

Game Hacking: How to not be a script kiddie



Chris & Ravi



Write meeting flag on board

Downloads

Games are just code!

- Stack
- Heap
- Libc
- All reversing concepts apply

Common Attack Vectors

- Exploit from within game
 - (teleport challenge)
- Recon/ social engineering
- Modify game state in memory
- Exploit bugs in game code- code execution?
- Code injection!

Exploiting In-Game



Minecraft - 1.9 DUPLICATION GLITCH (Anything) [Tutorial] MCPE / Bedrock / Xbox / Switch

Skippy 6 Gaming • 51K views • 3 weeks ago

Help me get to 300k ! Join SQUAD6 🔥✅ <https://goo.gl/MOq1tx> ✅ How to DUPLICATE ANYTHING and Diamonds Glitch for Minecraft ...



Minecraft Duplication Glitch! EASY DIAMONDS!! DUPLICATE ANY RESOURCE ITEM! PS4/ Console Edition

ThunderCatGaming • 46K views • 1 month ago

Y000, What is up guys?? This is ThunderCat Gaming here today with another AWESOME Minecraft Duplication Glitch!



Minecraft - 1.8 DUPLICATION GLITCH [Anything + XP] MCPE / Xbox / Bedrock

Skippy 6 Gaming • 117K views • 2 months ago

Help me get to 300k ! Join SQUAD6 🔥✅ <https://goo.gl/MOq1tx> ✅ Today I am going to show you how to do a DIAMOND DUPLICATION ...

Exploiting In-Game



Recon/ Social Engineering



Using a Fortnite Cheat to get FREE V-BUCKS

Sernandoe ✓ 1.4M views · 4 months ago

Fortnite CHEATER Tried Giving Me FREE V-BUCKS Twitter: <https://twitter.com/sernandoe> Subscribe Here - <http://goo.gl/jps6WY> ...

Modify Game Memory

- Must be done while game running
- Scan memory for known value
- Change value, rescan
- Eventually find where that value is stored
- ASLR? Never heard of it

Modify Game Memory



Exploit Bugs in Game Code

Example: Integer overflow/ underflow (Civilization)



Code Injection

- The crown jewel of game hacking
- Layer escalation: low level (C++) -> C# (.NET)
- Unmanaged: C++/ Machine Code
- Managed: C#/ IL/ CLR

Cheat Engine

Cheat Engine 6.8.3

File Edit Table D3D Help

0000557C-ac_client.exe

Found: 616

Address	Value	Previous
0018DCEC	100	100
0018DFB8	100	100
0019C2E4	100	100
009471B8	100	100
00947230	100	100
00947238	100	100
00947248	100	100
00947258	100	100
00947268	100	100
009472BC	100	100
009485F4	100	100
00953130	100	100
009727E4	100	100
009727FC	100	100
00983E60	100	100
00983E7C	100	100

New Scan Next Scan Undo Scan

Value: 100

Hex 100

Scan Type Exact Value Not

Value Type 4 Bytes

Memory Scan Options

All

Start 0000000000000000

Stop 00007FFFFFFFFFFFFFFF

Writable CopyOnWrite Executable

Fast Scan 4 Alignment Last Digits

Pause the game while scanning

Unrandomizer

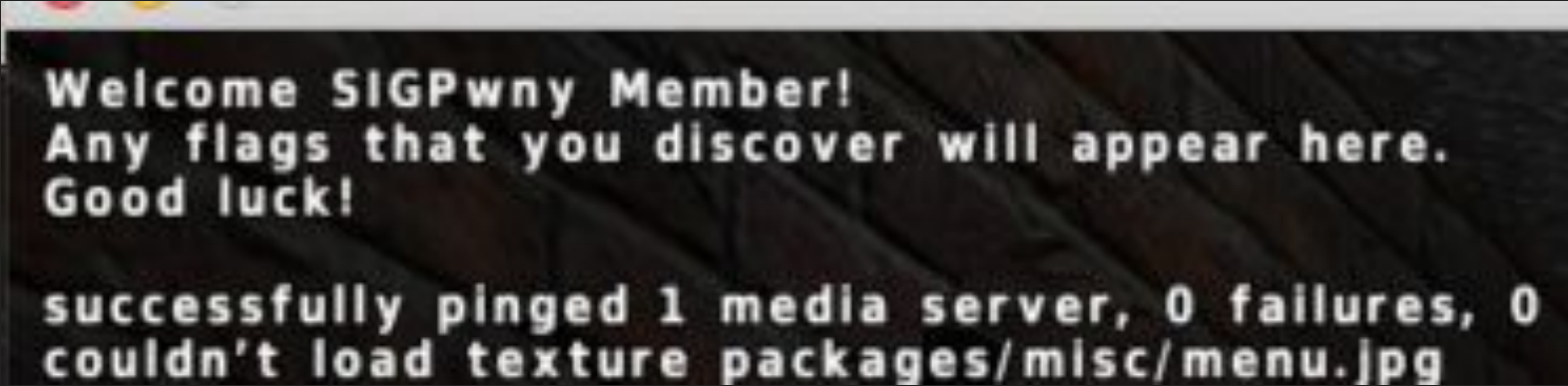
Enable Speedhack

Settings

The Target: AssaultCube

Flags will be reported to the console in the top left!

To exit the game, type 'exit' into the chat (open chat with 'T')



Welcome SIGPwny Member!

Any flags that you discover will appear here.

Good luck!

**successfully pinged 1 media server, 0 failures, 0
couldn't load texture packages/misc/menu.jpg**

Challenge 1

Set your ammo to a
very large value!

Challenge 2

Set your X coordinate
to > 1000 for a flag!

Challenge 3

Disable the part of the code that causes health to decrease.

Challenge 4

Use static analysis to
find a hidden flag in
the binary!

Challenge 5: Buffer Overflow

Goal: Overwrite a stack
variable to a desired value

Challenge 5: Buffer Overflow

Input Vector: the chat field!

To try this, send a message
where the first character is

\%'

Challenge 5: Buffer Overflow

Called every time a message is sent where the first character is '%':

```
void sigPwny_vulnerable_buffer_1 (char* buf) {
    int canary = 0xDEADBEEF;
    char local_buffer[4];
    int length = 0;
    char* cursor = buf;
    while (*(cursor++)) { length++; }

    length = (length > sizeof(local_buffer) + 4) ? sizeof(local_buffer) + 4 : length;

    memcpy(local_buffer, buf, length);

    conoutf("The canary is: %x", canary);

    if (canary == 0x78786168) {
        conoutf("sigpwny{xxxxxxxxxx}");
    }
}
```

Challenge 6: Format String Attack

Goal: Leak a variable from the stack.

Challenge 6: Format String Attack

The variable is of the form:

0x50XXXX50 and is on the stack
near the problematic call.

Challenge 6: Format String Attack

To try it, send a message where the first character is ``#'`. The output in the top is the result of your format string.

Challenge 6: Format String Attack

When you have the variable, convert it from ASCII and send the 4-character message (without a # sign).

Creative 🙌 Challenge 🙌

- Create the best hacked client you can!
- Work alone or with a partner
- Post a cheats montage á la 2009 to Youtube
- Coolest hacks win lots of pwnypoints!