

Leaderboard Security

Levi D. Smith
Knox Game Design
May 2020

Overview

- Someone added a score not generated by the game to the leaderboard
- Not really malicious, but exposed vulnerability in the leaderboard system
- I never had an interest in hacking, but I need to be aware of how it can be used to exploit games and leaderboards
- It does mean that people are at least taking the time to come to my site and look at the code

KNOX
GAME
DESIGN

First detection



















Chicken Little	
Longest Time	
LD Hacker!	16:40.00
James	0:49.11
frenchie	0:36.73
James	0:36.52
James	0:36.51
gwheel	0:36.19
gwheel	0:36.11
jcmonkey	0:36.03
knason	0:35.89
gwheel	0:35.79
gwheel	0:35.76
Snail	0:35.76
jcmonkey	0:35.00
James	0:34.94
name	0:34.66
record	0:34.11
LMB	0:34.09
jcmonkey	0:34.02
Snail	0:33.91
gwheel	0:33.39

Chicken Little Leaderboard	
Longest Time	
LD Hacker!	16:40.00
James	0:49.11
frenchie	0:36.73
James	0:36.52

- Added a value of 100000 to the leaderboard
- Time scores are in hundredths of a second
- 16 minutes, 40 seconds
 - $16 * 6000 = 96,000$
 - $40 * 100 = 4,000$
 - $0 * 1 = 0$

KNOX
GAME
DESIGN

Checking the Database

<input type="checkbox"/>	 Edit	 Copy	 Delete	510	Slim_Bun	3288	2020-04-28 00:17:53	6651
<input type="checkbox"/>	 Edit	 Copy	 Delete	511	Slim_Bun	1859	2020-04-28 00:18:18	6651
<input type="checkbox"/>	 Edit	 Copy	 Delete	512	woohoo	1538	2020-04-28 00:26:45	6651
<input type="checkbox"/>	 Edit	 Copy	 Delete	513	LD Hacker!	100000	2020-04-28 00:32:08	6651
<input type="checkbox"/>	 Edit	 Copy	 Delete	514	knason	3109	2020-04-28 03:46:02	6651
<input type="checkbox"/>	 Edit	 Copy	 Delete	515	knason	3589	2020-04-28 03:46:58	6651

Checking the web logs

Downloaded the Apache web server logs from CPanel

```
73.202.225.72 - - [28/Apr/2020:00:32:07 -0700] "GET /scores/AddScore.php?game=6651&name=LD+Hacker%21&score=100000&hash=6f44c6c9f184e9233a45454568e47e2a HTTP/1.1" 200 158 "https://levidsmith.com/web-games/chicken-little/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36"
```

Obviously not a brute force hack

How did they calculate the hash value without the key?

```
hBot/6~b1; +http://www.semrush.com/bot.html)"
73.202.225.72 - - [28/Apr/2020:00:26:45 -0700] "GET /scores/AddScore.php?game=6651&name=woohoo&score=1538&hash=32f7bccf364a1efe2d90d4ed3afe6a HTTP/2.0" 200 153 "https://levidsmith.com/web-games/chicken-little/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36"
73.202.225.72 - - [28/Apr/2020:00:26:47 -0700] "GET /scores/TopScores.php?game=6651 HTTP/2.0" 200 97 "https://levidsmith.com/web-games/chicken-little/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36"
```

If there was no record in the web logs, then I would be worried (direct access into the database)

GHMC
DESIGN

Tracing


Home | Internet tools InfoByIp.com

73.202.225.72 Get info

IP: 73.202.225.72

IP data

Domain	c-73-202-225-72.hsd1.ca.comcast.net
ISP	COMCAST-7922
ASN	7922
Tools	whois ping traceroute mtr dns



Geographical Data

Country	United States (US)
State/region	California
City	San Mateo

May not be an accurate location if they used a VPN

```
C:\Users\gatec>tracert 73.202.225.72
```

```
Tracing route to c-73-202-225-72.hsd1.ca.comcast.net [73.202.225.72]  
over a maximum of 30 hops:
```

```
 1  <1 ms  <1 ms  <1 ms  [REDACTED]  
 2  10 ms  10 ms  12 ms  [REDACTED]  
 3  10 ms  11 ms  14 ms  [REDACTED]  
 4  11 ms  17 ms  28 ms  xe-0-0-0-0-sur01.bridgewater.tn.knox.comcast.net [68.85.171.153]  
 5  17 ms  30 ms  21 ms  162.151.95.117  
 6  31 ms  34 ms  30 ms  be-33132-cs03.350ecermak.il.ibone.comcast.net [96.110.42.233]  
 7  29 ms  29 ms  48 ms  be-1311-cr11.350ecermak.il.ibone.comcast.net [96.110.35.10]  
 8  57 ms  53 ms  56 ms  96.110.37.158  
 9  54 ms  54 ms  52 ms  be-12021-cr01.champa.co.ibone.comcast.net [68.86.84.225]  
10  83 ms  78 ms  84 ms  be-11020-cr02.sunnyvale.ca.ibone.comcast.net [68.86.84.9]  
11  76 ms  74 ms  75 ms  be-7922-rar01.santaclara.ca.sfba.comcast.net [68.86.91.74]  
12  78 ms  78 ms  83 ms  po-1-rur01.sanmateo.ca.sfba.comcast.net [68.86.91.74]  
13  76 ms  85 ms  79 ms  96.110.177.74  
14 108 ms  97 ms  98 ms  c-73-202-225-72.hsd1.ca.comcast.net [73.202.225.72]
```

```
Trace complete.
```

```
C:\Users\gatec>
```

