

Game Hacking 101

Julian Dunning

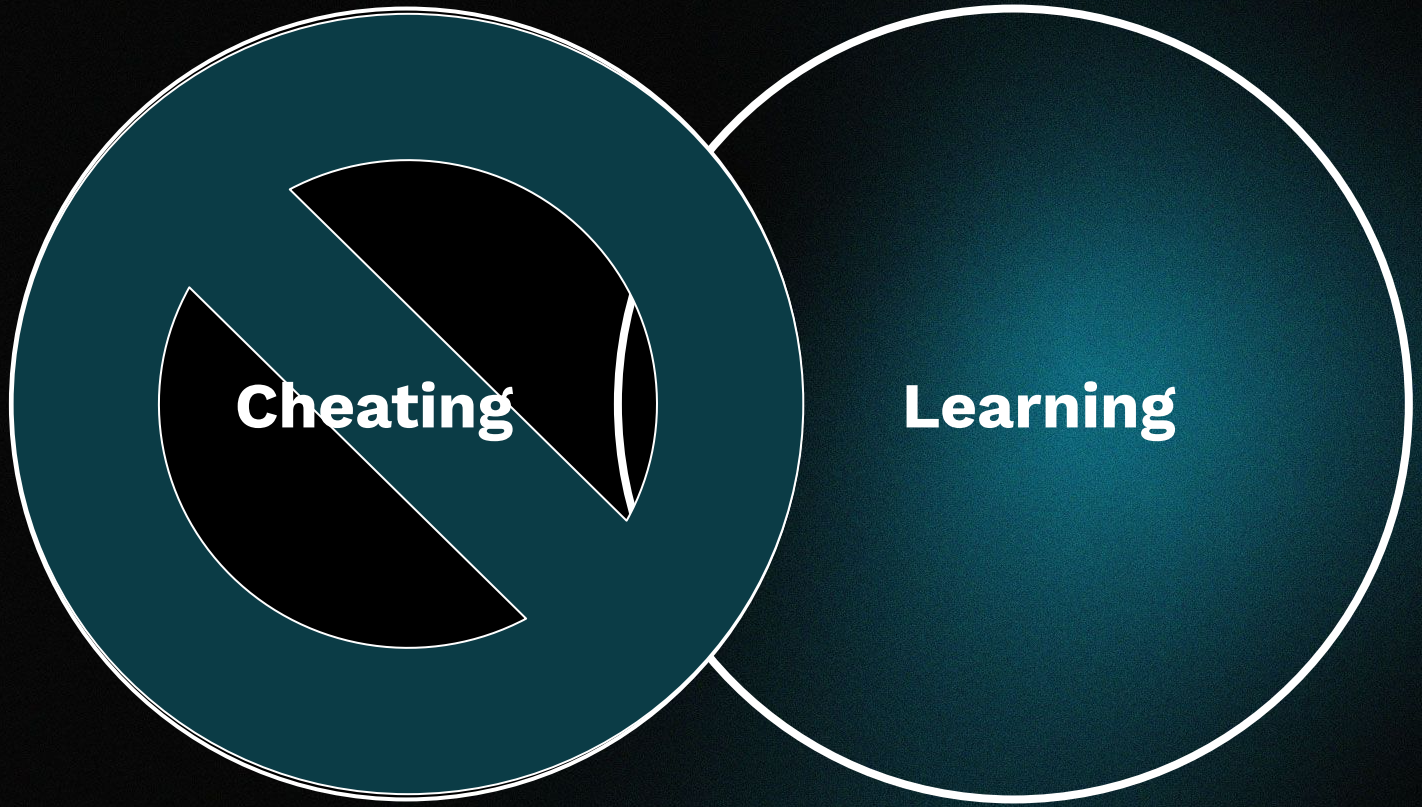
GAMEHACKING VILLAGE V1.0

DEFCON

whoami : Julian Dunning

- **Offensive Security**
- **Co-founded Truffle Security**
  - TruffleHog - open source secrets scanning
- **Statistical based password cracking**
  - Hob0rules: hob064, d3adhob0
- **Forbes 30 under 30**
- **Founder of GameHacking.GG**
  - New GameHacking DEFCON village




Cheating
Learning

Why Game Hacking?

