

# Game Hacking 101

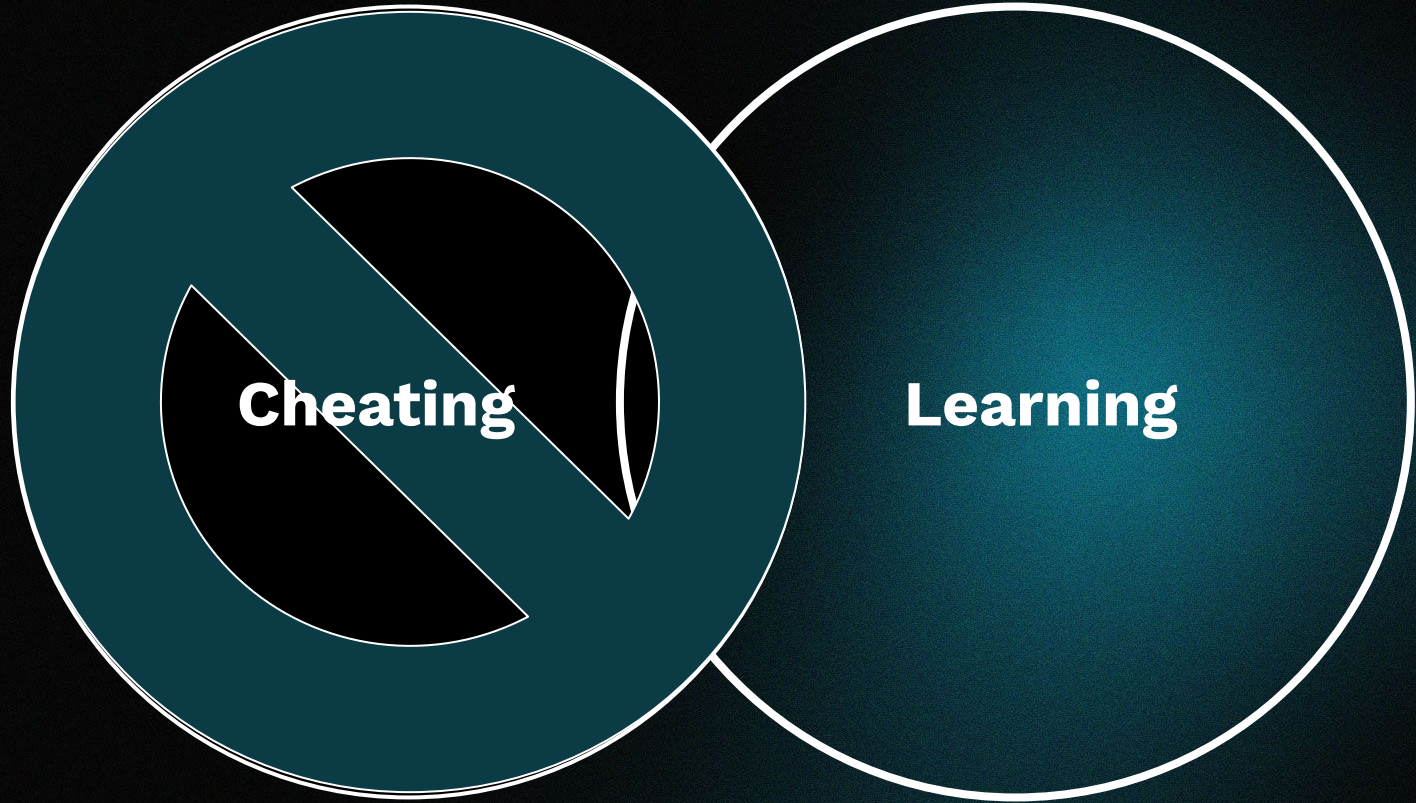
Julian Dunning



# 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





# Why Game Hacking?





# Fastest time to complete



(2023) 3m 19s



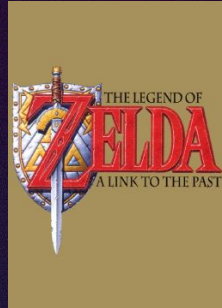
(2011) 7m 1s



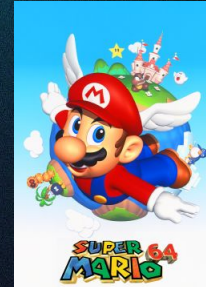
(2017) 22m 58s



(2022) 3m 56s



(1991) 1m 28s



(1996) 6m 15s

