



# Seraph Security Analysis

2023.11.24

Senna

DAMOCLES LABS

# Contents

- **Summary(Game Security Ratings)**
- **Game Background**
  - ◆ **Game Version**
  - ◆ **Genres & Engine**
  - ◆ **Possible Issues In GamePlay**
- **Game Security Analysis**
  - ◆ **Game Code Protection**
  - ◆ **Game Basic Anti-Cheat**
  - ◆ **Game Logic Issues**
  - ◆ **Game Protocol Analysis**
- **Web3 Security Analysis**
  - ◆ **Token Contract Security Analysis**
  - ◆ **Game Economy System Security Analysis**
- **About Damocles**

## 一、 Summary

Seraph opened its third beta test on November 22, 2023. On November 24, the Damocles team conducted a security analysis and assessment of the game. However, the assessment results were not satisfactory. Firstly, the project contained a significant amount of logging information in the code, which allowed the inference that the project team was not from Korea but from China. Additionally, the game adopted the Unity engine to load Lua scripts without any protection measures or the use of techniques like Lua JIT to enhance reverse engineering difficulty and protect the source code. This resulted in the complete exposure of the source code, as it could be dumped from memory by simply hooking the load function. However, since the game belongs to the ARPG genre, it has a natural advantage against cheating. Most of the game data is synchronized through the server, which mitigates the security issues to some extent.

Security Rating:



## 二、 Game Background

- Game Version: v0.0.0.6
- Genres & Engine: ARPG, Unity
- Possible Issues in Gameplay:
  - Teleportation
  - Accelerated (Accelerated Movement, Accelerated Skill Usage)












- Auto-Grinding
- Multiplier Modification
- Invincibility
- Buff Modification (Buff Modification to Increase Soul Crystal Output or Other Benefits)

### 三、 Game Security Analysis

#### Game Code Protection:

##### Analysis Process:

1. Since different engines have different analysis modes, it is important to determine the game engine used after obtaining the game EXE. By analyzing the basic information of the game, we can determine that this game was developed using Unity.

 out	2023/11/29 16:22	文件夹	
 out - 副本	2023/11/29 12:30	文件夹	
 SeraphGamma_Data	2023/11/21 23:52	文件夹	
 baselib.dll	2023/11/21 22:51	应用程序扩展	410 KB
 GameAssembly.dll	2023/11/21 22:52	应用程序扩展	45,209 KB
 out.zip	2023/11/25 18:26	WinRAR ZIP 压缩...	955 KB
 SeraphGamma.exe	2023/11/21 22:51	应用程序	651 KB
 UnityCrashHandler64.exe	2023/11/21 22:51	应用程序	1,089 KB
 UnityPlayer.dll	2023/11/21 22:51	应用程序扩展	29,905 KB

2. By examining the GameAssembly.dll and global-metadata.dat files in the game directory, it can be determined that the game was

compiled using the il2cpp compilation mode. Therefore, the source code can be recovered using il2Cpddumper.

Unity_Tools > Il2CppDumper-net6-v6.7.40 > seraph_output				在 seraph_outp
名称	修改日期	类型	大小	
DummyDll	2023/11/22 14:34	文件夹		
out	2023/11/24 1:18	文件夹		
dump.cs	2023/11/22 14:33	C# 源文件	21,784 KB	
il2cpp.h	2023/11/22 14:34	C Header 源文件	34,906 KB	
out.zip	2023/11/24 1:17	WinRAR ZIP 压缩...	955 KB	
script.json	2023/11/22 14:34	JSON 源文件	66,861 KB	
stringliteral.json	2023/11/22 14:34	JSON 源文件	1,135 KB	

```
F: > GameFi > Unity_Tools > Il2CppDumper-net6-v6.7.40 > seraph_output > dump.cs

1 // Image 0: mscorlib.dll - 0
2 // Image 1: UnityEngine.UIElementsModule.dll - 1901
3 // Image 2: System.dll - 2984
4 // Image 3: UnityEngine.CoreModule.dll - 3871
5 // Image 4: Unity.RenderPipelines.Universal.Runtime.dll - 4811
6 // Image 5: Unity.ThirdParty.dll - 5378
7 // Image 6: AstarPathfindingProject.dll - 5854
8 // Image 7: MagicaCloth.dll - 6256
9 // Image 8: com.rlabrecque.steamworks.net.dll - 6570
10 // Image 9: System.Core.dll - 7076
11 // Image 10: Unity.Mathematics.dll - 7702
12 // Image 11: ZFBrowser.dll - 7794
13 // Image 12: Unity.TextMeshPro.dll - 8563
14 // Image 13: RayFireAssembly.dll - 8690
15 // Image 14: UnityEngine.UI.dll - 8897
16 // Image 15: Unity.RenderPipelines.Core.Runtime.dll - 9104
17 // Image 16: UnityEngine.TextCoreTextEngineModule.dll - 9364
18 // Image 17: ThirdPartyPlugins.dll - 9432
19 // Image 18: Unity.VisualScripting.Core.dll - 9585
20 // Image 19: UnityEngine.IMGUIModule.dll - 9816
21 // Image 20: Pathfinding.Ionic.Zip.Reduced.dll - 9869
22 // Image 21: RuntimeInspector.Runtime.dll - 9956
23 // Image 22: Mono.Security.dll - 10065
24 // Image 23: Unity.Patch.dll - 10169
25 // Image 24: Unity.AutoLOD.dll - 10256
26 // Image 25: UnityEngine.ParticleSystemModule.dll - 10320
27 // Image 26: UnityEngine.PhysicsModule.dll - 10402
28 // Image 27: Unity.Collections.dll - 10448
29 // Image 28: UnityEngine.dll - 10599
30 // Image 29: Unity.Timeline.dll - 10600
31 // Image 30: UnityEngine.AnimationModule.dll - 10672
32 // Image 31: Whinarn.UnityMeshSimplifier.Runtime.dll - 10734
33 // Image 32: protobuf-net.dll - 10765
34 // Image 33: Assembly-CSharp.dll - 10803
35 // Image 34: UnityEngine.AndroidJNIModule.dll - 10871
36 // Image 35: UnityEngine.TerrainModule.dll - 10886
37 // Image 36: CString.dll - 10911
38 // Image 37: LitJson.dll - 10926
39 // Image 38: UnityEngine.PropertiesModule.dll - 10956
40 // Image 39: Pathfinding.ClipperLib.dll - 11043
41 // Image 40: UnityEngine.UnityWebRequestModule.dll - 11063
```

However, in the dump.cs file, no strongly relevant code logic related to the game was found. Therefore, it is speculated that the game may not have been developed using C#, but rather loaded through Lua. As a result, by hooking into the functions related to loading buffs in the game's code, the actual source code of the game was obtained.

