

Forum:[Hack Forums](#)

Thread: [Compiler.NET Discord Bot - With live snippet compilation and executions](#)

Barret - August 29, 2017, 4:53 pm

Discord bot that can compile and execute your code snippet live in the channel.

Tutorial

This tutorial is based on Debian but should be simple enough for other distro's as well, i assume you read the thread and seen the requirements.

We need NodeJS, Php, Mono and a unix box in order for this to work, notice that you need to be the admin (root) of the unix box you have.

Preparations

Download the base files from: <https://github.com/TheBarret/Compiler.NET> and place these in a folder where your bot is going to operate.

Via your discord account you can add a new application which is going to be your bot, if you never done this before i recommend

that you follow these instructions:

<https://github.com/reactiflux/discord-irc/wiki/Creating-a-discord-bot-&-getting-a-token>

This token you finally get after you created it, is the token that is going to be in auth.json from my project files.

So go ahead and edit that config and place your bot's token in there.

Install mono-complete and build-essentials if you haven't already

Code `sudo apt-get install build-essential`

`sudo apt-get install mono-complete`

Install NodeJS 6.* or NodeJS 8.*

Code `curl -sL https://deb.nodesource.com/setup_6.x | sudo -E bash -`

`sudo apt-get install -y nodejs`

Code `curl -sL https://deb.nodesource.com/setup_8.x | sudo -E bash -`

`sudo apt-get install -y nodejs`

Install the Discord.JS and Random-id.js

This must be executed INSIDE the directory where you placed the compiler bot files

Code `npm install --save discord.js`

`npm install --save random-id`

After doing this, we have created the environment to execute and operate your compiler bot.

Confirm the following commands to check everything is in place:

Adjustments

The bot.js file contains config settings that you might want to check out, the functions.php has functions that include keyword filtering.

Most keywords have been setup by me, but if you want to change that make sure you use php regex formats, example:

Lets say you want to block System.Text you would add:

```
Code \bSystem\b\\bText\b
Adding admins (people you trust...)
```

The bot.js holds also your admins whitelist, it accepts only discord user id's (not the small one, the large number format).

```
Code var admins = ['1111111111111111','2222222222222222','3333333333333333'];
```

If you done all that we are ready to startup and test it out but whatever you do, DON'T EVER EXECUTE AS ROOT

The bot has a feature that blocks compiles being executed as root, but still, bad practise to run services as root.

So create or change into another (lower) account and type node bot.js in the bot folder we created earlier

Things to consider and facts

Room for improvement, feel free to adjust the scripts if you see fit.

The bot uses two pre-set c#/vb solution files that contain pre-coded wrapper classes.

Compilations are usually finished within 3~6 seconds, depending on system hardware and speed.

The bot keeps session id's that correspond with log files in the log folder that hold more detailed info of a session.

Each user using the bot gets a separated log folder that holds all requests and builds.

The bot uses Framework 4.5, change this by changing the settings when you open the project files in the VS.

Mono might have a lot already built in, a small portion has yet to be ported.

Why CAS is not been utilized? Sadly Mono does not yet support these namespaces.

Commands!showid Shows user's discord id (everyone)

!uptime Shows system uptime (everyone)

!mem Shows system memory table (everyone)

!version Shows current version along with system's OS info (everyone)

!mono Shows current mono version (everyone)

!chmode Enables or Disables lock for free compiles for non-admins users (only admin, enabled by default)

!vbnet ..code.. Compiles and executes vb.net code (only admins or if lock is disabled)

!csharp ..code.. Compiles and executes c#.net code (only admins or if lock is disabled)

FeaturesC# Compile and Run

VB Compile and Run

Supports Framework 4.5

Whitelist members only

Safety: filter (intercept potential unsafe code)

Safety: Max execution time

Safety: Max output responds

Safety: Will not compile if process is root

RequirementsUnix server

Mono (runtime and sdk)

Java environment (Node.js, Discord.js)

Php environment (version 5.*)

And...decent knowledge of all items named above

Diagram of system flow

VB.NET

C#.NET

Some loop testing

Unix Debug Terminal

People involved with testing in this project

Panthera (advice, tester), Cawk (advice tester), forceberg (tester), Wops (tester), Naywyn (tester), NewMecha (model), Rhez (tester), Electroalek (php regex)

(if i forgot your name, please forgive me and pm me)

Rhez - August 29, 2017, 6:53 pm

What do you fucking expect with Barret's thread? Of course another fucking high quality thread. ?