# Newer == Complicated == Exploitable



(2023) 3m 19s



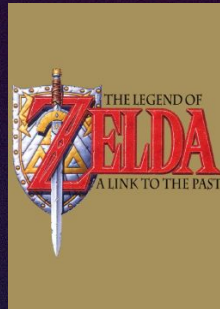
(2011) 7m 1s



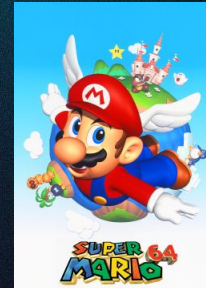
(2017) 22m 58s



(2022) 3m 56s

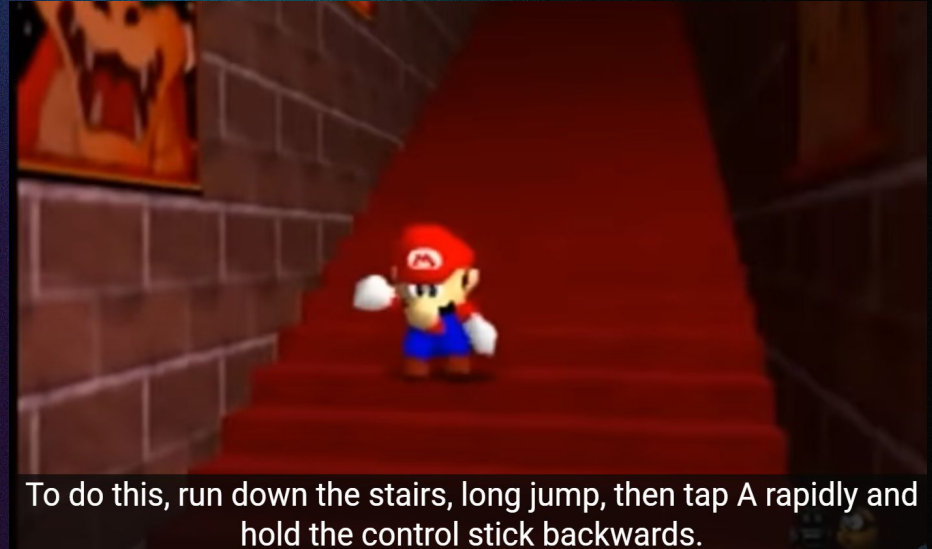


(1991) 1m 28s



(1996) 6m 15s

# Game Logic Exploitation Examples



To do this, run down the stairs, long jump, then tap A rapidly and hold the control stick backwards.