@AI_ai_utils.lua	2023/11/29 11:56	Lua 源文件	3 K
@AI_bt_action_nodes.lua	2023/11/29 11:56	Lua 源文件	39 K
@AI_bt_base_nodes.lua	2023/11/29 11:56	Lua 源文件	13 K
@AI_bt_condition_nodes.lua	2023/11/29 11:56	Lua 源文件	12 K
@AI_mgr_entity_aggro_cell.lua	2023/11/29 11:56	Lua 源文件	8 K
@AI_mgr_entity_ai_cell.lua	2023/11/29 11:56	Lua 源文件	202 K
@BT_bt94.lua	2023/11/29 12:06	Lua 源文件	3 K
@BT_bt20003.lua	2023/11/29 12:03	Lua 源文件	2 K
@BT_bt20004.lua	2023/11/29 12:06	Lua 源文件	1 K
@BT_bt21000.lua	2023/11/29 12:16	Lua 源文件	1 K
@BT_bt21015.lua	2023/11/29 12:15	Lua 源文件	1 K
@BT_bt23007.lua	2023/11/29 12:11	Lua 源文件	1 K
@BT_bt23020.lua	2023/11/29 12:08	Lua 源文件	2 K
@Core_Class.lua	2023/11/29 11:56	Lua 源文件	4 K
@Core_Entity.lua	2023/11/29 11:56	Lua 源文件	7 K
@Core_EventDispatcher.lua	2023/11/29 11:56	Lua 源文件	2 K
@Core_FrameTimerHeap.lua	2023/11/29 11:56	Lua 源文件	1 K
@Core_FunctionInvoker.lua	2023/11/29 11:56	Lua 源文件	1 K
@Core_GameWorld.lua	2023/11/29 11:56	Lua 源文件	52 K
@Core_LoggerHelper.lua	2023/11/29 11:56	Lua 源文件	3 K
@Core_LuaBehaviour.lua	2023/11/29 11:56	Lua 源文件	2 K
@Core_PrintTable.lua	2023/11/29 11:56	Lua 源文件	4 K
@Core_Queue.lua	2023/11/29 11:56	Lua 源文件	2 K
@Core_Stack.lua	2023/11/29 11:56	Lua 源文件	2 K
@Core_StringEx.lua	2023/11/29 11:56	Lua 源文件	4 K
@Core_TableEx.lua	2023/11/29 11:56	Lua 源文件	6 K
@Core_TimerHeap.lua	2023/11/29 11:56	Lua 源文件	4 K
@Core_XmlSimple.lua	2023/11/29 11:56	Lua 源文件	6 K
@CSFacade.lua	2023/11/29 11:56	Lua 源文件	25 K
@Dramas_drama_trigger_cg.lua	2023/11/29 11:56	Lua 源文件	1 K
@Dramas_drama_trigger_guide.lua	2023/11/29 11:56	Lua 源文件	3 K
@Entities_Avatar.lua	2023/11/29 16:19	Lua 源文件	16 K

```

require "Core.GameWorld"
require "GameDataHelper.GameDataHelper"
require "GameManager.GameManager"
require "GameConfig.GameConfig"
require "GameUtil.GameUtil"
require "PlayerManager.PlayerManager"
require "CSFacade"
require "AI/bt_base_nodes"
require "AI/bt_action_nodes"
require "AI/bt_condition_nodes"

local Application = UnityEngine.Application
local OperationLogManager = GameManager.OperationLogManager
local SystemConfig = GameLoader.SystemConfig
local DataParseHelper = GameDataHelper.DataParseHelper

--主入口函数，从这里开始lua逻辑
function Main()
    GameManager.OperationLogManager.BaseLogData(GameWorld.public_config.OPERATION_LOG_14)
    --package.cpath = package.cpath .. ";c:/Users/admin/AppData/Roaming/JetBrains/Idealc2020.1/plugins/intellij-emy/lua/classes/debugger/emy/windows/x64/?;dll"
    --local dbg = require('emy_core')
    --dbg.tcplisten('localhost', 9966)
    Init()
    Start()
end

function Init()
    local platformType = GameWorld.GetPlatformSetting()
    if platformType == "pc" then
        GameWorld.platformType = 1
    elseif platformType == "mobile" then
        GameWorld.platformType = 2
    else
        GameManager.BagItemManager:Init()
    end
    GameWorld.platformType = 3
end
GameConfig.Global.SetLang()
GameWorld.LoggerHelper:Init()
GameManager.XMLManager.CheckReloadXML()
GameManager.GUIManager:Init()
GameManager.ModuleManager:Init()
GameManager.LanguageManager:Init()
GameManager.CreateRoleManager:Init()
GameManager.DramaManager:Init()
GameManager.TimelineManager:Init()
GameManager.LoadingBarManager:Init()
RegisterEntities()
--GameManager.ModuleManager.TestF = function() end
--LoggerHelper.Log("Init1::",GameManager.XMLManager.map[1])
--LoggerHelper.Log("Init2::",GameManager.XMLManager.spell[21].group)
end