See also www.whatsmyip.org

Hashing Method

- MD5 - security issues
- Hash variables are publicly available in the game source code
 - name, score, game ID, key
 - Changing any of these values changes the hash value
- Is Open Source more secure?
 - Closed source - security through obscurity
 - Open source - more mature solutions due to vulnerabilities being found and corrected
- Hash generated on the client (game) side (C#), then verified on the server side (PHP)

1 reference

```
public void doSubmitScore(int iScore) {  
    Debug.Log("doSubmitScore: " + iScore);  
    string strHash = Md5Sum(strName + iScore.ToString() + iGameID.ToString() + strSecretKey);  
    string strURL = "https://levidsmith.com/scores/AddScore.php?game=" + iGameID + "&name=" + www.EscapeURL  
        (strName) +  
        "&score=" + iScore + "&hash=" + strHash;  
    StartCoroutine(submitScore(strURL));  
}
```

KNOX
GAME
DESIGN


```
$name = mysqli_real_escape_string($conn, $_GET['name']);
$score = mysqli_real_escape_string($conn, $_GET['score']);
$game = mysqli_real_escape_string($conn, $_GET['game']);
$hash = $_GET['hash'];

//This is the polite version of our name
$politestring = sanitize($name);

//This is your key. You have to fill this in! Go and generate a
$key = "XXXXXXXXXXXXXXXXXXXX";

//We md5 hash our results.
$expected_hash = md5($name . $score . $game . $secretKey);

//If what we expect is what we have:
if ($expected_hash == $hash) {
    // Here's our query to insert/update scores!
    $query = "INSERT INTO score
```

The logo for KNOX GAME DESIGN is located in the top left corner. It features the word "KNOX" in red, "GAME" in green, and "DESIGN" in blue, all in a pixelated, blocky font.

Verifying the hash

- Calls using an invalid hash parameter will not be inserted into the database

- Use `-n` parameter to suppress newline, which will generate an entirely different hash!

```
$ echo -n knoxgamedesign426651hello | md5sum  
2ea85dbf8123ae1d8bc03e294310c048 *-
```

Example

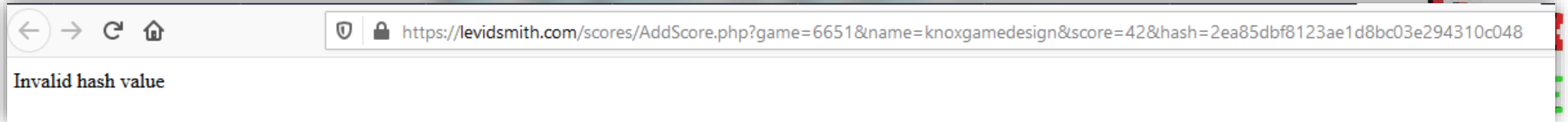
name = knoxgamedesign

score = 42

game = 6651

hash key = hello

hash value = 2ea85dbf8123ae1d8bc03e294310c048



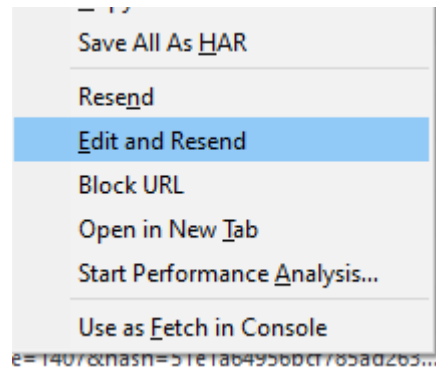
DESIGN

Monitoring network connection

- Firefox > Web Developer > Debugger > Network tab

200	GET	levidsmith.com	AddScore.php?game=6651&name=foo&score=1407&hash=51e1a64956bcf785ad263...	xhr	html	386 B	162 B	278 ms
200	GET	levidsmith.com	TopScores.php?game=6651	xhr	html	340 B	120 B	189 ms
200	GET	levidsmith.com	AddScore.php?game=6651&name=foo&score=1407&hash=51e1a64956bcf785ad263...					
200	GET	levidsmith.com	TopScores.php?game=6651					

Right click > Edit and Resend



Cancel

Send

Method

URL

GET

https://levidsmith.com/scores/AddScore.php?game=6651&name=foo&score=1407&hash=51e1a64956bcf785ad263fd6b90b5bcf

Query String

game=6651
name=foo
score=1407
hash=51e1a64956bcf785ad263fd6b90b5bcf

MD5 reverser

```
$ echo -n newton | md5sum  
da6fa909f1c0188c539feb08d4496eb7 *-
```

```
$ echo -n newton5216651[REDACTED] | md5sum  
aeac9b90aec689ec47ca56ea1aacf5a5 *-
```

MD5

MD5 conversion and reverse lookup

MD5 reverse for da6fa909f1c0188c539feb08d4496eb7

The MD5 hash:

da6fa909f1c0188c539feb08d4496eb7

was successfully reversed into the string:

newton

Feel free to provide some other MD5 hashes you would like to try to reverse.

Reverse a MD5 hash

da6fa909f1c0188c539feb08d4496eb7

Reverse

MD5

MD5 conversion and reverse lookup

MD5 conversion and MD5 reverse lookup

Provided MD5 hash could not be reversed into a string: no reverse string was found.