# SHADOW BOXING:

## 1. Box glitch



## 2. "Betray" your ally



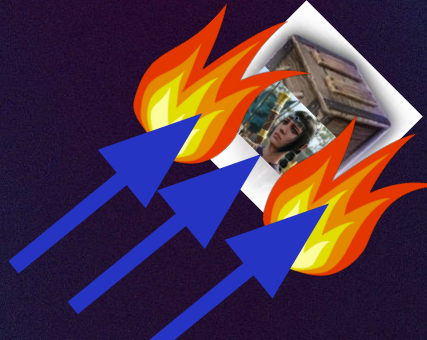
## 3. Coffin your ally in box



## 4. Light box on fire

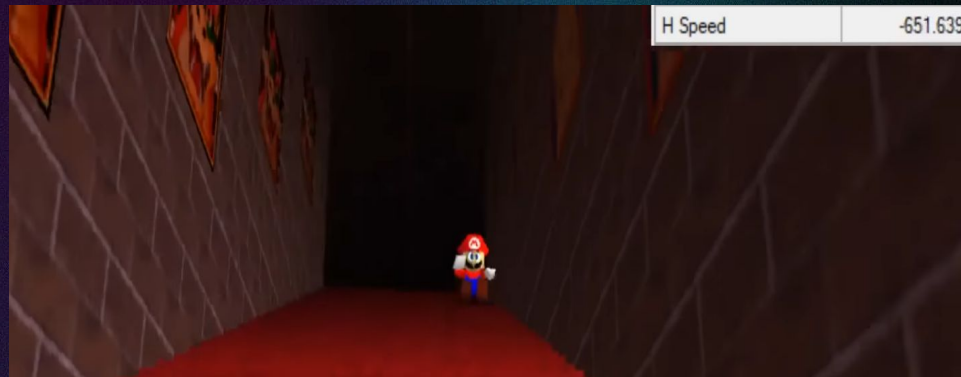
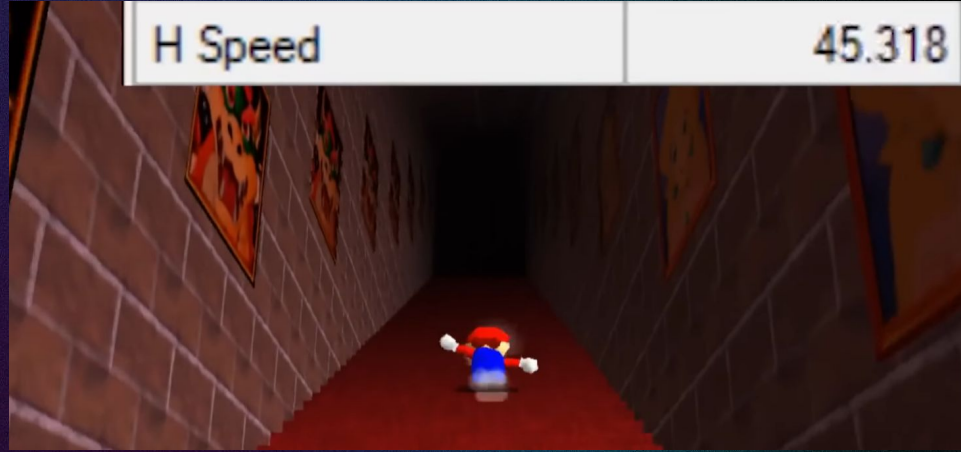


## 5. Throw into void



## 6. Profit?







**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\*

STEAMCHARTS *An ongoing analysis of Steam's concurrent players.*

Top Games By Current Players

[Next page](#)

Name	Current Players	Last 30 Days	Peak Players	Hours Played
<b>League of Legends - 180,000,000</b>				
1. Counter-Strike 2	1,382,545		1,811,827	777,810,415
<b>Fortnight - 996,000</b>				
2. Dota 2	602,140		630,716	292,355,848
3. PUBG: BATTLEGROUNDS	484,571		861,598	241,094,233

# Logic Bugs -> Active Exploits



# Memory Hacking



In order to get this box you need to just keep hitting it, so lets see what happens when I do that.





# Memory Hacking

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



Memory Viewer - Running

file Search View Debug Tools Kernel tools

Toggle Breakpoint Run Step Into Step Over Step Out

Address	Bytes	Opcode	Comment
Tutorial-1386.exe+268D9	8D 84 26 00000000	lea esi,[esi+00000000]	
Tutorial-1386.exe+268E0	88 E8030000	hmov eax,000003E8	1000
Tutorial-1386.exe+268E5	E8 E683FEFF	call Tutorial-1386.exe+ECDD	
Tutorial-1386.exe+268EA	89 45 F0	mov [edi+10],eax	
Tutorial-1386.exe+268ED	83 45 EC 01	add dword ptr [ebp-14],01	1
Tutorial-1386.exe+268F1	83 7D EC 64	cmp dword ptr [ebp-14],64	100
Tutorial-1386.exe+268F5	74 02	je Tutorial-1386.exe+268F9	
Tutorial-1386.exe+268F7	EB 23	jmp Tutorial-1386.exe+2691C	
Tutorial-1386.exe+268F9	88 0D 64535700	hmov ecx,[Tutorial-1386.exe+175364]	(005DC648)
Tutorial-1386.exe+268FF	BA 01000000	mov edx,00000001	1
Tutorial-1386.exe+26904	88 44965E00	mov eax,Tutorial-1386.exe+1E9644	(12)
Tutorial-1386.exe+26909	EB D2ED0100	call Tutorial-1386.exe+456E0	
Tutorial-1386.exe+2690E	8A F9684200	mov ecx,Tutorial-1386.exe+268F9	(139)
Tutorial-1386.exe+26913	89 E9	mov ecx,ebp	
Tutorial-1386.exe+26915	E8 E6EFFFFF	call Tutorial-1386.exe+D800	
Tutorial-1386.exe+2691A	89 F6	mov esi,esi	
Tutorial-1386.exe+2691C	88 45 F0	hmov eax,[ebp-10]	
Tutorial-1386.exe+2691F	3B 45 F4	cmp eax,[ebp-0C]	
Tutorial-1386.exe+26922	74 BC	je Tutorial-1386.exe+268E0	
Tutorial-1386.exe+26924	EB 00	jmp Tutorial-1386.exe+26926	
Tutorial-1386.exe+26926	88 45 F8	hmov eax,[ebp-08]	
Tutorial-1386.exe+26929	8B 80 A4040000	mov eax,[eax+000004A4]	
Tutorial-1386.exe+2692F	8B 55 F0	mov edx,[ebp-10]	
Tutorial-1386.exe+26932	89 10	mov [edi],eax	

