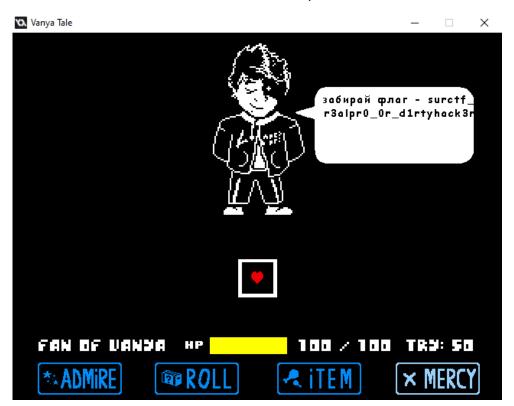
1. Vanyatale

Для получения флага нужно пройти игру до конца (довести «хп» Вани до минимума).

Круто, если сделать все это на скиле, но никто и не запрещал накрутить себе, к примеру, XП через тот же Cheat Engine или уменьшить XП босса.

В конечном диалоги Ваня сообщит флаг.



2. Vanyatale_y3t_dark3r

Флаг находится в главном меню. Для того, чтобы его увидеть, необходимо осветлить изображение. Ну или просто тыкнуть пипеткой в Paint по черному фону: D.





surctf_vanja_m39a_h1dd3n_flag

3. Vanyatale_hidden_snd

Заходим в SoundTest, листаем до 13 записи «Т3L3PH0N3_CA77», содержащую DTMF запись - звуки клавиш кнопочных телефонов, где каждая клавиша имеет свое уникальное звучание.

Записываем это аудио любым способом и декодируем DTMF декодером. На месте пауз между звуками расставляем _, а также не забываем дописать перед полученной последовательностью цифр surctf_.



surctf_777_169_609_01_111

4. Vanyatale_cursed_image

Играя в игру, можно встретить следующее сообщение:



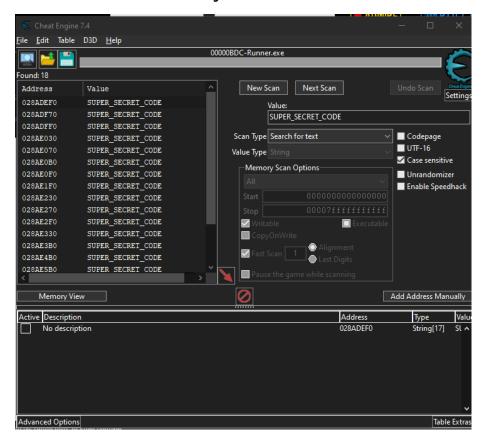
Первая его часть зашифрована шифром Цезаря (ROT24), расшифровав получим:

Don't even look for the ЫГЗУК_ЫУСКУЕ_СЩВУ!

Последние 3 слова написаны русской раскладкой, нужно восстановить английские буквы, в итоге получится:

Don't even look for the SUPER SECRET CODE!

Открываем **CheatEngine**, ставим режим поиска String и вставляем в поле наше полученное значение.



Выбираем любой из найденных адресов и жмем *Browse This Memory Region*. Видим последовательность значений в шестнадцатеричном формате.