Reverse a MD5 hash

aeac9b90aec689ec47ca56ea1aacf5a5

Reverse

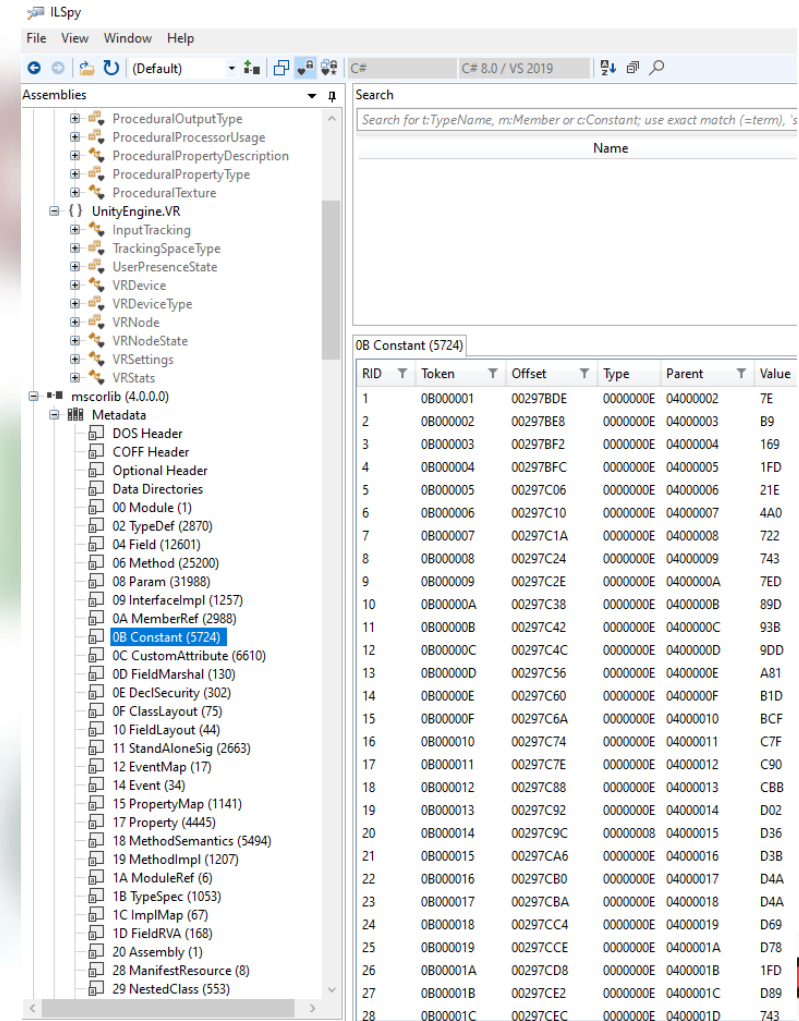
GAME
DESIGN

Unity Decompilation Tools

- ILSpy
- DevXUnity
- uTinyRipper
- dotPeek

ILSpy

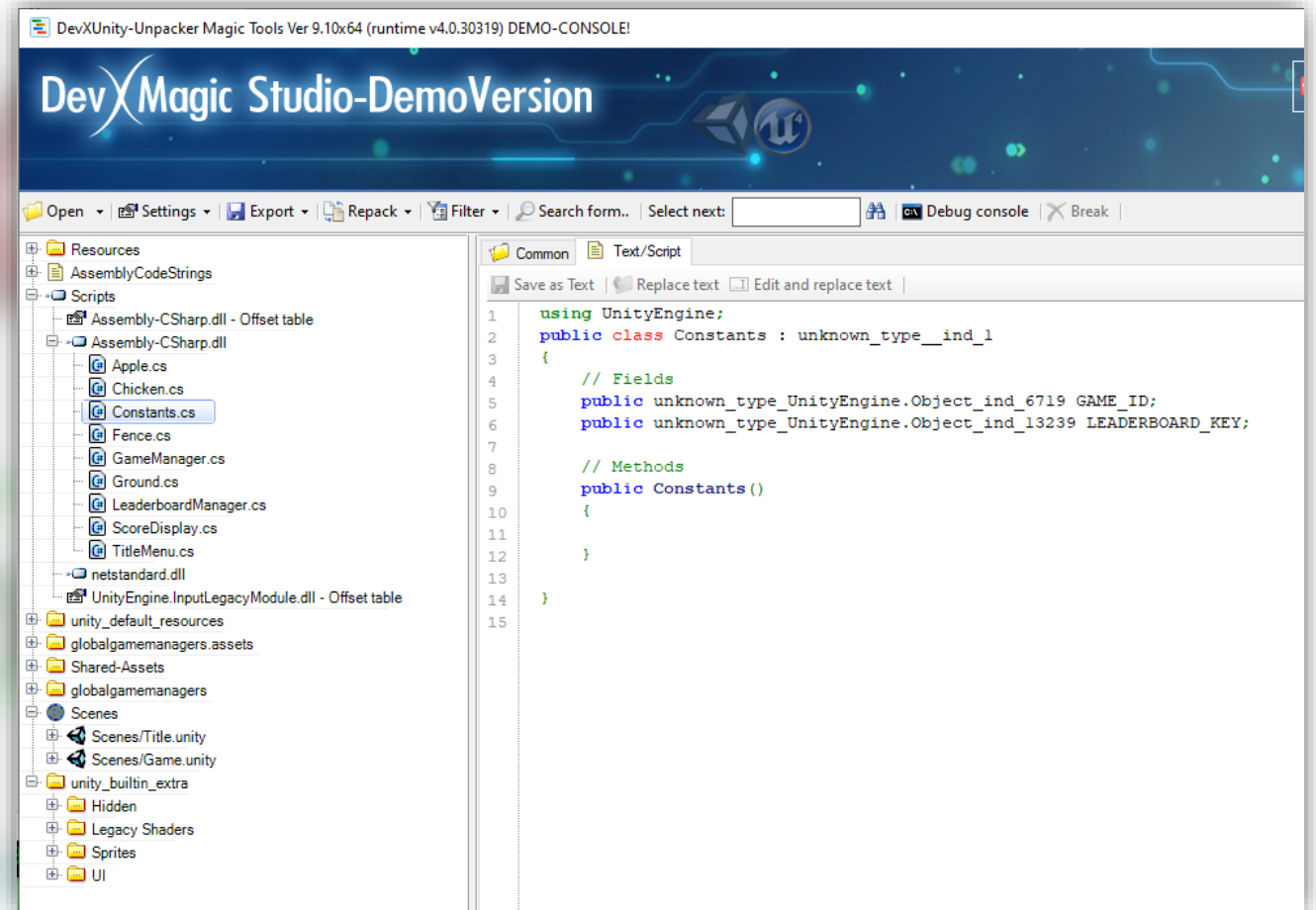