.cYRil. - August 29, 2017, 7:00 pm

This is really amazing and different share, great job as always.

Cecilia - August 30, 2017, 3:05 am

Fun bot to play with, well done :)

warpje - August 30, 2017, 7:08 am

Wow you always deliver nice and quality projects.

Is the bot on your discord?

cawkre - August 30, 2017, 4:13 pm

Very nice bot!

It's a nice feature in a discord server to have fun with

Nice job!

Barret - August 30, 2017, 5:33 pm

(Aug 30, 2017 04:13 PM)danny1313 Wrote: [\[CITE\]](#) Very nice bot!

It's a nice feature in a discord server to have fun with

Nice job!

Oh and they have.... ? they trying all fucked up voodoo linq in there....

I had to rewrite a ton of security measures (filters) to avoid pesky info leakage.

Helios. - August 30, 2017, 6:43 pm

Great job.

Now regarding security you shouldn't just rely on "filters". You should use sandboxing in .net (CAS policy) and since you are using Unix you can run the process under a user with the lowest permissions possible (read/write/execute).

Barret - August 31, 2017, 12:03 am

Ok finally updated the thread, tutorial is made, questions can be asked.

Parse - August 31, 2017, 1:46 am

this is sick good work man i like the organization

Ninja - August 31, 2017, 4:21 am

I am assuming you blocked people from accessing your PC information and hardware info and such?

This looks nice though, good job.

Rhez - August 31, 2017, 5:02 am

(Aug 31, 2017 04:21 AM)Ninja Wrote: [\[CITE\]](#) I am assuming you blocked people from accessing your PC information and hardware info and such?

This looks nice though, good job.

He filtered methods that can have security issue on his side.

Ninja - August 31, 2017, 10:33 am

(Aug 31, 2017 05:02 AM)Rhez Wrote: [\[CITE\]](#) He filtered methods that can have security issue on his side.

Ah ok.

And also I hope you blocked CodeDOM.

Barret - August 31, 2017, 10:35 am

The bot is currently offline, some asshole managed to do something and corrupted the filesystem on the SD, so ill have to replace that with a new one, downtime, 3 or 4 days

Ninja - August 31, 2017, 10:53 am

(Aug 31, 2017 10:35 AM)Barret Wrote: [\[CITE\]](#) The bot is currently offline, some asshole managed to do something and corrupted the filesystem on the SD, so ill have to replace that with a new one, downtime, 3 or 4 days

There will probably always be exploits. I suggest you get a couple of good guys you know to beta test it some more.

Barret - August 31, 2017, 11:20 am

(Aug 31, 2017 10:53 AM)Ninja Wrote: [\[CITE\]](#) There will probably always be exploits. I suggest you get a couple of good guys you know to beta test it some more.

Funny you say that, that is exactly what i did. Admins only, well lesson learned, fuck trust and prepare for the worst. I can be pissed off or not, it would have happened anyway i suppose.

Ninja - August 31, 2017, 2:21 pm

(Aug 31, 2017 11:20 AM)Barret Wrote: [\[CITE\]](#) Funny you say that, that is exactly what i did. Admins only, well lesson learned, fuck trust and prepare for the worst. I can be pissed off or not, it would have happened anyway i suppose.

Well then I am out of ideas. I am sure you blocked CodeDOM, maybe even sockets/webclients/etc.,

any Process method, anything with database interaction, anything with hardware interaction, and such?

And do you at least know who it was that did it? I assume you keep some form of logs?

Barret - August 31, 2017, 3:54 pm

(Aug 31, 2017 02:21 PM)Ninja Wrote: [\[CITE\]](#) Well then I am out of ideas. I am sure you blocked CodeDOM, maybe even sockets/webclients/etc., any Process method, anything with database interaction, anything with hardware interaction, and such?

And do you at least know who it was that did it? I assume you keep some form of logs?
codedom.... ? apparently u did not read the thread.

Washi - September 1, 2017, 2:16 am

(Aug 31, 2017 02:21 PM)Ninja Wrote: [\[CITE\]](#) Well then I am out of ideas. I am sure you blocked CodeDOM, maybe even sockets/webclients/etc., any Process method, anything with database interaction, anything with hardware interaction, and such?

And do you at least know who it was that did it? I assume you keep some form of logs?
You cant really rely on source code filters only. Even if you filter out keywords or sequences of code words such as namespaces and the like, people will come up with ideas to bypass that. For example, you can get a very long way with a couple of reflection calls and very simple string encryption to hide the stuff you're looking for. If you block reflection, then suddenly a lot of code becomes unusable so I'd assume that isn't an option either.