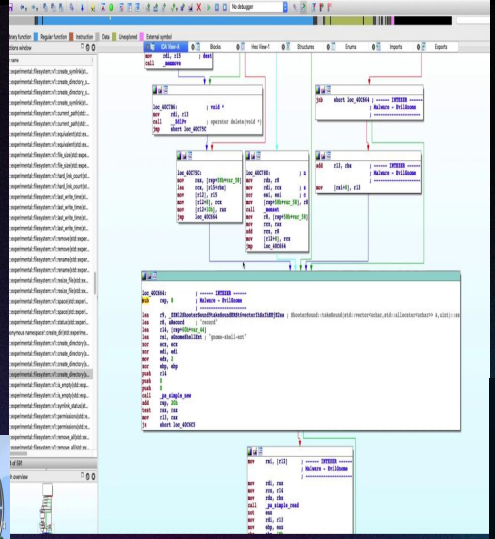




Game Logic Exploits (Speed Running)



Modding



Memory Hacking & Reverse Engineering



Anti-Cheat

Fastest time to complete



(2023) 3m 19s



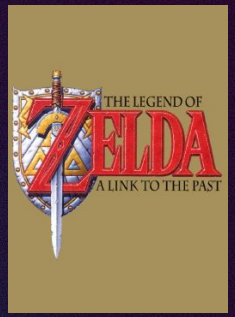
(2011) 7m 1s



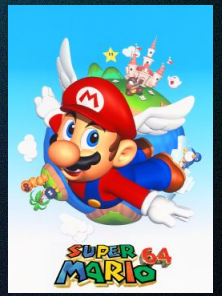
(2017) 22m 58s



(2022) 3m 56s



(1991) 1m 28s



(1996) 6m 15s

Newer == Complicated == Exploitable



(2023) 3m 19s



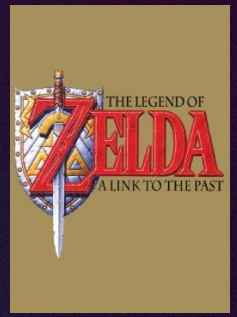
(2011) 7m 1s



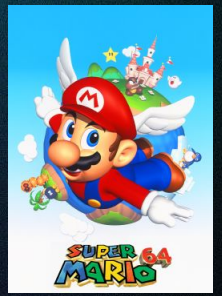
(2017) 22m 58s



(2022) 3m 56s



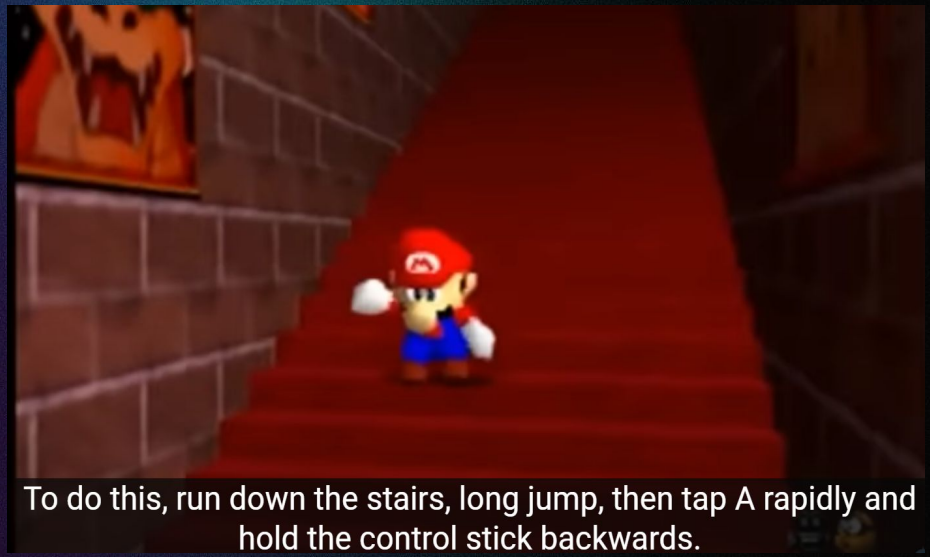
(1991) 1m 28s



(1996) 6m 15s

Game Logic Exploitation Examples





SHADOW BOXING:

1. Box glitch



2. “Betray” your ally



3. Coffin your ally in box



4. Light box on fire



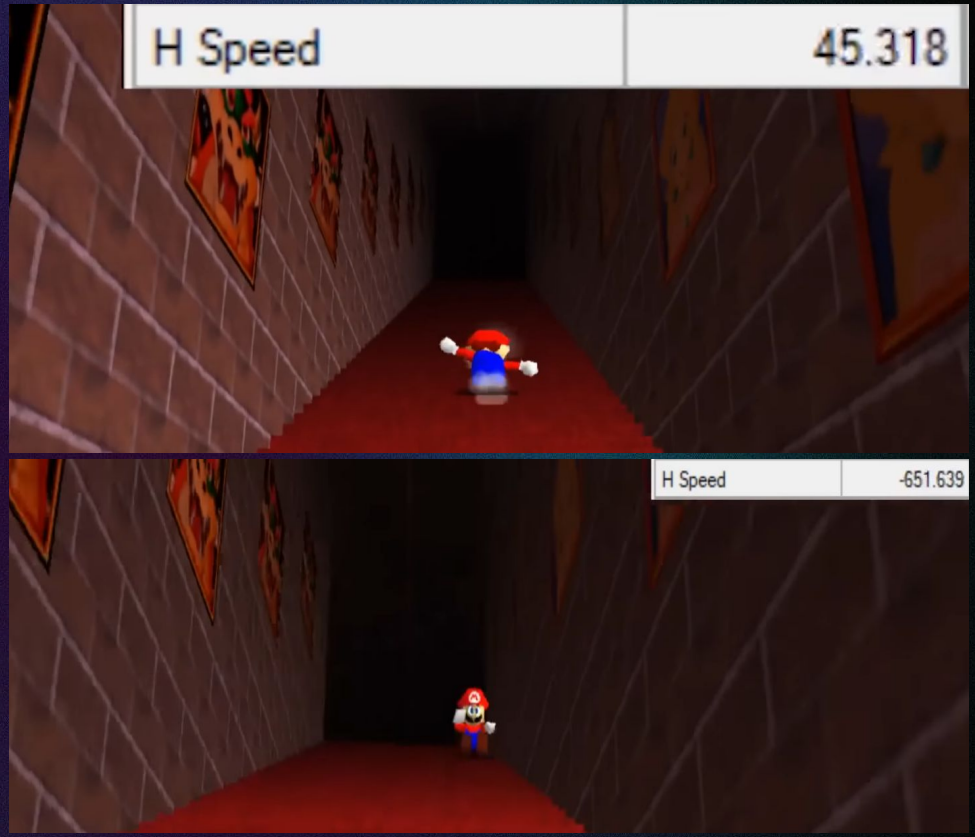
5. Throw into void



6. Profit?






H Speed
45.318
H Speed
-651.639

Is this more than fun and games?



Engineering for efficiency

+

Dexterity to perfectly exploit

+

Hunting of **vulnerabilities**

+

FREE

These bugs in Multiplayer games?



Modding









Modding

Add features you want:

- Quality of Life
- Localization
- Replace all models
- Arachnophobia?



Modding

Extend the game:

- Make your own DLC
- Add new levels, enemies, etc.
- Shoot car from pistol?



Modding

Make new games:

- **Counter Strike** = Half life mod
- **DOTA** = Warcraft mod
- **DOTA** -> League of Legends