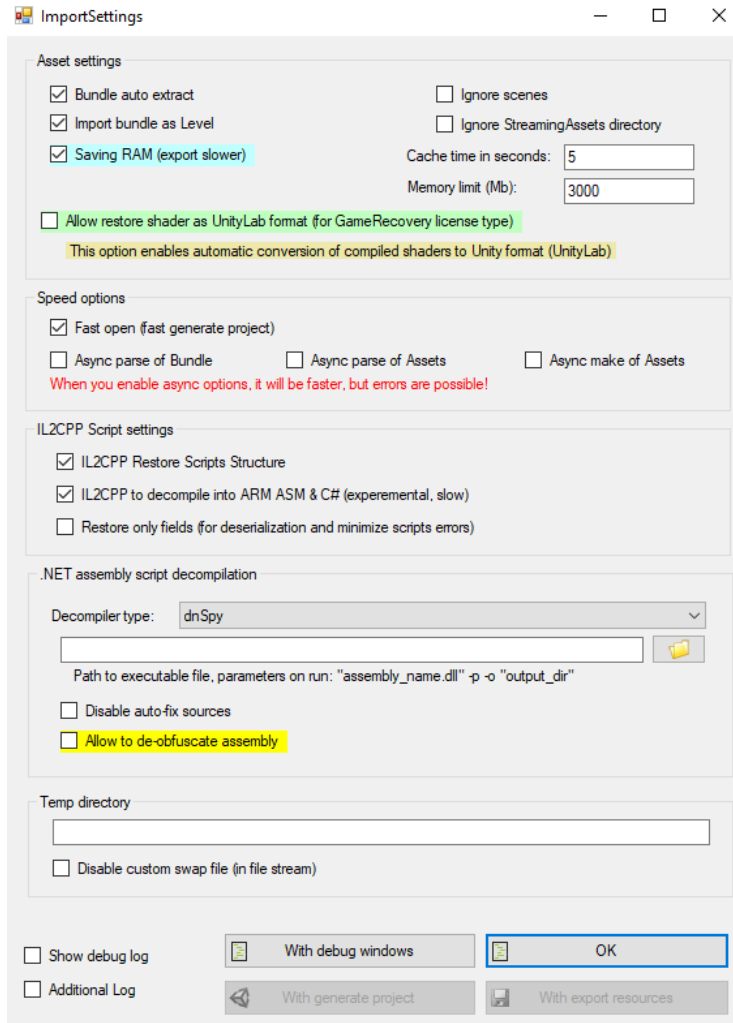
- Unity decompilation tool
- Can be used to look at core Unity files



Status	Meth...	Domain	File	Cause	Type	Transferred	Size
200	GET	levidsmith.c...	ChickenLittleWebGL.wasm.code.unityweb	xhr	vnd....	4.09 MB	4.14 ...

