

Forum:[Hack Forums](#)

Thread: [How to hook ROBLOX methods in a Lua environment that can modify protected metatables](#)

Informable - September 14, 2016, 8:14 pm

In a ROBLOX game, there is a metatable that all ROBLOX Instances share. In many Lua script injection exploits, there will be an added function which allows you to take that metatable and change it, even though it's normally locked and unchangeable.

It's important to take care when doing this, because one wrong move and the entire game will implode on itself in a flood of ugly errors. Or you might cause extremely unexpected behavior and crash yourself. Every single script on your client will be affected by the changes you make to this metatable, and so you want to keep it working.

However, with the ability to change this metatable, it's possible to hook any method inside of any instance. That is a very powerful thing. The changes you make to these methods will affect every script in the game that uses them, and that change will happen instantly during runtime, as if nothing ever happened.

This is extremely useful, especially for games that script with FilteringEnabled on. You can hook methods like FireServer/InvokeServer and trick your client into thinking the server is returning something that it isn't. Or you can spy on what methods a script is calling, and bend it to your will by hooking those methods to do your bidding.

Let me walk you through the process. In this example, we will assume your environment has a function called "getrawmetatable" (a common name for this particular function in ROBLOX scripting exploits), and that it returns a non-read-only version of any userdata's metatable.

We'll start out by creating two variables: One to hold the game's real metatable, and one to hold a table that we'll use to back up that metatable. The backup is important, because we still want to maintain the real metatable's original behavior for everything except what we hook.

```
Code local meta = getrawmetatable(game)
local oldmeta = {}
```

Next, we iterate through the real metatable's contents and copy them into the backup table:

```
Code for i,v in next,meta do
    oldmeta[i] = v
end
```

Now that we have the backup in place, it's time to modify the real metatable. This is where you need to be extra tricky. The metamethod that we want is `__index`. Every time any script on your client looks for a method inside an instance, it's indexing that instance, and it's the `__index` metamethod that decides what to return. We can change that and return our own thing.

```
Code meta.__index = function(t, k)
```

```
    return oldmeta.__index(t, k)
end
```

That return line, if reached, should pass the request over to the original `__index` that we backed up,

and return the result as it would under normal circumstances. But above that line, we can put some conditionals to return what we want instead. Let's try hooking the Kick function for fun:

```
Code meta.__index = function(t, k)
  if k:lower() == "kick" and t:IsA("Player") then
    return function(self)
      if self.Character:FindFirstChild("Humanoid") then
        self.Character.Humanoid.Health = 0
      end
    end
  end
  return oldmeta.__index(t, k)
end
```

What we've just done is made it so that if a script tries accessing the Kick method of a Player object (e.g. game.Players.Weenie:Kick()), it will instead return our custom function, which kills the player. Now every single script on our client that tries to call Kick will instead kill the player it was called on.

This isn't very useful by itself, but if you use your imagination, you can find many other creative uses for it. Remember that game creators on ROBLOX don't normally realize that the LocalScripts they set up can be manipulated in that way. You may find a vulnerability in an admin script or some sort of vector for exploiting a FilteringEnabled game, and the only way to exploit that vulnerability may be through this type of hooking.

Thanks for reading. If you have any questions, post them! ?

Discuss - September 15, 2016, 4:28 am

Wow, I didn't think people still played that game.

Nice contribution though; you put a lot of effort into this thread!

Informable - September 15, 2016, 4:34 pm

(Sep 15, 2016 04:28 AM)Discuss Wrote: [\[CITE\]](#) Wow, I didn't think people still played that game.

Nice contribution though; you put a lot of effort into this thread!

Thanks! And yeah, people don't just play it, it's becoming one of the most played family games ever. It has millions of active players. It's very nostalgic for me, and the scripting side of it keeps me hooked.

xah_auL - October 28, 2016, 1:19 am

Is there a possible way to do this using Lua C Api and C++ to create an functional exploit?

Gorzoid - October 31, 2016, 3:08 pm

(Oct 28, 2016 01:19 AM)xah_auL Wrote: [\[CITE\]](#) Is there a possible way to do this using Lua C Api and C++ to create an functional exploit?

I swear I replied to this b4 but i guess i never clicked post... welp

If you want to make your own rawgetmetatable function basicly just copy the source code for luaB_getmetatable and remove the __metatable check. I have never played roblox so I am guessing they use the __metatable metafield to stop you accessing it. then just push that onto the global table and your grand.

Alureon - November 2, 2016, 12:57 am

(Oct 31, 2016 03:08 PM)Gorzoid Wrote: [\[CITE\]](#) I swear I replied to this b4 but i guess i never clicked post... welp

If you want to make your own rawgetmetatable function basicly just copy the source code for luaB_getmetatable and remove the __metatable check. I have never played roblox so I am guessing they use the __metatable metafield to stop you accessing it. then just push that onto the global table and your grand.

This would work but you have to do a lot more because their Lua environment is heavily modified (struct offsets changed around, TValue IDs different, etc.).

You're better off just editing their luaB_getmetatable, provided you can bypass their check which detects editing of .text section memory (which is pretty easy, to be completely honest).