@op Your best bet is probably setting up a new Unix user that has a lot of restrictions. Only preventing execution from root is definitely not enough. You need to run the server on a user that can only access and execute a very limited amount of files etc. So that even if they manage to bypass your filters, they still wont get far, unless they found an exploit in the kernel itself, which is highly unlikely. Also you might wanna have a look at the CAS policy mechanisms .net provides, since they are a very robust way to prevent execution of code without having to analyze the code itself.

Ninja - September 1, 2017, 3:26 am

(Sep 1, 2017 02:16 AM)Washi Wrote: [\[CITE\]](#) You cant really rely on source code filters only. Even if you filter out keywords or sequences of code words such as namespaces and the like, people will come up with ideas to bypass that. For example, you can get a very long way with a couple of reflection calls and very simple string encryption to hide the stuff you're looking for. If you block reflection, then suddenly a lot of code becomes unusable so I'd assume that isn't an option either.

To be fair this is just a compiler bot, I doubt people will upload snippets that are advanced and use reflection and such. There is no debugging using this tool, and people writing advanced code snippets usually test their stuff thoroughly in the process of doing so, probably in the normal IDE (VS).

Washi - September 1, 2017, 4:11 am

(Sep 1, 2017 03:26 AM)Ninja Wrote: [\[CITE\]](#) To be fair this is just a compiler bot, I doubt people will upload snippets that are advanced and use reflection and such. There is no debugging using this tool, and people writing advanced code snippets usually test their stuff thoroughly in the process of doing so, probably in the normal IDE (VS).

True, but that is not really the point here. Of course this system is not meant to be used like this, but we're talking about security here, not about what the intentions of the creator was. If people see a way to run arbitrary code (which is what the purpose of this program is), it's basically is providing the user with a seedbed for malware, and they will try their best to find loopholes in it and hack into the

system. This is probably what happened here as well.

Ninja - September 1, 2017, 4:20 am

(Sep 1, 2017 04:11 AM)Washi Wrote: [\[CITE\]](#) True, but that is not really the point here. Of course this system is not meant to be used like this, but we're talking about security here, not about what the intentions of the creator was. If people see a way to run arbitrary code (which is what the purpose of this program is), it's basically is providing the user with a seedbed for malware, and they will try their best to find loopholes in it and hack into the system. This is probably what happened here as well.

I'm saying you don't really have to provide the users with every feature possible in .NET (besides things that can be used maliciously), but I get where you come from.

stefsot - September 1, 2017, 4:41 am

You can run the code in a sandboxed appdomain with limited permissions.

Lots of exampels around the web.

[https://msdn.microsoft.com/en-us/library/system.appdomain.setappdomainpolicy\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.appdomain.setappdomainpolicy(v=vs.110).aspx)

Barret - September 1, 2017, 9:10 am

(Sep 1, 2017 04:41 AM)stefsot Wrote: [\[CITE\]](#) You can run the code in a sandboxed appdomain with limited permissions.

Lots of exampels around the web.

[https://msdn.microsoft.com/en-us/library/system.appdomain.setappdomainpolicy\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.appdomain.setappdomainpolicy(v=vs.110).aspx)

Mono's security namespace is not yet fully implemented/ported, read the thread dude.

Ajumma - September 10, 2017, 12:08 am

Would it be possible to add an option to run a certain command and have the bot output the result? something like !run "chrome.exe"

Barret - September 10, 2017, 12:14 am

(Sep 10, 2017 12:08 AM)Ajumma Wrote: [\[CITE\]](#) Would it be possible to add an option to run a certain command and have the bot output the result? something like !run "chrome.exe"

chrome is a gui, the bot is currently only trialed and tested on unix with the mono runtime and sdk. console based apps are possible, windows gui is not.

Rhez - September 10, 2017, 7:44 am

(Sep 10, 2017 12:14 AM)Barret Wrote: [\[CITE\]](#) chrome is a gui, the bot is currently only trialed and tested on unix with the mono runtime and sdk. console based apps are possible, windows gui is not.

He means like executing a task (process.start)

Barret - September 10, 2017, 10:38 am

(Sep 10, 2017 07:44 AM)Rhez Wrote: [\[CITE\]](#) He means like executing a task (process.start)

<https://stackoverflow.com/questions/2255624/how-to-use-process-start-or-equivalent-with-mono-on-a-mac-and-pass-in-argument>