CNOX
GAME
DESIGN

DevXUnity

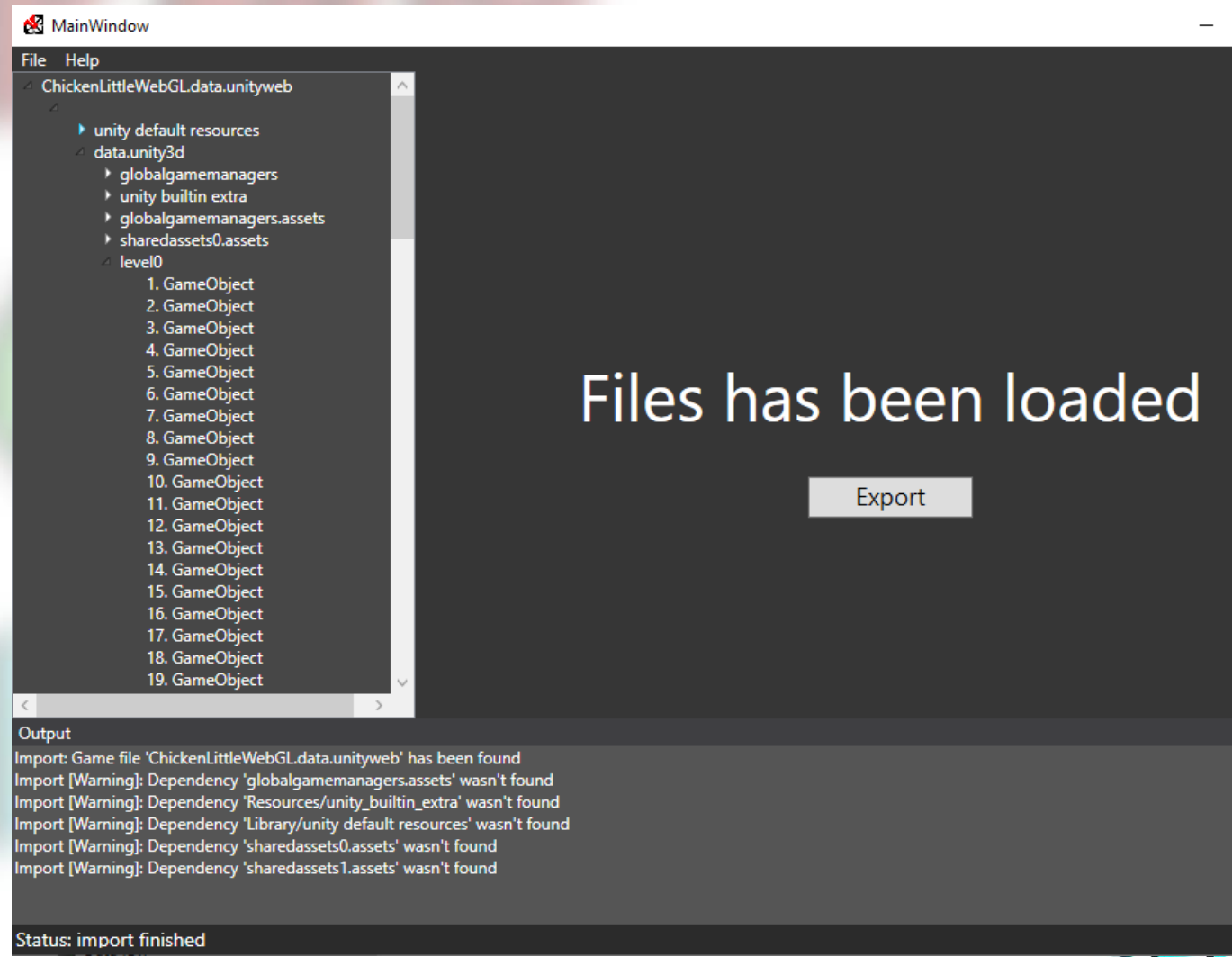
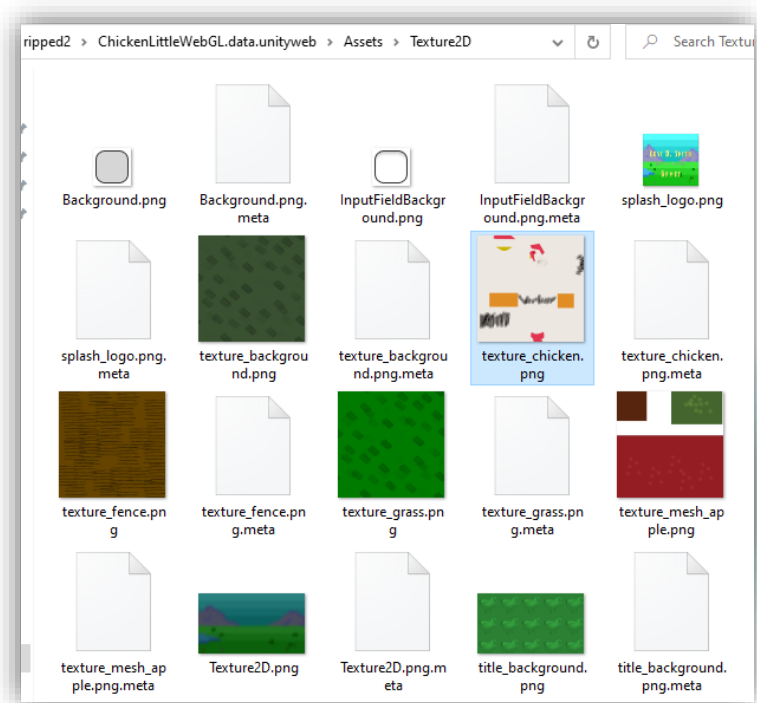


- Able to extract CS files, but could not read constant values
- Shows constant names, but not values