```

And interesting comments were found in the game source code:

```
@ServerConfig_attr_config.lua  @ServerConfig_error_code.lua X dump.cs @Entities_Monster.lua @Entities_Avatar.lua @Entities_PlayerAvatar.lua @GameManager_PlayerCommandManager.lua
@ServerConfig_error_code.lua > ~
790 SYS_ID_TEAM_LEAVE = 30012, --队伍内广播: xx离开队伍
791 SYS_ID_TEAM_BE_KICK = 30013, --个人通知: 被踢除队伍了
792 SYS_ID_TEAM_BE_KICK_TEAM = 30014, --队伍内广播: xx被踢除队伍了
793 SYS_ID_APPLY_WAIT_REPLY = 30018, --申请已发出, 等待对方回应
794
795 --拍卖行
796 AUCTION_PLEASE_ENTER_PRICE = 36040, --请输入价格
797 AUCTION_PLEASE_PUT_ITEM = 36041, --还未放入商品, 无法上架寄售
798 AUCTION_PUT_ITEM_CD = 36045, --该摊位上架冷却中, 请稍后再试
799 AUCTION_BUY_SUCCESS = 36047, --购买成功
800 AUCTION_PKG_NOT_OPEN = 36052, --寄售尚未开启
801 AUCTION_PKG_OPENED = 36053, --寄售已经开启, 不能重复开
802 AUCTION_PKG_OPEN_NOT_ENOUGH = 36054, --钱不够, 不能开启
803 AUCTION_PKG_TYPE = 36055, --寄售类型不对
804 AUCTION_BUY_NOT_ENOUGH = 36056, --钱不够, 不能购买
805 AUCTION_BUY_ALREADY_BOUGHT = 36057, --物品已经被别人购买或下架
806 AUCTION_BIT_MUST_HIGHER = 36058, --出价必须比旧价高
807 AUCTION_BIT_MUST_NOT_BIT = 36059, --卖家设定, 不能竞拍
808 AUCTION_BUY_MUST_NOT_BUY = 36060, --卖家设定, 不能购买
809 AUCTION_PUT_ON_PRICE = 36061, --钻石溢价超过范围
810
811 ----
812 SYS_ID_SERVERS_CUMULATIVE_CHARGE = 40005, --恭喜xxx完成了开服累积目标, 领取了***钻石抽奖奖励
813 SYS_ID_SERVERS_EQUIP_STREN = 40017, --恭喜AAA(玩家名称)将888(装备名称)强化到ccc级(强化等级), 战力提升!
814 SYS_ID_SERVERS_GEN = 40018, --AAA(玩家名称)成功得到888级ccc(宝石类型, 如: 攻击/生命)宝石, 一瞬间流光闪烁, 璀璨冲天!
815 SYS_ID_SERVERS_EQUIP_NASH = 40020, --AAA(玩家名称)将888(装备名称), 洗练出ccc条000属性!
816
817 ----
818 --SYS_ID_SERVERS_COMBAT_VALUE_RANK_ONE_ONLINE = 40027, --[传闻]本服战神AAA(玩家名称)已降临人间, 神威尽显!
819 --SYS_ID_SERVERS_COMBAT_VALUE_RANK_ONE_CHANGE = 40028, --[传闻]AAA成功超越888成为新的战神, 威震天下!
820 SYS_ID_SERVERS_UNLOCK_PASSIVE_SKILL = 40029, --[传闻]AAA(玩家名称)完成了失书寻宝(获得途径), 掌握了绝技(888)(技能名字), 杀怪经验提升30%(描述)
821 SYS_ID_SERVERS_ILLUSION_ACTIVATE = 40030, --[传闻]AAA(玩家名称)成功激活888(化形名字), 战力突飞猛进!
822 SYS_ID_SERVERS_ILLUSION_GRADE_UP = 40031, --[传闻]AAA(玩家名称)将888(坐骑/宠物的化形名字)升级到ccc阶, 战力飙升!
823 SYS_ID_SERVERS_ILLUSION_STAR_UP = 40032, --[传闻]AAA(玩家名称)将888(时装/翅膀/法宝/神兵的化形名字)升级到ccc星, 战力飙升!
824
825 ----
826 SYS_ID_SERVERS_SUPREME_GUARD_CUPID = 40101, --AAA(玩家名称)获得了888(道具名字), 杀怪经验提升50%, 升级速率飙升!
827 SYS_ID_SERVERS_SUPREME_GUARD_PANDA = 40102, --AAA(玩家名称)获得了888(道具名字), 伤害减免提升20%, 战斗能力飞跃提升!
828 SYS_ID_SERVERS_SUPREME_GUARD_HALLMOON_IMP = 40103, --AAA(玩家名称)成功合成了888(道具名字), 杀怪经验提升70%, 伤害提升10%
829 SYS_ID_SERVERS_SUPREME_GUARD_SKULL_KING = 40104, --AAA(玩家名称)成功合成了888(道具名字), 伤害减免提升30%, 暴击提升10%, 暴击减免10%
830 SYS_ID_SERVERS_DROP_SUPREME_ITEM = 40105, --AAA(玩家名称)在888(地点名)与ccc(BOSS名字)大战三百回合, 获得极品000(珍稀物品)!
831 SYS_ID_SERVERS_OPEN_SUPREME_ITEM = 40106, --AAA(玩家名称)开启888(箱子道具名), 获得极品ccc(珍稀物品)!
832 SYS_ID_SERVERS_PICK_DROP_CROSS = 40107, --(AAA)区的(888)在(ccc)击杀了(000), 获得了(EEE)
833 SYS_ID_SERVERS_BLOM_EQUIP = 40108, --xxx在xxx园获得了xxx
834 SYS_ID_SERVERS_COMPOSE = 40201, --玩家成功合成n1ub1道具
835 SYS_ID_SERVERS_VIP_MERCHANDISE = 40266, --金主 仅用 998 买了原价 2 钻石的贵族 礼包, 顶风作案!
```

```
2 文件中有 1 个结果 - 在编辑器中打开
@Modules_ModuleBag_BagPanel.lua
-- 不知道什么意思 先注释 有问题找东明
@PlayerManager_SkillManager.lua
-- "T" then --长松要求加的逻辑, 有问题找他
@PlayerManager_SkillManager.lua_cheat
-- "T" then --长松要求加的逻辑, 有问题找他
@ServerConfig_attr_config.lua  @ServerConfig_error_code.lua X dump.cs @Entities_Monster.lua @Entities_Avatar.lua @Entities_PlayerAvatar.lua @GameManager_PlayerCommandManager.lua
@ServerConfig_attr_config.lua > ~
790 SYS_ID_TEAM_LEAVE = 30012, --队伍内广播: xx离开队伍
791 SYS_ID_TEAM_BE_KICK = 30013, --个人通知: 被踢除队伍了
792 SYS_ID_TEAM_BE_KICK_TEAM = 30014, --队伍内广播: xx被踢除队伍了
793 SYS_ID_APPLY_WAIT_REPLY = 30018, --申请已发出, 等待对方回应
794
795 --拍卖行
796 AUCTION_PLEASE_ENTER_PRICE = 36040, --请输入价格
797 AUCTION_PLEASE_PUT_ITEM = 36041, --还未放入商品, 无法上架寄售
798 AUCTION_PUT_ITEM_CD = 36045, --该摊位上架冷却中, 请稍后再试
799 AUCTION_BUY_SUCCESS = 36047, --购买成功
800 AUCTION_PKG_NOT_OPEN = 36052, --寄售尚未开启
801 AUCTION_PKG_OPENED = 36053, --寄售已经开启, 不能重复开
802 AUCTION_PKG_OPEN_NOT_ENOUGH = 36054, --钱不够, 不能开启
803 AUCTION_PKG_TYPE = 36055, --寄售类型不对
804 AUCTION_BUY_NOT_ENOUGH = 36056, --钱不够, 不能购买
805 AUCTION_BUY_ALREADY_BOUGHT = 36057, --物品已经被别人购买或下架
806 AUCTION_BIT_MUST_HIGHER = 36058, --出价必须比旧价高
807 AUCTION_BIT_MUST_NOT_BIT = 36059, --卖家设定, 不能竞拍
808 AUCTION_BUY_MUST_NOT_BUY = 36060, --卖家设定, 不能购买
809 AUCTION_PUT_ON_PRICE = 36061, --钻石溢价超过范围
```

```
2 文件中有 14 个结果 - 在编辑器中打开
@GameConfig_EntityConfig.lua
-- 属性限制属性: 特殊守护符包 Luatable --pkg_world_ring特殊角就是具体到包
function PlayerSetAttrManager:set_pkg_world_ring(change, get_way)
    if next(Gameworld.Player().pkg_world_ring) then
        BagManager:OnChanged(PkgConfig.BAG_TYPE_PKG_SPECIAL_AMALET, ({}) + Gameworld.Player().pkg_world_ring, change == nil and ({}) = change) or nil, get_way)
    else
        BagManager:OnChanged(PkgConfig.BAG_TYPE_PKG_SPECIAL_AMALET, {}, change == nil and ({}) = change) or nil, get_way)
    end
end
function PlayerSetAttrManager:set_expand_bag_pos_info(change, get_way)
    EventDispatcher:TriggerEvent(Gameworld.BAG_DATA_UPDATE, public_config.PKG_TYPE_LOAD_EXPAND_POS)
end
-- 属性限制属性: 特殊守护符包 Luatable
function PlayerSetAttrManager:set_pkg_getion(change, get_way)
    EventDispatcher:TriggerEvent(Gameworld.BAG_DATA_UPDATE, public_config.PKG_TYPE_POTION)
end
-- 属性限制属性: 特殊守护符包 Luatable
function PlayerSetAttrManager:set_pkg_temporary(change, get_way)
    BagManager:OnChanged(PkgConfig.BAG_TYPE_PKG_TEMPORARY, Gameworld.Player().pkg_temporary, change, get_way)
end
-- 属性限制属性: 特殊守护符包 Luatable
function PlayerSetAttrManager:set_tem_persistent_data(change, get_way)
```