Registers: Flags

EAX	013B58E8	OF	0
EBX	00000000	DF	0
ECX	00000000	SF	0
ESI	00000000	AF	1
EDI	00617D78	PF	0
EBP	0165F554	CF	0
ESP	0165F40C		
EIP	00426932		

Segment Registers

CS	0023
SS	002B
DS	002B
ES	002B
FS	0053
GS	002B

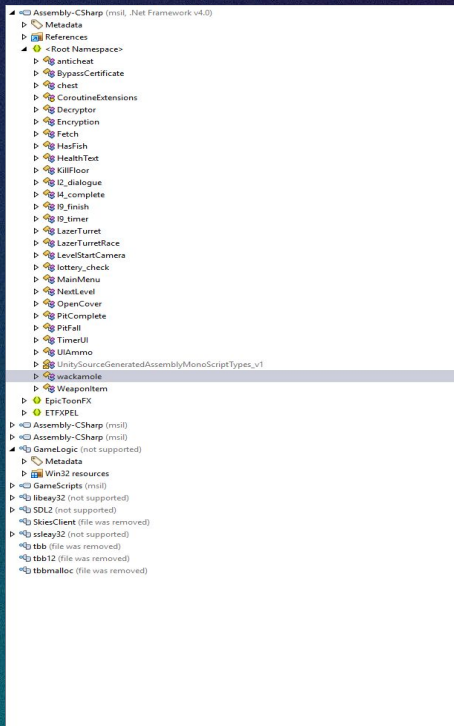


# Reverse Engineering



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

# “Reverse Engineering”



```
private void Beginwackamole()
{
    this.gameActive = true;
    this.timer = this.gameTime;
    this.StartCoroutine(this.SpawnMole());
}

private IEnumerator SpawnMoles()
{
    while (this.gameActive)
    {
        this.SpawnMole();
        yield return (object) new WaitForSeconds(this.spawnInterval);
    }
}

private void SpawnMole()
{
    if (this.SpawnPoints.Length == 0)
        return;
    GameObject gameObject = Object.Instantiate<GameObject>(this.molePrefab, this.SpawnPoints[Random.Range(0, this.SpawnPoints.Length)]);
    Object.Destroy<GameObject>(gameObject, 3f);
}

private void OnTriggerEnter(Collider other)
{
    if (other.CompareTag("Player"))
        return;
    this.playerHealth = other.GetComponent<Health>();
    if (this.gameActive)
        return;
    this.Beginwackamole();
}


private void Start()
{
}

private void Update()
{
    if (!this.gameActive)
        return;
    this.timer -= Time.deltaTime;
    if ((double) this.timer > 0.0)
        return;
    this.EndGame();
}

private void EndGame()
{
    this.gameActive = false;
    this.StopAllCoroutines();
    this.CheckWin();
}

private void OnEnable() => this.HPEvents;
private void OnDisable() => this.HPEvents;
private bool CheckWin()
{
    Debug.Log((object) string.Format("{0}: I",
    if (this.spawnCount == this.killCount)
    {
        this.completionFeedback.PlayFeedback<GameObject>(this.molePrefab);
        return true;
    }
    this.shootingFeedback.PlayFeedback();
    this.StartCoroutine(this.WaitDelay(0.5f));
    this.playerHealth.Kill();
    return false;
}
}
```