KNOX
GAME
DESIGN

uTinyRipper

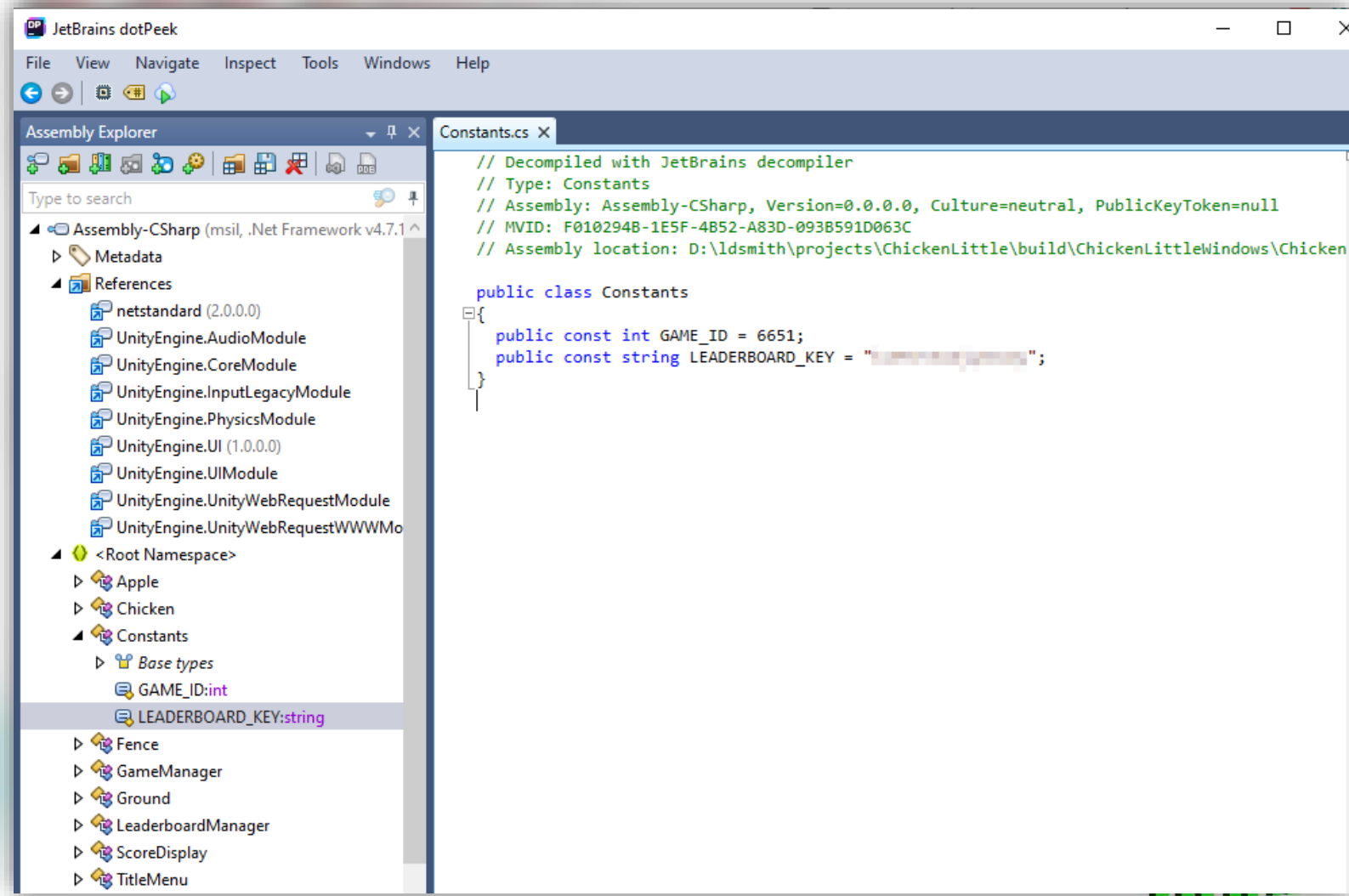
- Extracts asset files such as textures, audio, and fonts
- Didn't appear to extract code