Gorzoid - November 4, 2016, 5:43 am

Just downloaded roblox and I was able to find the functions like luaB_getmetatable and luaL_loadbuffer. I was trying to get my loadbuffer hook for gmod to work but for some reason DllMain won't run, using extreme injector and standard injection gives some "no permission exception" and ManualMap just doesn't do anything. Do they have anything blocking dll injection? Theres not much public info about it (google search is cluttered with idiots on roblox forum who have no idea what they are talking about)

Informable - December 17, 2016, 2:38 am

(Nov 4, 2016 05:43 AM)Gorzoid Wrote: [\[CITE\]](#) Just downloaded roblox and I was able to find the functions like luaB_getmetatable and luaL_loadbuffer. I was trying to get my loadbuffer hook for gmod to work but for some reason DllMain won't run, using extreme injector and standard injection gives some "no permission exception" and ManualMap just doesn't do anything. Do they have anything blocking dll injection? Theres not much public info about it (google search is cluttered with idiots on roblox forum who have no idea what they are talking about)

ROBLOX has some very weird checks, but DLL injection should work. If you're using AllocConsole then you should know that there is a loop in the game that constantly calls FreeConsole. You can just kill FreeConsole when your DLL is injected to get around that. There's a certain website with a community that's nearly 90% devoted to ROBLOX exploiting (even though most people there are skids just like HF) but I don't know if I'm allowed to say the name of it here.

EDIT: You should know something really important: luaL_loadbuffer (and ALL related functions) have been removed from the client. There is no way to generate bytecode traditionally. Also, the format of their entire Lua VM is secret and custom to prevent exploiting. You need to be VERY tricky to run your own scripts.

Gorzoid - December 17, 2016, 9:43 am

(Dec 17, 2016 03:38 AM)Informable Wrote: [\[CITE\]](#) luaL_loadbuffer (and ALL related functions) have been removed from the client.

Weird, pretty sure I found luaL_loadbuffer by comparing with lua 5.1 source code, and it seemed to be very similar to regular lua, just with a tiny bit of code added in between and of course all exports of luafunctions were removed.

Also could you PM me that site, people often post URLs in base64 and they don't get banned for that so idk.

Edit: I'm guessing your talking about v3rm***ion and my god is that site horrible, the red theme just boldens all of the shitposts there, and the only relatively informative moderate area is VIP only which sucks.

Informable - December 17, 2016, 5:47 pm

(Dec 17, 2016 10:43 AM)Gorzoid Wrote: [\[CITE\]](#) Weird, pretty sure I found luaL_loadbuffer by comparing with lua 5.1 source code, and it seemed to be very similar to regular lua, just with a tiny bit of code added in between and of course all exports of luafunctions were removed.

Also could you PM me that site, people often post URLs in base64 and they don't get banned for that so idk.

Edit: I'm guessing your talking about v3rm***ion and my god is that site horrible, the red theme just boldens all of the shitposts there, and the only relatively informative moderate area is VIP only which sucks.

That's the site yea. There is an underground subculture of people on that site who really know what they're doing. It's just hard to find and hard to get into. ROBLOX exploits are VERY profitable on places like that, it's a high demand market with very low supply.

daymon - December 17, 2016, 5:50 pm

This is autum's script my dude, at least give credit

Informable - December 17, 2016, 5:53 pm

(Dec 17, 2016 06:50 PM)Sin+ Wrote: [\[CITE\]](#) This is autum's script my dude, at least give credit
Wow are you from V3rm? It's tempting to start fresh in a new community I haven't participated in yet, but I am actually Autumn.

daymon - December 17, 2016, 5:59 pm

(Dec 17, 2016 06:53 PM)Informable Wrote: [\[CITE\]](#) Wow are you from V3rm? It's tempting to start fresh in a new community I haven't participated in yet, but I am actually Autumn.

Of course my dude, roblox scripting is the essence of my existence. And seriously? PM proof, because if you are, then we gotta talk lmao.

?Dominate - December 17, 2016, 11:16 pm

(Dec 17, 2016 06:59 PM)Sin+ Wrote: [\[CITE\]](#) Of course my dude, roblox scripting is the essence of my existence. And seriously? PM proof, because if you are, then we gotta talk lmao. Yep, that's Autumn.

I registered on her forums previously but got inactive.

Haven't played the game ever since the termination of my account and never accessed v3rm again due to that.

Gorzoid - December 18, 2016, 2:04 pm

One of the main reasons I keep getting annoyed at reversing this game is converting the addresses to working pointers in runtime, GetModuleHandle("RobloxPlayerBeta.exe")+offset doesn't work and neither does the function I got from v3rm:

```
DWORD base = (DWORD)GetModuleHandle("RobloxPlayerBeta.exe");
DWORD getaddy2(int address) {
    return (address - 0x400000 + base);
}
```

Is this something roblox is purposely doing in order to stop us? Or am I being an idiot, cus some addresses are offset more from their IDA address than others even if they both in .rdata

Informable - December 18, 2016, 8:29 pm

(Dec 18, 2016 03:04 PM)Gorzoid Wrote: [\[CITE\]](#) One of the main reasons I keep getting annoyed at reversing this game is converting the addresses to working pointers in runtime, GetModuleHandle("RobloxPlayerBeta.exe")+offset doesn't work and neither does the function I got from v3rm:

```
DWORD base = (DWORD)GetModuleHandle("RobloxPlayerBeta.exe");
DWORD getaddy2(int address) {
    return (address - 0x400000 + base);
}
```

Is this something roblox is purposely doing in order to stop us? Or am I being an idiot, cus some addresses are offset more from their IDA address than others even if they both in .rdata
Address - 0x400000 + base is correct, it works fine for me. Maybe you have you offset in IDA set to something weird? I'm really not sure about .rdata, most of the fun stuff is in .text (but that's also where all their truly evil security checks are).

Thomas Meme - *December 19, 2016, 3:00 pm*

Oh roblox the OG minecraft I grew up with old pc games.