## Analysis Conclusion:

Seraph receives a score of 0 in terms of game code protection, indicating a complete lack of protection. In traditional Lua-based games, custom Lua interpreters are often used with LuaJIT to provide a certain level of code protection.

However, since Seraph lacks a robust code protection mechanism, it results in a low barrier and cost for malicious players to analyze the code. This can lead to unfairness for regular players if cheats or hacks are introduced, and there is a possibility of impacting the game's economic model.

## Game Basic Anti-Cheat:

### Analysis Process:

1. In terms of basic anti-cheat detection, we primarily determine whether the game loads and executes external logic by replacing Lua files.
2. After injecting the DLL using CE injection tool, we examine the game's log files to see if third-party logs are being printed.

```
2023-11-29 16:25:29,414 [SYS_ERROR]: 16:25:29.414-579: [Seraph] 事件二次触发casterId: 45089400当前ID45089400 oldMp: 6278 newMp: 6140 attackType: 1
stack traceback:
  Core/LoggerHelper:62: in function <error>
  Entities/Monster:489: in function <Entities/Monster:453>
  GameMain.CombatSystem.SkillActionManagerServer:JudgeSkillActionByServer(Uint32, Uint32, PbSpellDamageInfo)
  GameMain.CombatSystem.SkillActionManagerServer:JudgeSkillActionByServer(Uint32, Uint32, PbSpellDamageInfo)
  GameMain.CombatSystem.SkillManager:JudgeSkillActionByServer(Uint32, Uint32, PbSpellDamageInfo)
  GameMain.GlobalManager.PlayerSkillManager:SpellDamageResp(Byte[])
  GameMain.KnittyLayer:SpellDamageResp(Byte[])
  GameEngine.Mgrs.EntityMgr:RPCall(String, Object[])
  GameEngine.Events.GameEvent:2:Invoke(String, Object[])
  GameEngine.Events.EventController:TriggerEvent(String, String, Object[])
  GameEngine.Events.EventDispatcher:TriggerEvent(String, String, Object[])
  GameEngine.RPC.RPCallProto:HandleData()
  GameEngine.RPC.RemoteProxy:DataHandler(Byte[], Int32, Int32)
  GameEngine.RPC.RemoteProxy:Update()
  EngineDriver:Update()
  UnityEngine.Debug:LogError(Object)
  LuaInterface.LuaDll:lua_pcall(Int32, Int32, Int32)
  LuaInterface.LuaDll:lua_pcall(Int32, Int32, Int32)

[Seraph]
1771 2023-11-29 15:34:08,201 [SYS_ERROR]: 15:34:08.201-3801 [Seraph] 事件二次触发casterId: 46138046当前ID46138046 oldMp: 1893 newMp: 1749 attackType: 1
1772 2023-11-29 15:34:11,747 [SYS_ERROR]: 15:34:11.747-5931 [Seraph] 事件二次触发casterId: 46138046 oldMp: 1842 newMp: 5125 attackType: 1
1773 2023-11-29 15:34:15,800 [SYS_ERROR]: 15:34:15.800-9411 [Seraph] 事件二次触发casterId: 46138046 oldMp: 4626 newMp: 1870 attackType: 1
1774 2023-11-29 15:34:15,800 [SYS_ERROR]: 15:34:15.800-9411 [Seraph] 事件二次触发casterId: 46138046当前ID46138046 oldMp: 4626 newMp: 1870 attackType: 1
1775 2023-11-29 15:34:15,801 [SYS_ERROR]: 15:34:15.801-9411 [Seraph] 事件二次触发casterId: 46138046 oldMp: 4626 newMp: 520 attackType: 1
1776 2023-11-29 15:34:15,802 [SYS_ERROR]: 15:34:15.802-9411 [Seraph] 事件二次触发casterId: 46138046当前ID46138046 oldMp: 4626 newMp: 520 attackType: 1
1777 2023-11-29 15:34:20,747 [SYS_ERROR]: 15:34:20.746-1341 [Seraph] 事件二次触发casterId: 46138046 oldMp: 5873 newMp: 5132 attackType: 1
1778 2023-11-29 15:34:20,747 [SYS_ERROR]: 15:34:20.747-1341 [Seraph] 事件二次触发casterId: 46138046当前ID46138046 oldMp: 5873 newMp: 5132 attackType: 1
1779 2023-11-29 15:34:20,748 [SYS_ERROR]: 15:34:20.748-1341 [Seraph] 事件二次触发casterId: 46138046 oldMp: 1901 newMp: 1813 attackType: 1
1780 2023-11-29 15:34:20,748 [SYS_ERROR]: 15:34:20.748-1341 [Seraph] 事件二次触发casterId: 46138046当前ID46138046 oldMp: 1901 newMp: 1813 attackType: 1
1781 2023-11-29 15:34:26,543 [SYS_ERROR]: 15:34:26.543-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 7058 newMp: 6755 attackType: 1
1782 2023-11-29 15:34:26,544 [SYS_ERROR]: 15:34:26.544-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 4423 newMp: 6412 attackType: 1
1783 2023-11-29 15:34:26,544 [SYS_ERROR]: 15:34:26.544-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 6452 newMp: 6349 attackType: 1
1784 2023-11-29 15:34:26,545 [SYS_ERROR]: 15:34:26.545-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 4423 newMp: 6349 attackType: 1
1785 2023-11-29 15:34:26,545 [SYS_ERROR]: 15:34:26.545-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 6090 newMp: 5707 attackType: 1
1786 2023-11-29 15:34:26,546 [SYS_ERROR]: 15:34:26.546-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 4767 newMp: 4464 attackType: 1
1787 2023-11-29 15:34:26,546 [SYS_ERROR]: 15:34:26.546-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 7462 newMp: 7099 attackType: 1
1788 2023-11-29 15:34:26,546 [SYS_ERROR]: 15:34:26.546-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 4423 newMp: 6120 attackType: 1
1789 2023-11-29 15:34:26,546 [SYS_ERROR]: 15:34:26.546-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 6460 newMp: 6087 attackType: 1
1790 2023-11-29 15:34:26,546 [SYS_ERROR]: 15:34:26.546-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 7152 newMp: 6849 attackType: 1
1791 2023-11-29 15:34:26,546 [SYS_ERROR]: 15:34:26.546-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 6131 newMp: 5828 attackType: 1
1792 2023-11-29 15:34:26,546 [SYS_ERROR]: 15:34:26.546-4791 [Seraph] 事件二次触发casterId: 5779404 oldMp: 5797 newMp: 5494 attackType: 1
```