BOX
ME
DESIGN

dotPeek

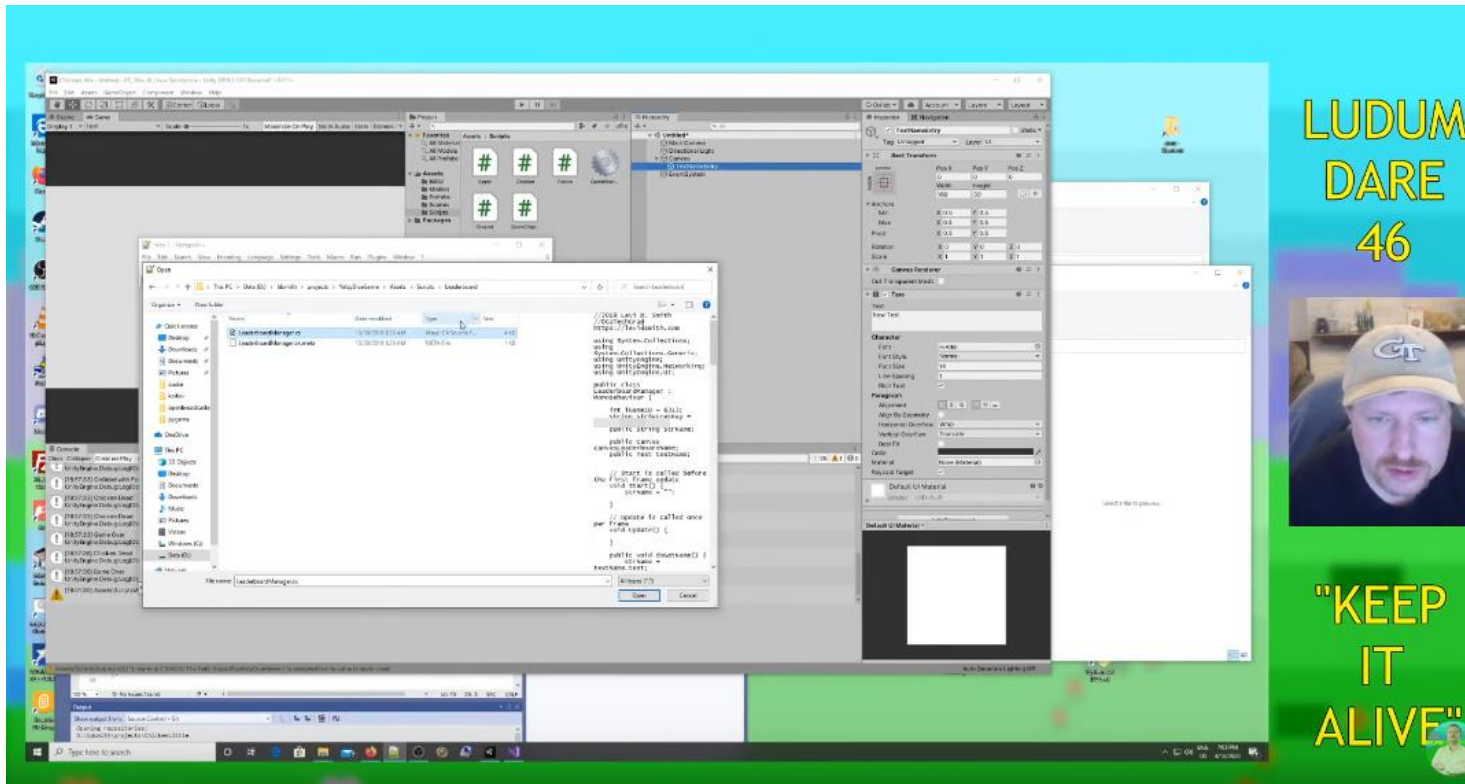
- JetBrains dotPeek
 - <https://www.jetbrains.com/decompiler/>
- File > Open >
build/ChickenLittleWindows/ChickenLittle_Data/Assembly-CSharp.dll
- I could only get it to work for Windows
build (not WebGL)