Modding



Fortnight = ArmA3 mod -> Players Unknown Battlegrounds ->

Fortnight pivot

Modding

THESE ARE THE MOST POPULAR GAMES IN THE WORLD



Logic Bugs -> Active Exploits

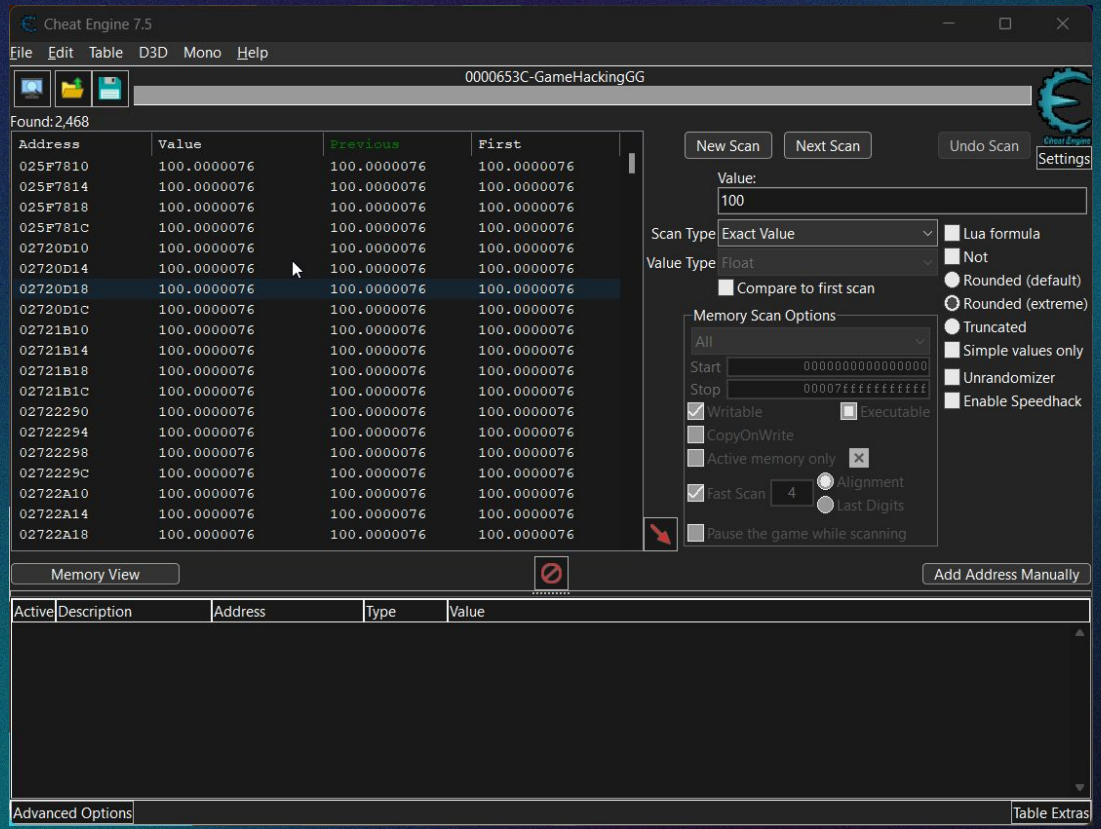


Memory Hacking





Memory Hacking

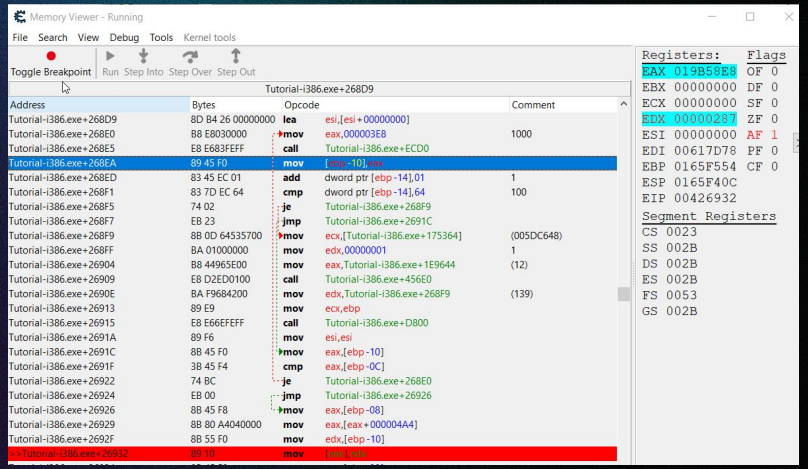




Memory Hacking

- Low barrier to entry
- Quick time to value
- Implications for non-games





Online Defense??



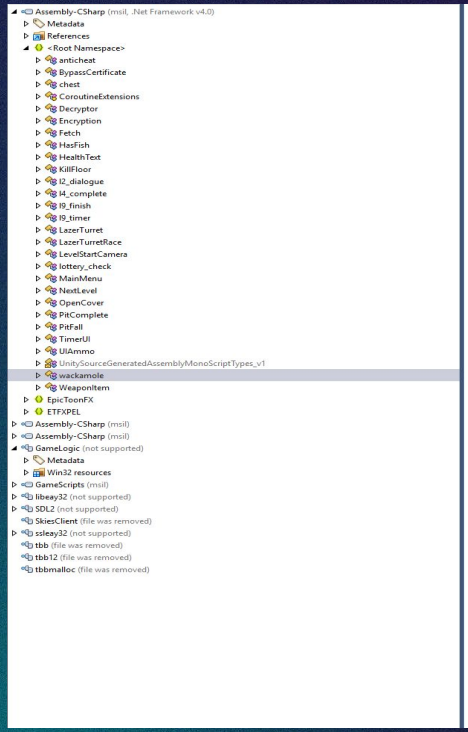
- Server Authoritativeness
- Logical / malicious checks
- Check for “cheat” programs