- By modifying the Lua logic, it was possible to modify in-game data such as critical hit rate, and the modifications were effective without any checks in the game. (Modifying attribute data only affects the visual display, as these fields are typically stored on the server-side, and local modifications usually do not have any actual effect.)



### Analysis Conclusion:

- Seraph scores 0 in terms of anti-cheat capabilities, which means that malicious users can cheat without any restrictions.

The main reason for specifically testing the reloading of Lua in the game is that this action serves as the foundation for cheating in Lua-based games. If this aspect cannot be effectively addressed, it indicates a weak point in the anti-cheat measures, and it is likely that other aspects of anti-cheat will also be lacking or ineffective.

## Game Logic Issues

### Analysis Process:

Since we have obtained the game's source code, we conducted a security analysis focusing on the logic layer. We did not analyze the protocol layer. In terms of the logic layer, we primarily performed security testing on the following aspects:

Attribute tampering during character initialization: (It was found that there are not many sensitive attributes in this section, and it does not yield significant benefits.)

```
function PlayerAvatar:OnEnterWorld()
    self.canPickUpStatus = 0
    self:AddListeners()
    GameManager.OperationLogManager.BaseLogData(GameWorld.public_config.OPERATION_LOG_10)
    self.cs.isLoadImmediately = true
    PlayerAvatar._base.OnEnterWorld(self)
    GameWorld.SetAccount(self.account_name)
    GameWorld.SetAvatarName(self.name)
    GameWorld.CheckFullUploadLog()
    --self._stateManager:SetDispatchEnterDead(true)
    -- self:CheckNewPlayer()
    -- self:SetPosToSlot()
    RedPointManager:OnEnterWorld()
    PlayerDataManager:OnPlayerEnterWorld()
    --EquipManager:OnPlayerEnterWorld();
    BagManager:OnPlayerEnterWorld()
    PlayerActionManager:OnPlayerEnterWorld()
    -- PlayerCommandManager:Init()
    PlayerCommandManager:OnPlayerEnterWorld()
    ResourceMappingManager:OnPlayerEnterWorld()
    CopperAvatarManager:OnPlayerEnterWorld()
    TrainManager:OnPlayerEnterWorld()
    self:LoadPlayerBleedingUIfx()
    self:SetPreloadSkill(true)
    self:SetLearnedSkillDict(self:GetEquipSkillIdList())
    self:PlayerEnterWorldLog()
    GameWorld.SetMaxScreenMonsterCount(GlobalParamsHelper.GetParamValue(916))
    if GameStateManager.GetState() ~= GAME_STATE.SCENE then
        --遮盖创角选角短暂穿帮问题
        --LoadingBarManager:ShowProgressBar(0.1)
    end
    --self:CheckLoadEmptyWeapon()
    self:SetFunctionOpenActive()
    self:SetServerInfo(LocalSetting.settingData.SelectedServerID, ServerListManager.SelectedServerName())

    --EventDispatcher:TriggerEvent(GameEvents._GameON_FUNCTIONPREVIEWPANEL) --进入游戏后刷新functionPreview
    if GUIManager.hasHandleEscape then
        self._clearStackTimer = TimerHeap:AddSecTimer(0, self._clearStackTime, 0, function()
            GUIManager.ClearClosePanelStack()
        end)
    end
    end
    --GameWorld.ShowMainCamera()
    self:SetQualitySettingValue(0)

    if (GameLoader.SystemConfig.IsUsePlatformSdk and GameManager.LoginManager.accessToken) then
```