DESIGN

Live Streaming

- Don't accidentally display your key while live streaming

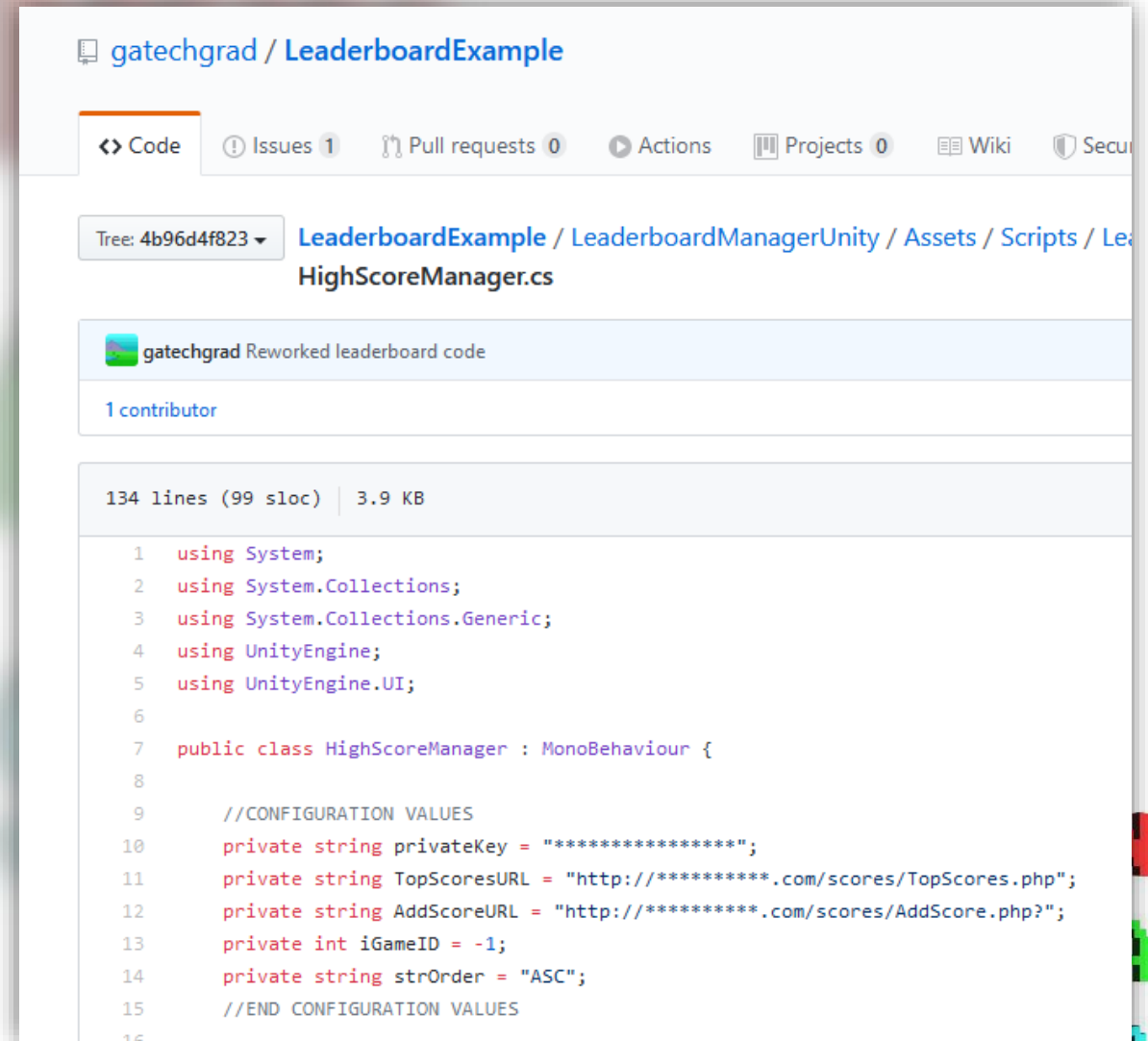


- Now set to *Private*
- Only viewed 4 times
- If key is exposed, then it has to be updated in all games

KNOX
GAME
DESIGN

Code Repository

- Remember to remove key from any checked-in code
 - Better - put keys in your .ignore or .gitignore file



The screenshot shows a GitHub repository page for 'gatechgrad / LeaderboardExample'. The file 'HighScoreManager.cs' is selected, showing its commit history and code. The code is a C# script for a HighScoreManager class, which is a MonoBehaviour. It includes configuration values for a private key, top scores URL, add score URL, game ID, and sort order.

```
1 using System;
2 using System.Collections;
3 using System.Collections.Generic;
4 using UnityEngine;
5 using UnityEngine.UI;
6
7 public class HighScoreManager : MonoBehaviour {
8
9     //CONFIGURATION VALUES
10     private string privateKey = "*****";
11     private string TopScoresURL = "http://*****.com/scores/TopScores.php";
12     private string AddScoreURL = "http://*****.com/scores/AddScore.php?";
13     private int iGameID = -1;
14     private string strOrder = "ASC";
15     //END CONFIGURATION VALUES
16 }
```

BOX
ME
DESIGN

Other Possibilities

- The value was modified in game memory before being sent to the web server
 - Should see pairs of **AddScore.php** and **TopScores.html** in the access log from the games
 - **AddScore.php** followed by **DisplayScores.html** is most likely a hacker
 - A glitch was found with the game itself and actually did run for 16 minutes
 - Automated clickers?
- MediaWiki exploit? Lots of AddScore.php followed by wiki request
 - Could just be a web crawler bot
 - MediaWiki 1.27.4 - November 2017
 - MediaWiki really needs an update button like Wordpress. Downloading, extracting, and reconfiguring packages is very time consuming
- Hacker bounties
 - Paid to find exploits in systems

KNOX
GAME
DESIGN









Better options

- SHA-2 instead of MD5
- Public key encryption
- Unity3D Obfuscator
- Don't make code open source
- Ticketing system
 - Provide IP and get back a key from the server
 - Server limits the time that the ticket can be used
 - Could still be emulated, but key isn't stored in source code



KNOX
GAME
DESIGN

Another example

<input type="checkbox"/>	 Edit	 Copy	 Delete	531	Fruity McLoops	2496	2020-05-03 21:04:14	6651
<input type="checkbox"/>	 Edit	 Copy	 Delete	532	Fruity McLoops	2496	2020-05-03 21:07:10	6651
<input type="checkbox"/>	 Edit	 Copy	 Delete	533	ILUVCHICKENS	6942069	2020-05-03 21:34:35	6651
<input type="checkbox"/>	 Edit	 Copy	 Delete	534	Newton	2441	2020-05-03 21:49:04	6651

```
185.163.46.141 - - [03/May/2020:21:34:35 -0700] "GET /scores/AddScore.php?game=6651&name=ILUVCHICKENS&score=6942069&hash=663c4ce4c6d87fe58e34aa1bd9a53a60 HTTP/2.0" 200 166 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18363"
185.163.46.141 - - [03/May/2020:21:34:35 -0700] "GET /scores/DisplayScores.html HTTP/2.0" 200 1505 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18363"
185.163.46.141 - - [03/May/2020:21:34:36 -0700] "GET /blog/wp-content/uploads/2015/03/website_bkg3.jpg HTTP/2.0" 200 32972 "https://levidsmith.com/scores/DisplayScores.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18363"
185.163.46.141 - - [03/May/2020:21:34:37 -0700] "GET /scores/leaderboard.json HTTP/2.0" 200 1239 "https://levidsmith.com/scores/DisplayScores.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18363"
```

```
45.21.158.227 - - [03/May/2020:21:07:54 -0700] "GET /scores/AddScore.php?game=6651&name=ILUVDABEST&score=6942069&hash=741790d400897e8b1dac862a449470fc HTTP/2.0" 200 41 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18363"
```

< Failed attempt

NOX
AME
DESIGN

References

- A practical tutorial to hack (and protect) Unity games
 - <https://www.alanzucconi.com/2015/09/02/a-practical-tutorial-to-hack-and-protect-unity-games/>
- MD5 reverser
 - <https://md5.gromweb.com/>
- What's My IP (and many other tools!)
 - www.whatsmyip.org
- ILSpy - <https://github.com/icsharpcode/ILSpy>
- DevXUnity - <https://www.devxdevelopment.com/>
- uTinyRipper - <https://github.com/mafaca/UtinyRipper>
- dotPeek - <https://www.jetbrains.com/decompiler/>

KNOX
GAME
DESIGN