## Unity: Decompile DLLs ILSpy / Dotpeek

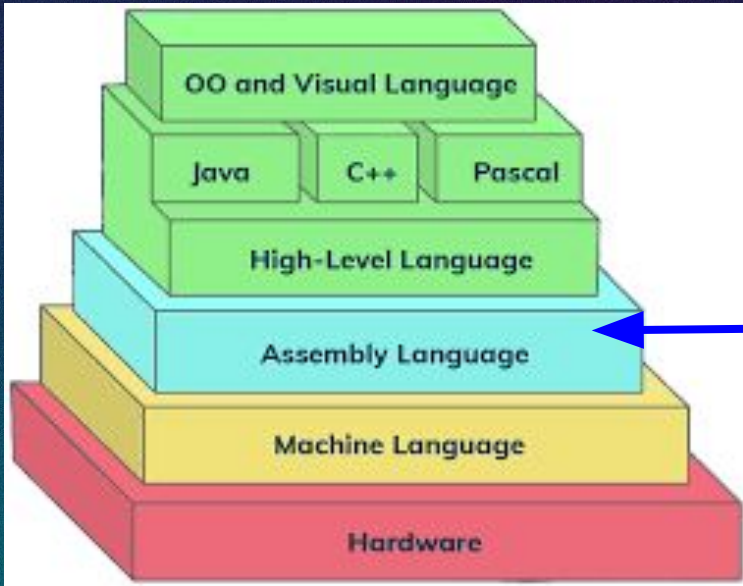
MonoBleedingEdge	3/17/2025 8:50 AM	File folder	
Plugins	3/18/2025 10:38 AM	File folder	
Stacklands_Data	3/17/2025 8:50 AM	File folder	
UserData	3/18/2025 10:42 AM	File folder	
UserLibs	3/18/2025 10:43 AM	File folder	
imgui	3/28/2025 10:47 AM	Configuration sett...	1 KB
	3/17/2025 8:50 AM	Application	651 KB
UnityCrashHandler64	3/17/2025 8:50 AM	Application	1,089 KB
UnityPlayer.dll	3/17/2025 8:50 AM	Application extens...	29,987 KB
version.dll	3/18/2025 10:38 AM	Application extens...	10,460 KB

# Reverse Engineering



- Hidden Levels?
- Unused code/ assets

# Reverse Engineering



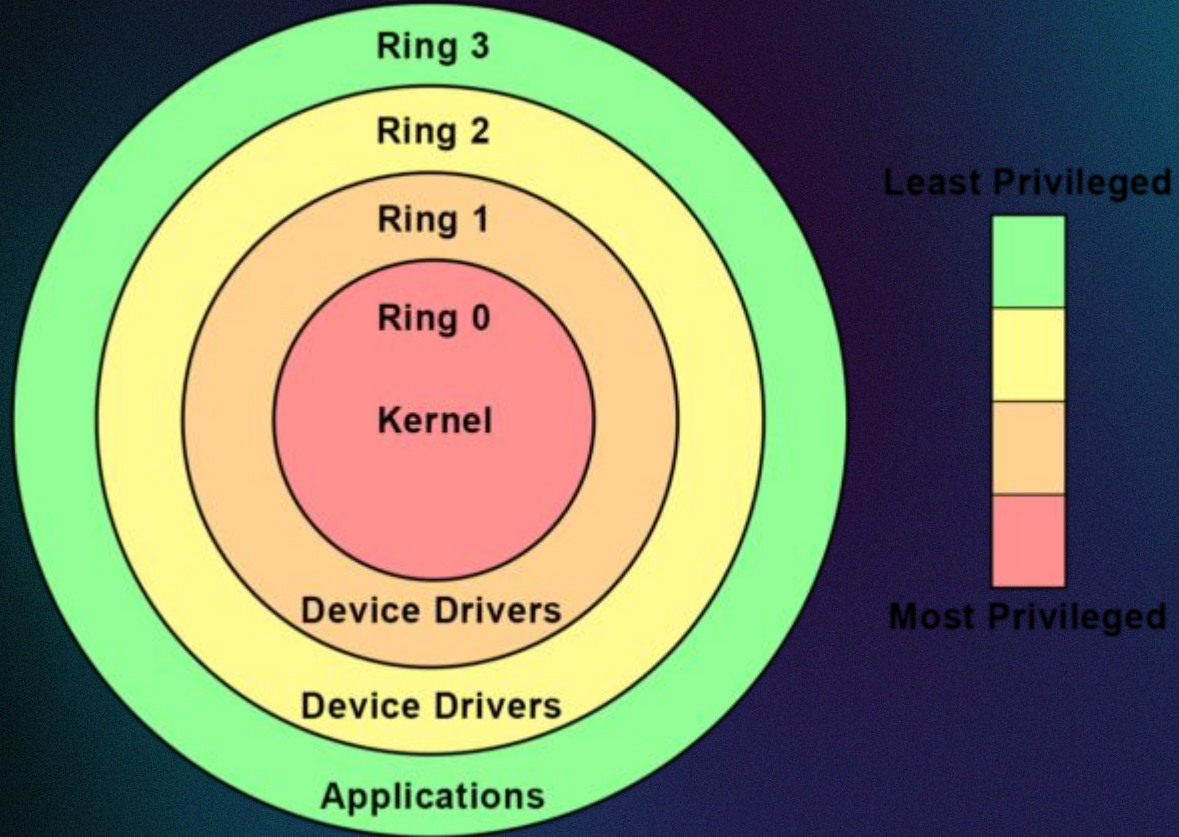
# Anti-Cheat?