The next aspect we tested was the manipulation of skills related to active attacks. It was found that this part is only for display purposes and does not actually participate in damage validation.

```

function SkillManager:GetSkillShowDamage(data, level)
    --技能主要伤害
    local skillId = data.skillId
    local owner = data.owner --owner: 1=玩家, 2=佣兵, 3=其他玩家
    local cal = SkillDataHelper:GetDamageCal(skillId)
    if next(cal) then
        local param = self:DescParam(data, level)
        local minDamage
        local maxDamage
        local factor
        if owner == 1 then
            minDamage = AttributeManager:GetAttributeByAttID(attri_config.ATTRI_ID_DMG_MIN)
            maxDamage = AttributeManager:GetAttributeByAttID(attri_config.ATTRI_ID_DMG_MAX)
            factor = AttributeManager:GetAttributeByAttID(attri_config.ATTRI_ID_NON_WEAPON_ED)
        elseif owner == 2 then
            if data.mercenaryAtt then
                minDamage = data.mercenaryAtt[attri_config.ATTRI_ID_DMG_MIN] or 1
                maxDamage = data.mercenaryAtt[attri_config.ATTRI_ID_DMG_MAX] or 1
                factor = data.mercenaryAtt[attri_config.ATTRI_ID_NON_WEAPON_ED] or 0
            else
                minDamage = 1
                maxDamage = 1
                factor = 0
            end
        elseif owner == 3 then
            local attData = OtherPlayerManager:GetAllAttributesData()
            minDamage = attData[attri_config.ATTRI_ID_DMG_MIN] or 1
            maxDamage = attData[attri_config.ATTRI_ID_DMG_MAX] or 1
            factor = attData[attri_config.ATTRI_ID_NON_WEAPON_ED] or 0
        end
        local min = 0
        local max = 0
        for i, v in ipairs(cal) do
            if v == 0 then
            elseif v == 1 then
                min = min + param[i][1]/100 * minDamage * (1 + factor/100)
                max = max + param[i][1]/100 * maxDamage * (1 + factor/100)
            elseif v == 2 then
                if #param[i] == 2 then
                    LoggerHelper.Error("Config Error!!!! Excel:spell.xml ---- damage_cal ----id:"..skillId)
                else
                    min = min + param[i][1]
                    max = max + param[i][2]
                end
            end
        end
        min = min - min % 0.1
        max = max - max % 0.1
        max = max * 100
        min = min * 100
        return {min, max}
    end
end

```

Lastly, we tested the modification of logic when monsters are attacked. It was found that modifying this aspect did not have any practical significance. It is speculated that the primary purpose of this module during development was to trigger events for recording purposes, rather than participating in actual calculations.

```
--这个方法，目前都是技能伤害导致血量变化。
function Monster:OnChangeHp(casterId, oldHp, newHp, attackType)

    -- 修改，只要血量变化 就会杀怪
    -- LoggerHelper.Error("[Senna]casterId:  " .. tostring(casterId) .. "   oldHp:  " .. tostring(oldHp) .. "   newHp:  " .. tostr
    if casterId == GameWorld.Player().id and newHp <= 0 then
        EventDispatcher:TriggerEvent(GameEvents.KillMonster_Exp)
    end

    if casterId ~= GameWorld.Player().id then
        return
    end

    if newHp <= 0 then
        return
    end
    -- LoggerHelper.Error("casterId:  " .. tostring(casterId) .. "   oldHp:  " .. tostring(oldHp) .. "   newHp:  " .. tostring(ne
    EventDispatcher:TriggerEvent(GameEvents.MONSTER_HP_CHANGE_EVENT, self.id)

    if self.behavior_state == 0 then
        local exit_action = MonsterDataHelper:GetExitAction(self.monster_id)
        if exit_action > 0 then
            local player = GameWorld.Player()
            player.server.set_monster_behavior_state(self.id, 1)
        end
    end

    if self:GetEntityAI() then
        self:GetEntityAI():on_change_hp(casterId, tonumber(newHp) - tonumber(oldHp), attackType)
    end
    --LoggerHelper.Error("[Senna]事件二次触发casterId:  " .. tostring(casterId)..当前ID"..GameWorld.Player().id .. "   oldHp:  " .. to
    casterId = GameWorld.Player().id
    newHp = 0
    attackType = 30
    if casterId == GameWorld.Player().id and newHp <= 0 then
        EventDispatcher:TriggerEvent(GameEvents.KillMonster_Exp)
        return
    end
end
end
```

## Analysis Conclusion:

1. Seraph did not show any effect on the three points we randomly tampered with, indicating that the damage calculation and display are separated, or the calculations are performed by the server, which provides a certain level of security. It receives a score of 3 out of 10.
2. However, some damage calculations are stored locally, leaving room for cheating.