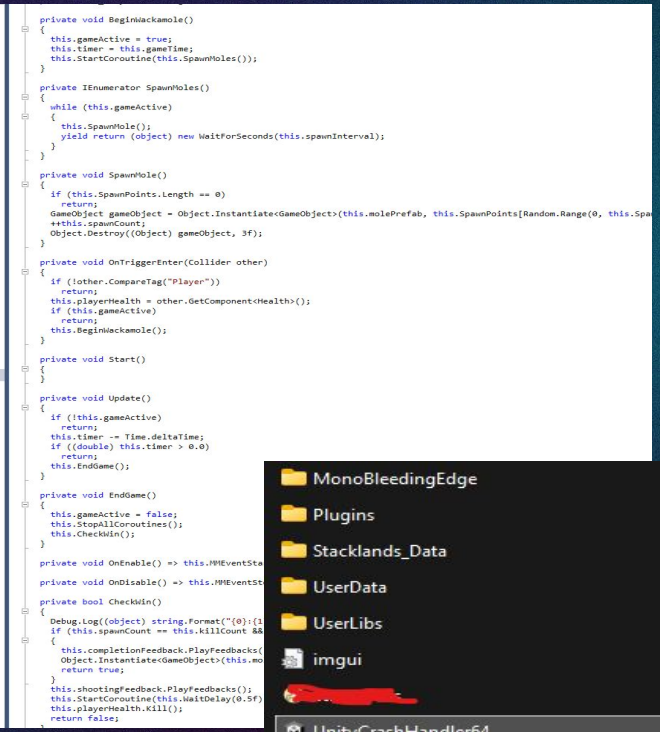
Reverse Engineering

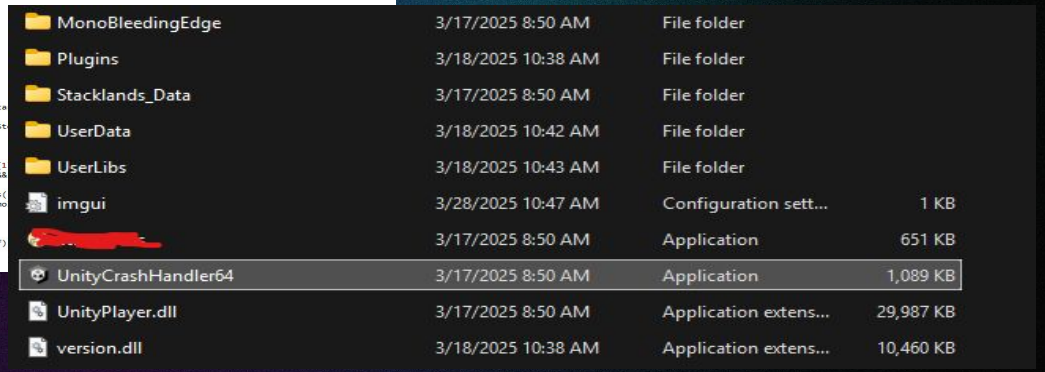


- Know how things work!
- Critical skill for all things security
- It’s fun interactable puzzle
- **(It’s legal)**

“Reverse Engineering”







