Game Hacking: How to not be a script kiddie

Chris & Ravi

Write meeting flag on board
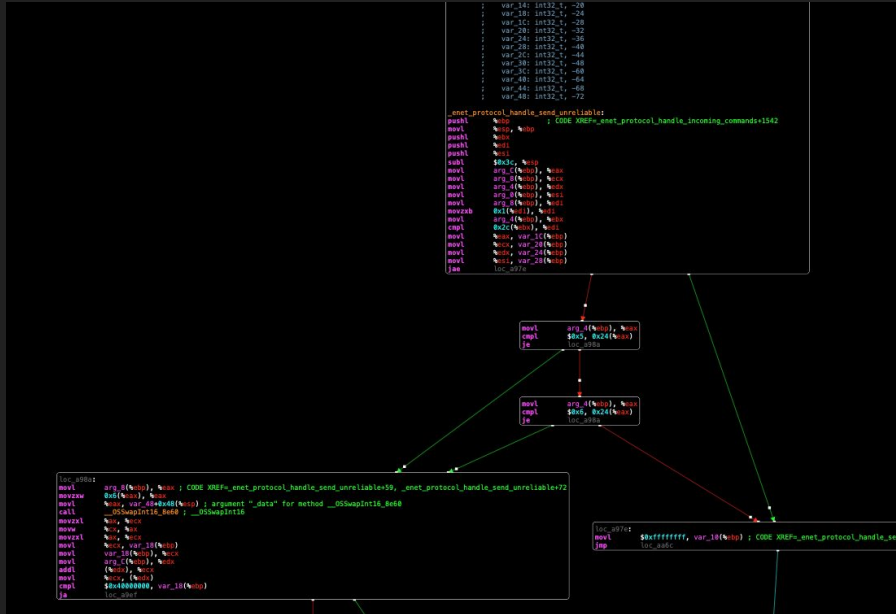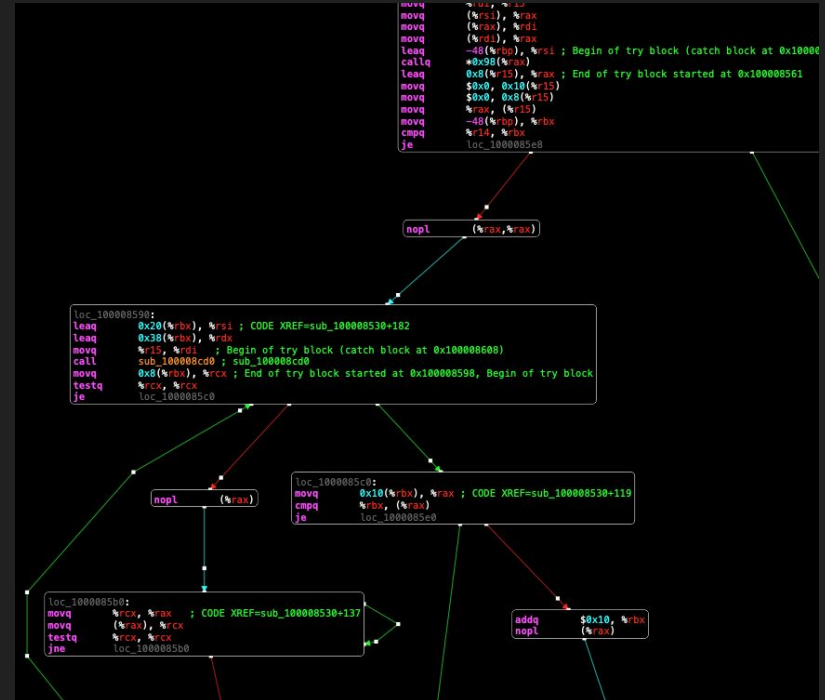
Games are just code!

- Stack
- Heap
- Libc
- All reversing concepts apply

Game Code VS Regular Application Code

Assault Cube:

Spotify:

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

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)

Greetings from M.Gandhi, ruler
and King of the Indians...
Our words are backed
with NUCLEAR WEAPONS!

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
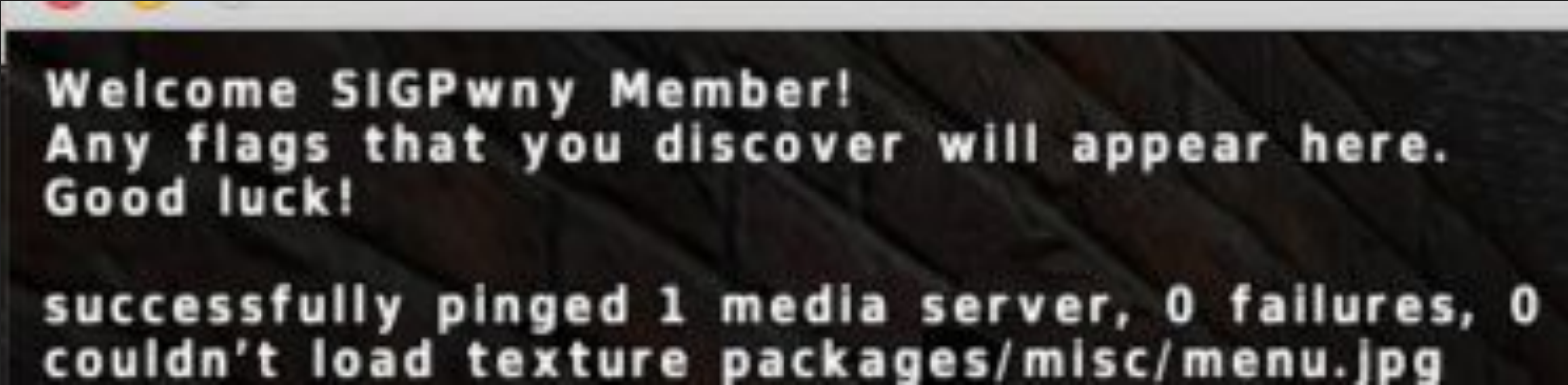
The Target: AssaultCube

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{xxxxxxxxx}");
    }
}
```

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!