# Game RPC Analysis

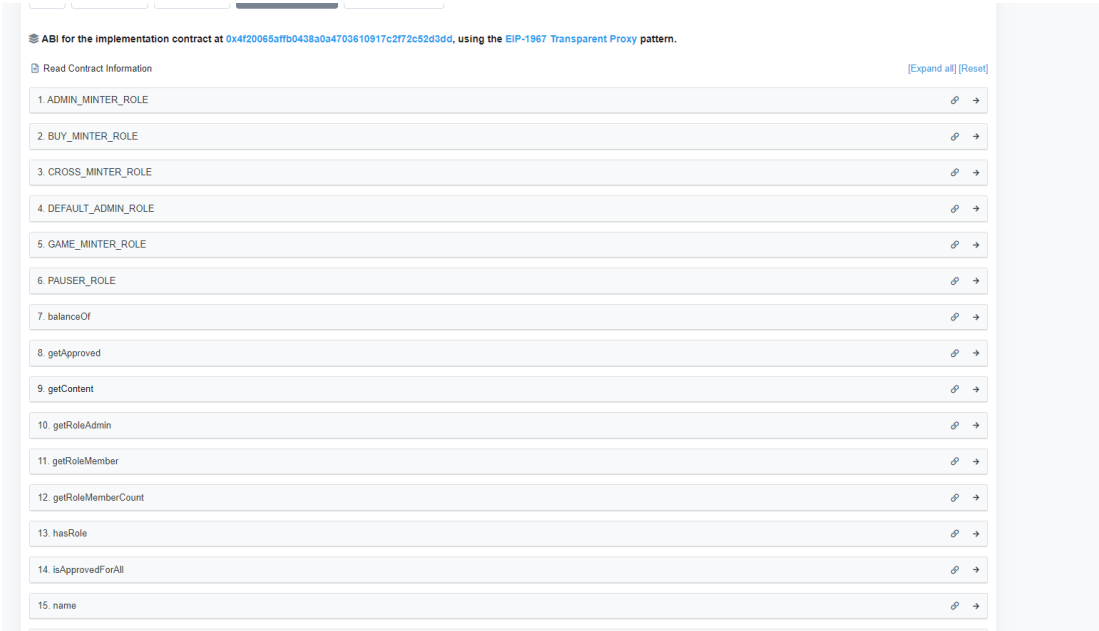
*The game utilizes Protocol Buffers (protobuf) for protocol interaction, including interactions related to Web3. Currently, detailed testing has not been conducted specifically for this part, but there may be plans for thorough testing of the protobuf portion in the future.*

```
> protobuf
79 文件中有 1076 个结果 在编辑器中打开
WEAPON__NIGHTMAREUPGRADE_FIELD = protobuf.FieldDe...
WEAPON__HELLUPGRADE_FIELD = protobuf.FieldDescripto...
WEAPON__RECENT_FIELD = protobuf.FieldDescriptor;
WEAPON__PICKUP_SOUND_FIELD = protobuf.FieldDescriptor;
WEAPON__EFFECT_FIELD = protobuf.FieldDescriptor;
WEAPON__MAINTYPE_FIELD = protobuf.FieldDescriptor;
WEAPON__BASE_CRIT_FIELD = protobuf.FieldDescriptor;
WEAPON__BASE_SKILLCRIT_FIELD = protobuf.FieldDescripto...
weapon = protobuf.Message(WEAPON)
@Protol_world_boss_pb.lua 23
local protobuf = require "protobuf.protobuf"
local protobuf = require "protobuf.protobuf"
protobuf = require "protobuf.protobuf"
WORLD_BOSS = protobuf.Descriptor;
WORLD_BOSS__ID_FIELD = protobuf.FieldDescriptor;
WORLD_BOSS__SINCE_ID_FIELD = protobuf.FieldDescriptor;
WORLD_BOSS__LEVEL_LIMIT_FIELD = protobuf.FieldDescript...
WORLD_BOSS__REALM_LIMIT_FIELD = protobuf.FieldDescript...
WORLD_BOSS__REALM_SHOW_FIELD = protobuf.FieldDescript...
WORLD_BOSS__REALM_LEVEL_FIELD = protobuf.FieldDescript...
WORLD_BOSS__BOSS_NAME_FIELD = protobuf.FieldDescript...
WORLD_BOSS__BOSS_NAME_ICON_FIELD = protobuf.FieldDescript...
WORLD_BOSS__BOSS_ICON_FIELD = protobuf.FieldDescript...
WORLD_BOSS__BOSS_MONSTER_ID_FIELD = protobuf.FieldDescript...
WORLD_BOSS__BOSS_DROPS_FIELD = protobuf.FieldDescript...
WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD = protobuf.FieldDescript...
WORLD_BOSS__BOSS_POS_FIELD = protobuf.FieldDescript... X
WORLD_BOSS__PEACE_SHOW_FIELD = protobuf.FieldDescript...
WORLD_BOSS__KILL_TIME_FIELD = protobuf.FieldDescriptor;
WORLD_BOSS__SCALE_FIELD = protobuf.FieldDescriptor;
WORLD_BOSS__PEACE_SHOW_FIELD = protobuf.FieldDescriptor;
WORLD_BOSS__MODE_FIELD = protobuf.FieldDescriptor;
world_boss = protobuf.Message(WORLD_BOSS)
@Protol_world_map_pb.lua 17
local protobuf = require "protobuf.protobuf"
local protobuf = require "protobuf.protobuf"
protobuf = require "protobuf.protobuf"
WORLD_MAP = protobuf.Descriptor;
WORLD_MAP__ID_FIELD = protobuf.FieldDescriptor;
WORLD_MAP__BUTTON_FIELD = protobuf.FieldDescriptor;
WORLD_MAP__BUTTON_NAME_FIELD = protobuf.FieldDescript...
WORLD_MAP__TYPE_MAP_ICON_FIELD = protobuf.FieldDescript...
WORLD_MAP__REGIONAL_ICON_FIELD = protobuf.FieldDescript...
WORLD_MAP__SCENE_ID_FIELD = protobuf.FieldDescriptor;
WORLD_MAP__DOWN_POSITION_FIELD = protobuf.FieldDescript...
WORLD_MAP__UP_POSITION_FIELD = protobuf.FieldDescriptor;
WORLD_MAP__MAP_LEVEL_FIELD = protobuf.FieldDescriptor;
WORLD_MAP__SCALE_FIELD = protobuf.FieldDescriptor;
WORLD_MAP__OFFSET_FIELD = protobuf.FieldDescriptor;
WORLD_MAP__SCALE2_FIELD = protobuf.FieldDescriptor;
world_map = protobuf.Message(WORLD_MAP)
119 WORLD_BOSS__BOSS_MONSTER_ID_FIELD.label = 2
120 WORLD_BOSS__BOSS_MONSTER_ID_FIELD.has_default_value = false
121 WORLD_BOSS__BOSS_MONSTER_ID_FIELD.default_value = 0
122 WORLD_BOSS__BOSS_MONSTER_ID_FIELD.type = 5
123 WORLD_BOSS__BOSS_MONSTER_ID_FIELD.cpp_type = 1
124
125 WORLD_BOSS__BOSS_DROPS_FIELD.name = "_boss_drops"
126 WORLD_BOSS__BOSS_DROPS_FIELD.full_name = ".world_boss__boss_drops"
127 WORLD_BOSS__BOSS_DROPS_FIELD.number = 11
128 WORLD_BOSS__BOSS_DROPS_FIELD.index = 10
129 WORLD_BOSS__BOSS_DROPS_FIELD.label = 2
130 WORLD_BOSS__BOSS_DROPS_FIELD.has_default_value = false
131 WORLD_BOSS__BOSS_DROPS_FIELD.default_value = ""
132 WORLD_BOSS__BOSS_DROPS_FIELD.type = 9
133 WORLD_BOSS__BOSS_DROPS_FIELD.cpp_type = 9
134
135 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.name = "_boss_extra_drops"
136 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.full_name = ".world_boss__boss_extra_drops"
137 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.number = 12
138 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.index = 11
139 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.label = 2
140 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.has_default_value = false
141 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.default_value = ""
142 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.type = 9
143 WORLD_BOSS__BOSS_EXTRA_DROPS_FIELD.cpp_type = 9
144
145 WORLD_BOSS__BOSS_POS_FIELD.name = "_boss_pos"
146 WORLD_BOSS__BOSS_POS_FIELD.full_name = ".world_boss__boss_pos"
147 WORLD_BOSS__BOSS_POS_FIELD.number = 13
148 WORLD_BOSS__BOSS_POS_FIELD.index = 12
149 WORLD_BOSS__BOSS_POS_FIELD.label = 2
150 WORLD_BOSS__BOSS_POS_FIELD.has_default_value = false
151 WORLD_BOSS__BOSS_POS_FIELD.default_value = ""
152 WORLD_BOSS__BOSS_POS_FIELD.type = 9
153 WORLD_BOSS__BOSS_POS_FIELD.cpp_type = 9
154
155 WORLD_BOSS__PEACE_SHOW_FIELD.name = "_peace_show"
156 WORLD_BOSS__PEACE_SHOW_FIELD.full_name = ".world_boss__peace_show"
157 WORLD_BOSS__PEACE_SHOW_FIELD.number = 14
158 WORLD_BOSS__PEACE_SHOW_FIELD.index = 13
159 WORLD_BOSS__PEACE_SHOW_FIELD.label = 2
160 WORLD_BOSS__PEACE_SHOW_FIELD.has_default_value = false
161 WORLD_BOSS__PEACE_SHOW_FIELD.default_value = 0
162 WORLD_BOSS__PEACE_SHOW_FIELD.type = 5
163 WORLD_BOSS__PEACE_SHOW_FIELD.cpp_type = 1
164
165 WORLD_BOSS__KILL_TIME_FIELD.name = "_kill_time"
166 WORLD_BOSS__KILL_TIME_FIELD.full_name = ".world_boss__kill_time"
167 WORLD_BOSS__KILL_TIME_FIELD.number = 15
168 WORLD_BOSS__KILL_TIME_FIELD.index = 14
169 WORLD_BOSS__KILL_TIME_FIELD.label = 2
170 WORLD_BOSS__KILL_TIME_FIELD.has_default_value = false
171 WORLD_BOSS__KILL_TIME_FIELD.default_value = 0
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

## WEB3 Security Analysis:

















### Summary:

Currently, Seraph has not issued its own token. The Mint contract is a standard NFT721 contract with a total supply of 3225, and both the Mint and cross-chain functionalities are controlled by roles. The on-chain security is controllable.



ABI for the implementation contract at 0x4f20065affb0438a0a4703610917c2f72c52d3dd, using the EIP-1967 Transparent Proxy pattern.

[Read Contract Information](#) [\[Expand all\]](#) [\[Reset\]](#)

1. ADMIN_MINTER_ROLE	 
2. BUY_MINTER_ROLE	 
3. CROSS_MINTER_ROLE	 
4. DEFAULT_ADMIN_ROLE	 
5. GAME_MINTER_ROLE	 
6. PAUSER_ROLE	 
7. balanceOf	 
8. getApproved	 
9. getContant	 
10. getRoleAdmin	 
11. getRoleMember	 
12. getRoleMemberCount	 
13. hasRole	 
14. isApprovedForAll	 
15. name	 

### Game Economy System Security Analysis:

Currently, the primary method for earning currency in Seraph is through Soul Crystals. Whether it is crafting Soul Caskets or opening them, the server is responsible for the determination, while the client initiates the requests. The security is primarily controlled by the server, so the security assessment falls outside the scope of client security evaluation. In the future, Damocles may perform a comprehensive review and black-box testing of all requests.