# Anti-Cheat

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

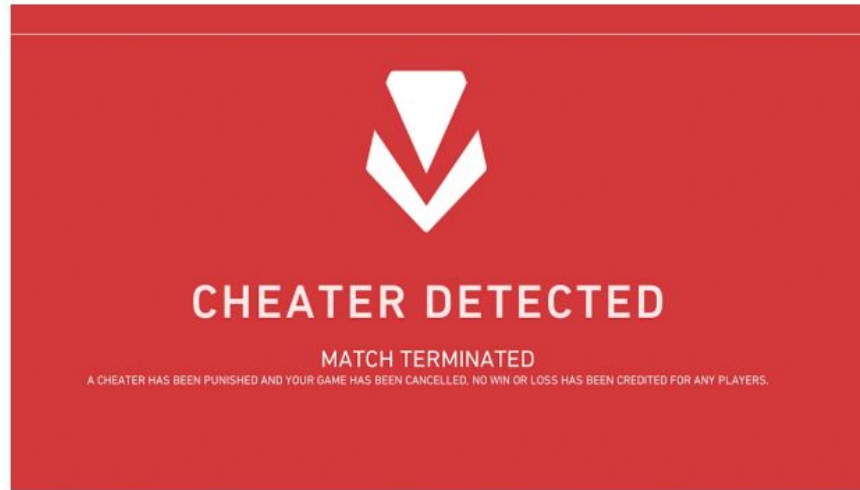




## Riot Games Offers 100k Bounty to Hackers

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



**Intro to Game Hacking: DEFCON 32**  
101K views • 8 months ago  
John Hammond  
<https://jh.live/vanta> | Prove your security compliance with