05 0A 12 12 0F 18

Protect:	Read	d/W:	rit	e 1	A110	ocat	io	ıBa:	se=(0282	000A	00 1	Base	==02	28AI	D00	0 Size=2000
address	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	FA	FB	FC	FD	FE	FF	0123456789ABCDEF
028ADEF0	53	55	50	45	52	5F	53	45	43	52	45	54	5F	43	4F	44	SUPER SECRET COD
028ADF00	45	21	21	21	20	30	35	20	30	41	20	31	32	20	31	32	E!!! 05 0A 12 12
028ADF10	20	30	46	20	31	38	00	00	24	94	2F	F7	C0	03	00	88	OF 18\$ /
028ADF20	28	00	00	00	DE	C0	AD	DE	0B	во	AD	BA	00	00	00	00	(
028ADF30	E0	E8	AF	02	48	E5	AF	02	40	E8	AF	02	30	E9	AF	02	.н . <mark>0 .0 .</mark>
028ADF40	98	E5	AF	02	00	E7	AF	02	C0	E5	AF	02	B0	E6	AF	02	
028ADF50	C8	E7	AF	02	D8	E6	AF	02	2C	94	17	F7	30	04	00	80	, . 0
028ADF60	27	00	00	00	DE	C0	AD	DE	0B	В0	AD	BA	00	00	00	00	****
028ADF70	53	55	50	45	52	5F	53	45	43	52	45	54	5F	43	4F	44	SUPER_SECRET_COD
028ADF80	45	21	21	21	20	30	35	20	30	41	20	31	32	20	31	32	E!!! 05 0A 12 12
028ADF90	20	30	46	20	31	38	00	00	34	94	1F	F7	90	05	00	8C	OF 18 <mark>4</mark>
028ADFA0	24	00	00	00	DE	C0	AD	DE	0B	B0	AD	BA	00	00	00	00	\$
																	0 . 2 . (0 .pz .
028ADFC0																	
028ADFD0	00	00	00	00	E0	C9	8A	02	3C	94	07	F7	E0	06	00	80	···· · <mark>< · ··</mark>
028ADFE0																	
																	SUPER_SECRET_COD
																	E!!! 05 0A 12 12
																	OF 18
028AE020																	
																	SUPER_SECRET_COD
																	E!!! 05 0A 12 12
																	0F 18 w
028AE060	27	00	00	00	DE	CO	AD	DE	0B	В0	AD	BA	00	00	00	00	· · · · · · · · · · · · · · · · · · ·
				4-				<u> </u>						-40			- AN ABA - ABABAM - AAB

Для получения изображения с флагом нужно по порядку проиграть песни в SoundTeste с кодами из полученной последовательности.



(Отсылка на https://youtu.be/idheGtky7os)

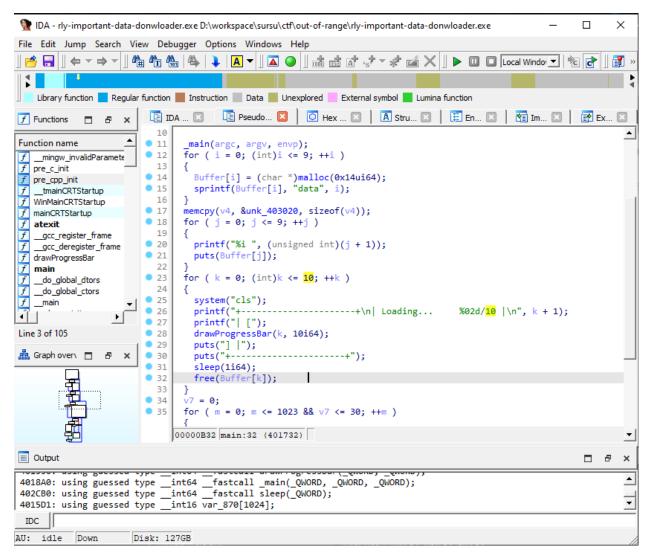
5. loading

Как можно догадаться, программа падает из-за выхода за пределы массива. Если это не очевидно, подсказка есть в одном из диалогов Vanyatale))

```
* Loading Dialogue... ERR!!

Index out of range!
```

Открываем любую тулзу по декомпиляции. К примеру IDA. Находим там косячный цикл:



Узнаем примерный адрес неправильного значения в экзешнике – 0xB3E:

