

Forum:[Hack Forums](#)

Thread: [Magic Mirror - Reflection Runtime Utility](#)

PlaySkool - October 30, 2016, 2:50 am

Magic Mirror is now available for a pre-pre-alpha. The tool is still brand new, but I figured I would share the progress I've made so far. Currently, all that is (semi) working is the scan-by-value feature. Lots will change, stay tuned for more information.

This tool is being developed by myself and Konloch.

<https://github.com/cryptotoad/MagicMirror>

Magic Mirror is a modern reflection client designed to replace the outdated clients plaguing the RSPS scene.

Magic Mirror was designed with 3 goals in mind.

- Magic Mirror is extensible with scripts (Not yet!)
- Magic Mirror supports code injection on jars and class folders
- Magic Mirror ?o??iM ?io?M -

.bnim ni ?l?oo ? Hliw b?noi??b ??w ?o??iM ?io?M

.?n??? ?9?? ?HI oniuo?lq ?ln?il? b?l?bluo ?HI ???lq?? ol b?noi??b ln?il? noil??l??? n??bom ? ?i
?o??iM ?io?M

Images below.

Spoiler ([Click to View](#))

le edgy fag - October 30, 2016, 10:27 am

Cool shit OP and nice to see Konloch on board too

GenericSkid - October 30, 2016, 10:50 pm

There's a lot of weird non-standard syntax in the source. The mirrored text on the repo is a cool gimmick though.

PlaySkool - October 31, 2016, 1:21 am

Lots of the GUI is generated with netbeans that may be what you're seeing.

If you're referring to my code, it's because I hate java.

Update: I've managed to get scan-by-val to actually write to the remote fields, and implemented a sort of bootleg cheat engine.

<https://i.imgur.com/HCKXsf7.mp4>

Irie Vibes - October 31, 2016, 4:32 am

What exactly would this allow you to do on a rps?

PlaySkool - October 31, 2016, 1:55 pm

<https://i.imgur.com/HCKXsf7.mp4>

Well for starters, it makes interface forcing much easier than it would be with cheat engine.

That said, the MAIN purpose of scan-by-value is to assist with deobfuscation, allowing you to quickly find the fields you need to run your reflection code.

What this allows you to do varies wildly depending on the server, but it will allow you to find obscure flaws much quicker than a reflection client packed with pre-made commands.

Long term, it will be scripted to also support premade commands, however the commands will reference an obfuscation map so there's no need to rename variables when you use a new client, you simply make a new map.

SIM-2501407 - October 31, 2016, 8:33 pm

Got to say when it comes to coding RSPS related tools, PlaySkool is the man.

PlaySkool - November 1, 2016, 3:29 pm

Tool has been updated, refining scan now works. Still only for ints. Once I add in-array scanning I'll port the functions to the other types.

PlaySkool - November 12, 2016, 2:44 pm

Updated on github, now includes rudimentary string support and fixed some bugs with null value handling.