



Название:	Кажется, я в мире Voxel Game
Категория:	Реверс-инжиниринг
Уровень:	Лёгкий
Очки:	350
Описание:	Ваша цель - найти флаг в этой игре
Теги:	Godot, побайтовое шифрование
Автор:	ROP

#### Прохождение:

Запустим файл.

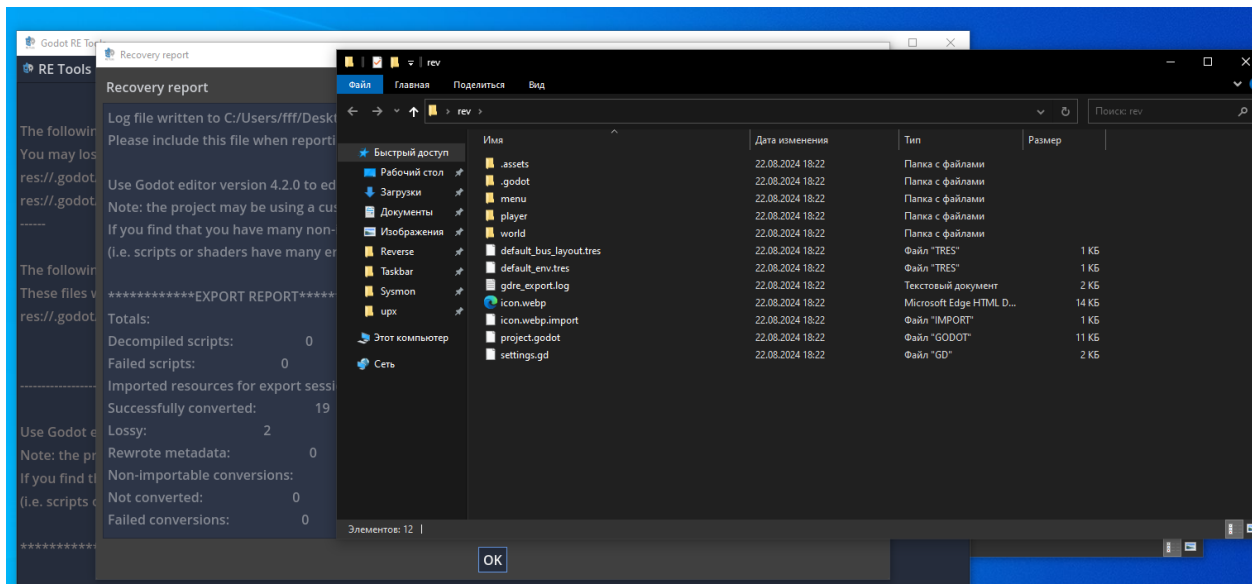




Это копия Minecraft. Перед его запуском на короткое время можно увидеть название движка - Godot. Гуглим и узнаём, что есть декомпилятор для игр на нём.

<https://github.com/bruvzg/gdsdecomp>

Экспортируем и получаем код.



По пути меню\main есть файл main\_menu.gd. В нём:

```
extends Control

@onready var tree = get_tree()

@onready var title = $TitleScreen
@onready var start = $StartGame
@onready var options = $Options
@onready var is_exist = 1

func _on_Start_pressed():
    start.visible = true
    title.visible = false

func _on_Options_pressed():
    options.prev_menu = title
    options.visible = true
    title.visible = false

func _on_Exit_pressed():
    tree.quit()

func _on_RandomBlocks_pressed():
    Settings.world_type = 0
    tree.change_scene_to_packed(preload("res://world/world.tscn"))
```

```

func _on_FlatGrass_pressed():
    Settings.world_type = 1

    var array = [
        0x88, 0x94, 0x89 , 0x8a, 0x87, 0x9e, 0xc0, 0xab, 0xb1, 0x85,
        0xac, 0xa4, 0x76, 0xb3, 0xa4, 0xb9, 0xad, 0x8a, 0xa4, 0xac,
        0x75, 0xa9, 0x94, 0xb9, 0xa4, 0x8c, 0x85, 0xb2, 0xaa, 0xc2
    ]

    for element in array:
        element = element - 0x45

    for element in array:
        element = element + 0x45

    is_exist = array[5]

    tree.change_scene_to_packed(preload("res://world/world.tscn"))

func _on_BackToTitle_pressed():
    title.visible = true
    start.visible = false

```

Подозрительный код:

```

var array = [
    0x88, 0x94, 0x89 , 0x8a, 0x87, 0x9e, 0xc0, 0xab, 0xb1, 0x85,
    0xac, 0xa4, 0x76, 0xb3, 0xa4, 0xb9, 0xad, 0x8a, 0xa4, 0xac,
    0x75, 0xa9, 0x94, 0xb9, 0xa4, 0x8c, 0x85, 0xb2, 0xaa, 0xc2
]

for element in array:
    element = element - 0x45

for element in array:
    element = element + 0x45

is_exist = array[5]

```

На самом деле он дешифрует и шифрует опять флаг. Если мы просто дешифруем флаг, то узнаем его.

[https://cyberchef.org/#recipe=From\\_Hex\('Auto'\)SUB\({'option':'Hex','string':'45'}\)&input=MHg40CwgMf](https://cyberchef.org/#recipe=From_Hex('Auto')SUB({'option':'Hex','string':'45'})&input=MHg40CwgMf)