Unity: Decompile DLLs

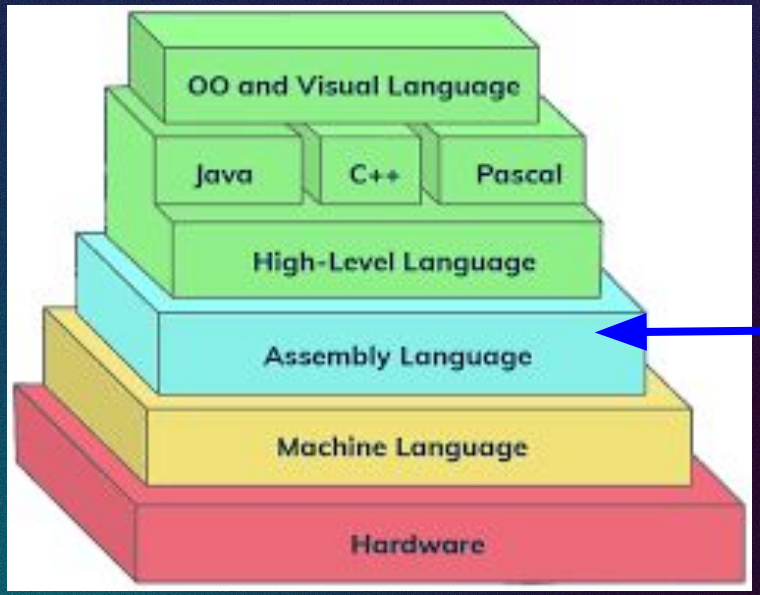
ILSpy / Dotpeek

Reverse Engineering



- Hidden Levels?
- Unused code/ assets

Reverse Engineering





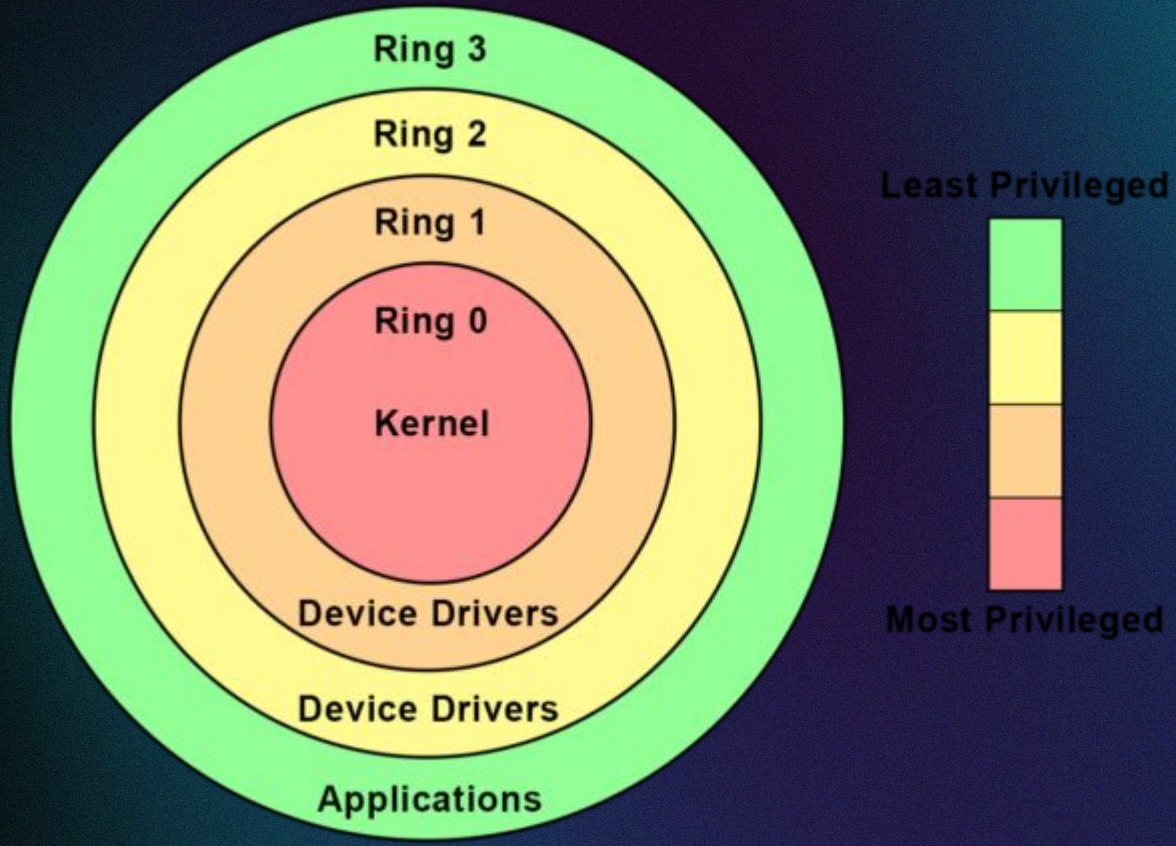
Anti-Cheat?



Anti-Cheat

- Similar attack and defense as Malware and Anti-Virus
- External cheats
- Internal cheats
- Kernel level cheats
- Hardware cheats

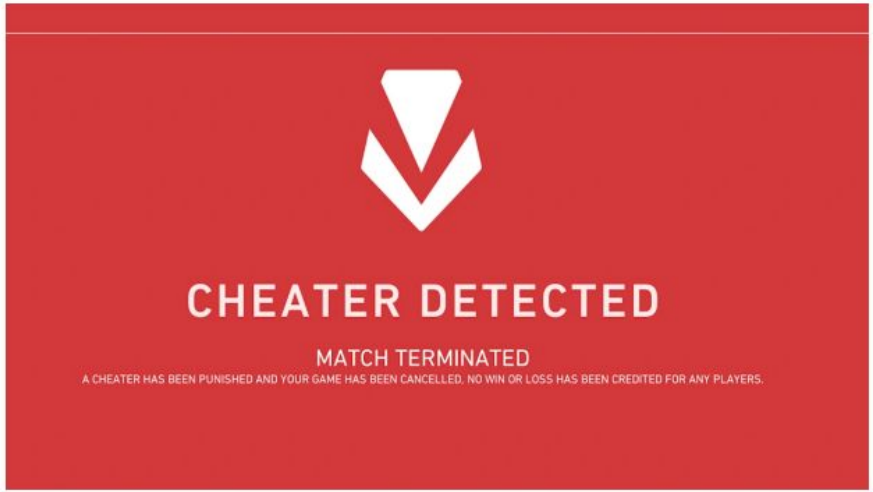



Ring 3
Ring 2
Ring 1
Ring 0
Kernel
Device Drivers
Device Drivers
Applications
Least Privileged
Most Privileged

Riot Games Offers 100k Bounty to Hackers

Riot Games is offering bounties of up to $100,000 to hackers who can crack its Vanguard anti-cheat. Here's what we know.

