	88	.....



UH うさみみハリケーン 32Bit 新型改良版 - [Game.exe (PID: 0000F57C/62844)]

プロセス(P) 移動(M) 編集(E) 検索(S) デバッグ(D) プラグイン(X) 表示(V) ウィンドウ(W) その他(A) ヘルプ(H)

Address	:	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
02E52730	:	4D	61	70	44	61	74	61	2F	63	74	66	34	62	2E	6D	70	MapData/ctf4b.mp
02E52740	:	73	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	s.....
02E52750	:	5D	B3	0E	05	00	39	00	88	39	30	25	5B	91	95	94	F5	]ウ...9. 90%[装備
02E52760	:	82	C8	82	E7	2D	31	30	25	5D	00	00	00	00	00	00	00	なら-10%].....
02E52770	:	0F	00	00	00	00	00	00	00	58	B3	05	05	00	3A	00	88	.....Xウ.....
02E52780	:	34	30	25	5B	91	95	94	F5	82	C8	82	E7	2D	36	30	25	40%[装備なら-60%
02E52790	:	5D	00	00	00	00	00	00	00	0F	00	00	00	00	00	00	00	].....
02E527A0	:	43	B3	00	05	00	3B	00	88	35	25	5B	91	95	94	F5	82	ウ...; 5%[装備な
02E527B0	:	C8	82	E7	2D	39	35	25	5D	00	DB	00	00	00	00	00	00	なら-95%].ロ.....
02E527C0	:	0F	00	00	00	00	00	00	00	4E	B3	1F	05	00	3C	00	88	.....Nウ...<..

マップデータには ctf4b.mps が確認できる。

ctf4b.mpsはわからないが、flag1.mpsとflag2.mpsが怪しい。

したがって、以下のどちらかを試してみる。

1.flag1.mpsをflag2.mpsにすべて変更する

2.flag2.mpsをflag1.mpsにすべて変更する

→ まずは1.を試してみる。

UH うさみハリケーン 32Bit 新型改良版 - [Game.exe (PID: 00004644/17988)]

プロセス(P) 移動(M) 編集(E) 検索(S) デバッグ(D) プラグイン(X) 表示(V) ウィンドウ(W) その他(A) ヘルプ(H)

Address	:	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
02E12190	:	4D	61	70	44	61	74	61	2F	66	6C	61	67	31	2F	6D	70	MapData/flag1.mn
02E121A0	:	73	00	00	00	00	00	00	00	0F	00	00	00					
02E121B0	:	B0	62	8D	68	00	15	00	88	88	EA	90	D8					
02E121C0	:	82	C8	82	A2	5B	2D	31	30	30	25	5D	00					
02E121D0	:	0F	00	00	00	00	00	00	00	BD	62	96	68					
02E121E0	:	31	30	30	25	5B	91	95	94	F5	82	C8	82					
02E121F0	:	30	25	5D	00	00	00	00	00	0F	00	00	00					
02E12200	:	C6	62	9B	68	00	17	00	88	33	30	25	5B					
02E12210	:	82	C8	82	E7	2D	37	30	25	5D	00	00	00					
02E12220	:	0F	00	00	00	00	00	00	00	C3	62	9C	68					

選択範囲を記録バッファとクリップボードにコピー(C) Ctrl+C

貼り付け(P) Ctrl+V

選択範囲内に貼り付け(R) Shift+V

自動貼り付け(A)

自動貼り付け処理を停止(D) V

選択アドレスへの直接書き込み・選択範囲の一括書き換え(I)... (中クリック)

10/16進数表形式入出力(J)... J

選択範囲への演算実行(L)... Ctrl+L

選択アドレスへの直接書き込み・選択範囲の一括書き換え

書き込み範囲/書き込みデータ/オプション指定

書き込み範囲アドレス

開始: 02E12198 終端: 02E1219C ☒ 範囲終端を入力データで決定

書き込むデータを入力

flag2

書き込むモードを指定

[ 整数 ]	[ 実数 ]	[ 文字列 ]	[ バイト列 ]
<input type="radio"/> 1Byte(Byte)	<input type="radio"/> Float	<input checked="" type="radio"/> Windows ANSI	<input type="radio"/> Bit列入力
<input type="radio"/> 2Byte(Word)	<input type="radio"/> Double	<input type="radio"/> Unicode(UTF-16LE)	<input type="radio"/> Byte列入力

①

書き込み

キャンセル

入力チェック

Address	:	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
02E12190	:	4D	61	70	44	61	74	61	2F	66	6C	61	67	32	2E	6D	70	MapData/flag2.mp
02E121A0	:	73	00	00	00	00	00	00	00	0F	00	00	00	00	00	00	00	s.....
02E121B0	:	B0	62	8D	68	00	15	00	88	88	EA	90	D8	8C	F8	82	A9	-b紘...・黚リ効か
02E121C0	:	82	C8	82	A2	5B	2D	31	30	30	25	5D	00	00	00	00	00	ない[-100%].....
02E121D0	:	0F	00	00	00	00	00	00	00	BD	62	96	68	00	16	00	88	.....sb防...・
02E121E0	:	31	30	30	25	5B	91	95	94	F5	82	C8	82	E7	2B	31	30	100%[装備なら+10
02E121F0	:	30	25	5D	00	00	00	00	00	0F	00	00	00	00	00	00	00	n%1

検索 → 「flag1」を「flag2」に置換を繰り返す

Address	:	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
0D1CB7B0	:	4D	61	70	44	61	74	61	2F	66	6C	61	67	32	2E	6D	70	MapData/flag2.mp
0D1CB7C0	:	73	00	32	5F	70	69	70	6F	2E	70	6E	67	00	6E	67	00	s.2_pipo.png.ng.
0D1CB7D0	:	7C	D0	03	6C	00	00	01	88	4D	61	70	43	68	69	70	2F	.T...apChip/
0D1CB7E0	:	5B	41	5D	49	63	65	32	5F	70	69	70	6F	2E	70	6E	67	[A]Ice2_pipo.png
0D1CB7F0	:	00	67	00	70	6E	67	00	00	79	D0	3E	6C	00	01	01	80	.g.png..y>l...
0D1CB800	:	4D	61	70	43	68	69	70	2F	5B	41	5D	53	6E	6F	77	5F	MapChip/[A]Snow
0D1CB810	:	44	69	72	74	32	5F	70	69	70	6F	2E	70	6E	67	00	00	Dirt2_pipo.png..
0D1CB820	:	82	D1	35	6C	00	02	01	80	4D	61	70	43	68	69	70	2F	び5l... MapChip/
0D1CB830	:	5B	41	5D	57	61	6C	6C	2D	55	70	32	5F	70	69	70	6F	[A]Wall-Up2_pipo
0D1CB840	:	2E	70	6E	67	00	6E	67	00	8F	D1	30	6C	00	03	01	80	.png.ng.肖0T...
0D1CB850	:	4D	61	70	43	68	69	70	2F	5B	41	5D	57	61	74	65	72	MapChip/[A]Water

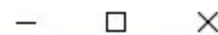




flag2にすべて置換した状態で  
階段に入る



F4:画面変更 / F8:情報変更



問題解説







# まとめ

- ・SECCON for beginners2021のMisc問題を見てきた。
- ・うさみみハリケーンを利用しメモリ改ざんを用いた解法を説明しました。
- ・これ以外の方法で解くこともできるそうなので、興味があれば試してみてください。
- ・個人的には、意外とメモリに情報が残っており、それを使ってチートができることがわかり面白い問題と感じました。