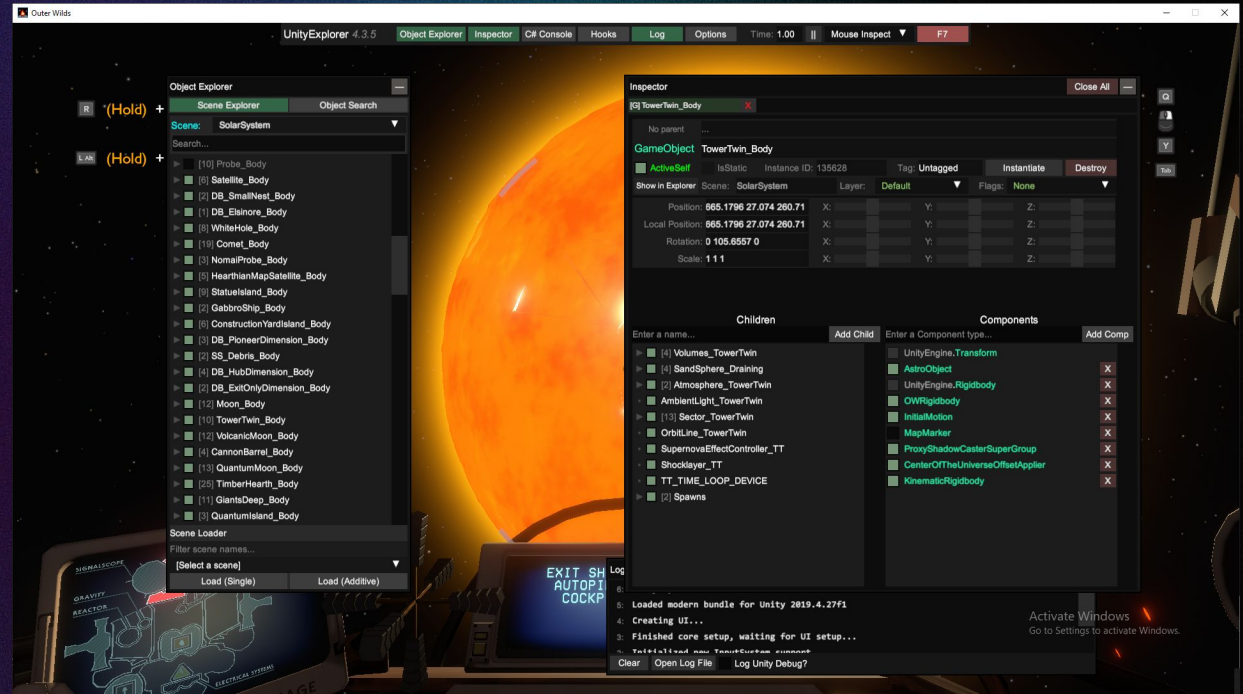
**Unity Game Hacking with dnSpy**  
74K views • 7 months ago  
John Hammond  
Learn Cybersecurity - Name Your Price Training with John



**Hacking ALL Levels in this Game!**  
52K views • 7 months ago  
John Hammond  
<https://jh.live/vanta> | Prove your security compliance with

# Game Hacking @ DEFCON

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



# Game Hacking @ DEFCON

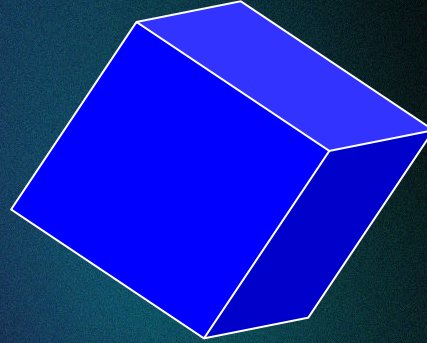
- “Gotcha” lottery hack

A screenshot of a game hacking tool interface. The Inspector window shows the following details:

- Assembly: MoreMountains.Tools.dll
- Filter names: ...
- Scope: All Instance Static Property Field Method Constructor
- MMLOotTable<MMLootGameObject, GameObject>.\_maximumWeightSoFar: float 30101 Apply Copy Paste
- MMLOotTable<MMLootGameObject, GameObject>.\_weightsComputed: True Apply Copy Paste
- MMLOotTable<MMLootGameObject, GameObject>.ObjectsToLoot: [6] System.Collections.Generic.List<MMLootGameObject> Inspect Copy Paste
- [6] List<MMLootGameObject>
- 0: Inspect MoreMountains.Tools.MMLootGameObject Copy Paste
- 1: Inspect MoreMountains.Tools.MMLootGameObject Copy Paste
- 2: Inspect MoreMountains.Tools.MMLootGameObject Copy Paste
- 3: Inspect MoreMountains.Tools.MMLootGameObject Copy Paste
- 4: Inspect MoreMountains.Tools.MMLootGameObject Copy Paste
- 5: Inspect MoreMountains.Tools.MMLootGameObject Copy Paste
- MMLOotTable<MMLootGameObject, GameObject>.WeightsTotal: float 30101 Apply Copy Paste
- MMLOotTableGameObject.MMLootTableGameObject(): Evaluate Not yet evaluated (MoreMountains.Tools.MMLootTableGameObject)

# 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](mailto:Julian@gamehacking.gg)

Website: **GameHacking.GG**

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