Gabby DeSena | Nov 27, 2024



Kernel Anti-Cheat Problems

- Trust the developer?
- Self-sign your own cheat driver
- Abuse vulnerable signed drivers
- Mouse and keyboard drivers
- Live Apex professional tournament

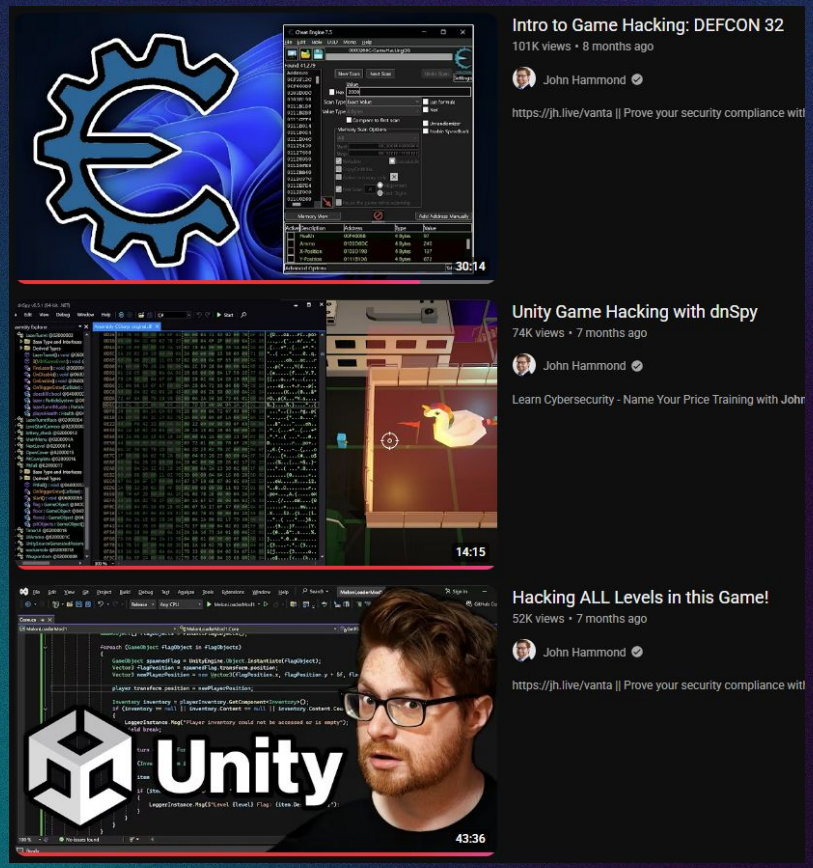


Game Hacking Village
DEFCON 33

- Hacker Vs. Hacker Olympics
- Minecraft Coding Puzzles
- Advanced Modding Workshop
- Mobile Game Hacking
- Game Hacking 101 Intro Game
- Gaming Bug Bounty Challenge