Идем в любой удобный редактор, к примеру HxD, находим там требуемое значение и меняем его с 0x0A (10) на 0x09 (9):

```
Offset(h) 00 01 02 03 04 05 06 07 08 09
Il rly-important-data-donwloader.exe
                                                                00000A80 E8 8B 16 00 00 8B 85 08 08 00
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Декодр ^
                                                                00000A90 C5 A0 07 00 00 48 89 C1 E8 63
00000A80 E8 8B 16 00 00 8B 85 08 08 00 00 48 98 48 8B 84
                                                                00000AA0 08 00 00 01 83 BD 08 08 00 00
00000A90 C5 A0 07 00 00 48 89 C1 E8 63 16 00 00 83 85 08
                                                      E ....F
                                                                000000AB0 08 00 00 00 00 00 00 E9 82 00
00000AA0 08 00 00 01 83 BD 08 08 00 00 09 7E C1 C7 85 04
                                                                00000AC0 29 00 00 E8 10 16 00 00 8B 85
00000AB0 08 00 00 00 00 00 E9 82 00 00 00 48 8D 0D 46
                                                                00000AD0 01 89 C2 48 8D 0D 36 29 00 00
00000AC0 29 00 00 E8 10 16 00 00 8B 85 04 08 00 00 83 C0
                                                                00000AE0 8D 0D 5F 29 00 00 E8 25 16 00
                                                       .%BHŔ.
00000AF0 00 BA 0A 00 00 00 89 C1 E8 53
00000AE0 8D 0D 5F 29 00 00 E8 25 16 00 00 8B 85 04 08 00
                                                       Ŕ._)..
                                                                00000B00 45 29 00 00 E8 F7 15 00 00 48
00000AF0 00 BA 0A 00 00 00 89 C1 E8 53 FE FF FF 48 8D 0D
                                                       .∈....
                                                                00000B10 E8 EB 15 00 00 B9 01 00 00 00
00000B00 45 29 00 00 E8 F7 15 00 00 48 8D 0D 3D 29 00 00
                                                       E)..ич
                                                      ил...В
                                                                00000B20 85 04 08 00 00 48 98 48 8B 84
00000B20 85 04 08 00 00 48 98 48 8B 84 C5 A0 07 00 00 48
                                                                00000B30 89 C1 E8 F9 15 00 00 83 85 04
00000B30 89 C1 E8 F9 15 00 00 83 85 04 08 00 00 01 83 BD
                                                                00000B40 04 08 00 00 09 0F 8E 71 FF FF
00000B40 04 08 00 00 PA OF 8E 71 FF FF FF C7 85 00 08 00
                                                                00000B50 00 00 00 00 07 85 FC 07 00
00000B50 00 00 00 00 00 C7 85 FC 07 00 00 00 00 00 EB
                                                                00000B60 57 83 BD 00 08 00 00 1E 7F 50
00000B60 57 83 BD 00 08 00 00 1E 7F 5C 8B 8D FC 07 00 00 Wfs...
                                                                00000B70 BA 67 66 66 66 89 C8 F7 EA DI
00000B70 BA 67 66 66 66 89 C8 F7 EA D1 FA 89 C8 C1 F8 1F
                                                      eafff%
                                                                00000B80 29 C2 89 D0 89 C2 C1 E2 02 01
00000B80 29 C2 89 D0 89 C2 C1 E2 02 01 C2 89 C8 29 D0 85 )BhPhi
                                                                00000B90 C0 75 1E 8B 85 FC 07 00 00 48
         CO 75 1E 8B 85 FC 07 00 00 48 98 0F B7 44 45 A0 Au.<.....
```

Сохраняем, запускаем программу и получаем флаг:

```
■ D:\workspace\sursu\ctf\out-of-range\rly-important-data-or-

| Loading... 10/10 |

| [###############] |

+-----+
Surctf_b3s1_r8verse_ta3k_e2v2r
Для продолжения нажмите любую клавишу . .
```



by GalaxyShad 2022

telegram: @galaxyshad

github: https://github.com/GalaxyShad

vk: https://vk.com/galaxyshad

youtube: https://www.youtube.com/aGalaxyShad102