```
end
elseif act_id == action_config.CHAOS_GET_MONEY_REQ then --获取账号pkg_chaos的货币数量
    self.XGoldCount = args
    EventDispatcher:TriggerEvent(gameEvents.ChaosWarehouse_XGoldCount,args)
    EventDispatcher:TriggerEvent(gameEvents.RefreshGoldNum)
elseif act_id == action_config.CHAOS_ADD_MONEY_REQ then --游戏内注册pkg_chaos货币
    ChaosWarehouseManager:RequestXGoldCount()
elseif act_id == action_config.CHAOS_REMOVE_MONEY_REQ then --游戏内从pkg_chaos取货币
    ChaosWarehouseManager:RequestXGoldCount()
elseif act_id == action_config.CHAOS_ITEM_UPDATE_RESP then --web端更新了pkg_chaos
    ChaosWarehouseManager:RequestPKGChaos(self.OnePageCount)
elseif act_id == action_config.CHAOS_MONEY_UPDATE_RESP then --web端更新了货币
    ChaosWarehouseManager:RequestXGoldCount()
elseif act_id == action_config.CHAOS_GET_PACK_Y_CNT then --获取构造一个灵魂之屋需要的y币数量
    EventDispatcher:TriggerEvent(gameEvents.ChaosWarehouse_YCoinToSoulBoxExchangeProportion,GameWorld.Player().tmp_persistent_data[public_config.TMP_PERSISTENT_DATA_KEY_DAY_PACK_Y_CNT])
elseif act_id == action_config.CHAOS_PACK_Y_COIN then --构造灵魂之屋
    EventDispatcher:TriggerEvent(gameEvents.ChaosWarehouse_UpdateSoulPackingView)

    GUIManager.ShowText(11,LanguageDataHelper.CreateContent(3035,{"0"}<ChaosWarehouseManager.itemCountText))
elseif act_id == action_config.CHAOS_UNPACK_SOUL_BOX then --开始灵魂之屋
    EventDispatcher:TriggerEvent(gameEvents.ChaosWarehouse_UpdateSoulPackingView)

    GUIManager.ShowText(11,LanguageDataHelper.CreateContent(3037,{"0"}<ChaosWarehouseManager.itemCountText))
elseif act_id == action_config.CHAOS_SRF_SMLT then --灵魂之屋兑换SRF
    EventDispatcher:TriggerEvent(gameEvents.ChaosWarehouse_UpdateSPFSmltView)

    GUIManager.ShowText(11,LanguageDataHelper.CreateContent(3038,{"0"}<ChaosWarehouseManager.itemCountText))
elseif act_id == action_config.CHAOS_SRF_EXCHANGE then --SRF兑换灵魂之屋
    EventDispatcher:TriggerEvent(gameEvents.ChaosWarehouse_UpdateSPFSmltView)

    GUIManager.ShowText(11,LanguageDataHelper.CreateContent(3040,{"0"}<ChaosWarehouseManager.itemCountText))
elseif act_id == action_config.CHAOS_CHARGE_REQ then --充值
    EventDispatcher:TriggerEvent(gameEvents.ChaosWarehouse_Recharge,args)
elseif act_id == action_config.CHAOS_WITHDRAW_REQ then --提现
    EventDispatcher:TriggerEvent(gameEvents.ChaosWarehouse_UpdateSPFSmltView)
end
end
```

## About Damocles

Damocles Labs is a security team established in 2023, specializing in security for the Web3 industry. Their services include contract code auditing, business code auditing, penetration testing, GameFi code auditing, GameFi vulnerability discovery, GameFi cheat analysis, and GameFi anti-cheat measures. They are committed to making continuous efforts in the Web3 security industry, producing as many analysis reports as possible, raising awareness among project owners and users about GameFi security, and promoting the overall security development of the industry.

Twitter: <https://twitter.com/DamoclesLabs>

Discord: <https://discord.gg/xd6H6eqFHz>