

Forum:[Hack Forums](#)

Thread: [Dynamic Functions on Dynamic Libraries](#)

30xic - March 9, 2019, 10:11 am

Hello everyone,

Last day's I was trying to do this in c++:

Let's say I have a function foo(arg1, arg2), one client and one server.

arg1 can be any type, arg2 can be any type and foo can return any type of data. function Foo also has always to arguments.

I want the client to take as an input this function(for example):

```
Code foo(arg1,arg2){
    if(arg1<arg2){
        return 1;
    }else{
        return 5.2;
    }
}
```

and then this function to be transferred and executed on the server.

I tried to build dynamic library with this function inside with templates. However templates are not supported with extern "C".

So any idea how can I implement this?

I know this is not secure but its only for educational purposes.

Auriana - March 9, 2019, 12:04 pm

You can not execute code remotely like that, it would extremely hazardous to security. You can attach remote debuggers and execute functions there. Maybe you want to send shellcode across a network and execute that? If that's the case the shellcode needs to be PIC or you need to map the shellcode into memory and make sure all required modules are loaded before being executed.

An alternative is to just write your function inside your client, then just send a command from the server to execute the code. It would have to already be defined in the client.

It's a little more complicated if you want to send shellcode across to the client and execute it dynamically. Look into Windows Portable Executable format.

Goodies - March 10, 2019, 11:44 pm

(Mar 9, 2019 01:04 PM)Auriana Wrote: [\[CITE\]](#) You can not execute code remotely like that, it would extremely hazardous to security. You can attach remote debuggers and execute functions there. Maybe you want to send shellcode across a network and execute that? If that's the case the shellcode needs to be PIC or you need to map the shellcode into memory and make sure all required modules are loaded before being executed.

An alternative is to just write your function inside your client, then just send a command from the server to execute the code. It would have to already be defined in the client.

It's a little more complicated if you want to send shellcode across to the client and execute it dynamically. Look into Windows Portable Executable format.

Honestly a flawless answer. Positionally independent shellcode really isn't that hard to write. While not designed for windows, this project I wrote, [called cshell](#), is similar in spirit, but for writing positionally independent shellcode in C. With windows it's actually easier to write PIC code in C. Tutorials [like this](#) helped me develop some software, the source of which I wouldn't share.

It's highly doubtful you actually would want to execute remote shellcode in a normal context though... there are very obvious security concerns as Auriana mentioned.

HFDone - *March 11, 2019, 11:56 am*

as said you cant and writing shell code for remote execute is not simple if you want more then msgbox

what you can do is to use c library as a backend for dynamic code generation which let you send any code and run it