Learn the basics by playing



- Free to download/play @

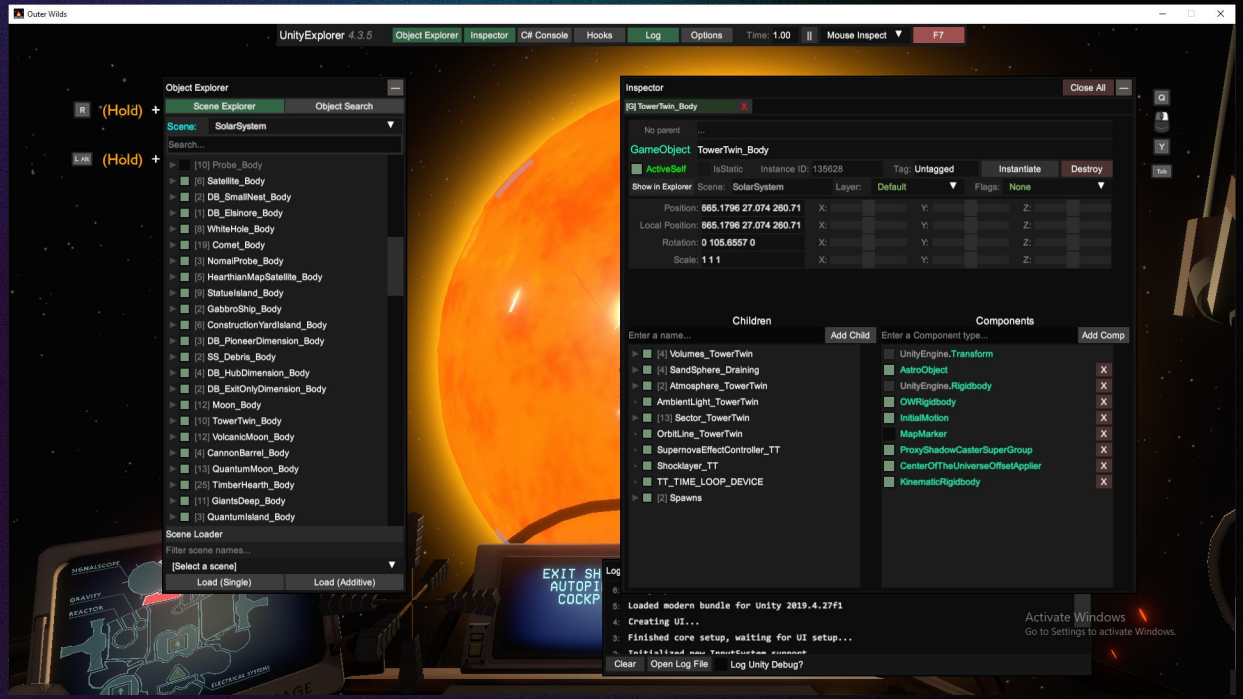
  gamehacking.gg

- Or watch the YouTube Videos

Game Hacking @ DEFCON

- True easy mode
- See the Matrix
- **Unity Explorer + Melon Loader**

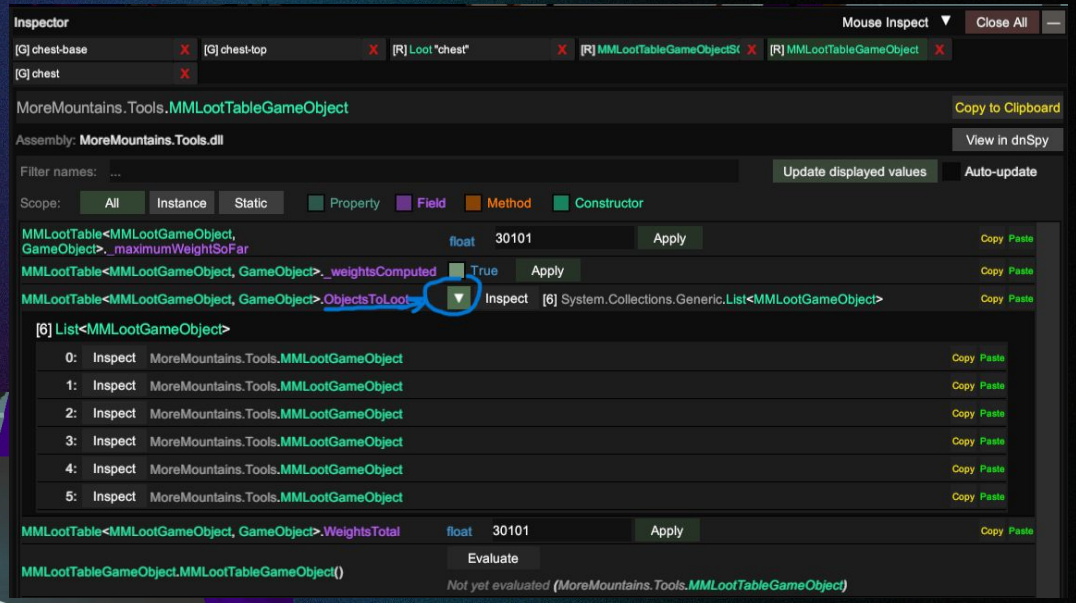




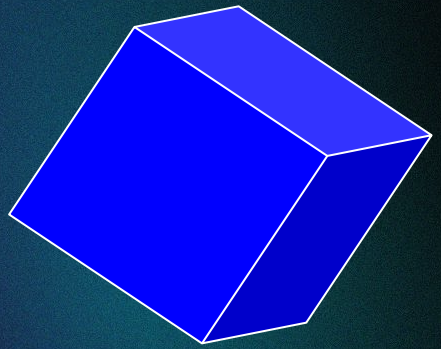
Game Hacking @ DEFCON

- “Gotcha” lottery hack





OpSec Challenges



- Randomly rotate invisible cube
- Hash rotation vector (X, Y, Z)
- Use that hash as encryption key
- Good enough? - GameHackingGG Cracking Obfuscation

THANK YOU

Contact: **Julian@gamehacking.gg**

Website: **GameHacking.GG**

Discord: **See website (JOIN US)**