

Information Gathering Automation

(misc.)

X-MAS CTF 2019

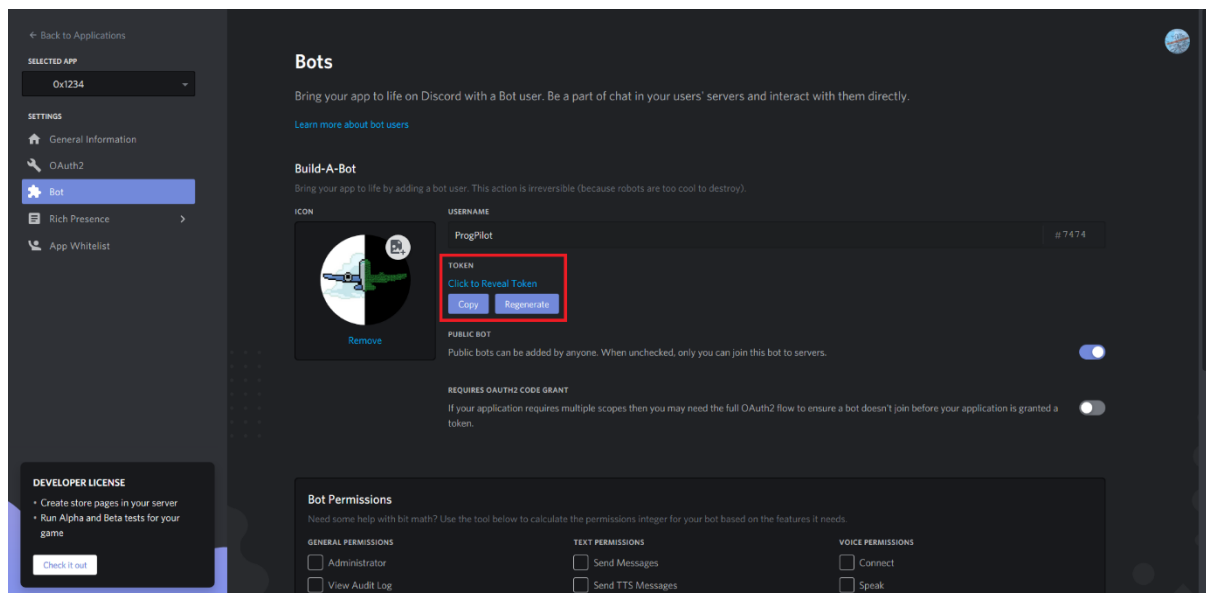
Written by Tom Pain (0x5444) for ProgPilot

Information Gathering Automation was a challenge which was part of the 2019 X-MAS CTF, organised by HTsP. The description was as follows:

“Our agency wants to collect information related to the next line-up of entertainment objects that are currently being built by Santa’s gnome team. We noticed that the factory only trusts Discord bots to enter, so we need you to create an Information Gathering Automation in order to collect the factory’s secrets.”

It sounded interesting and right up my street, so I thought I’d give it a shot.

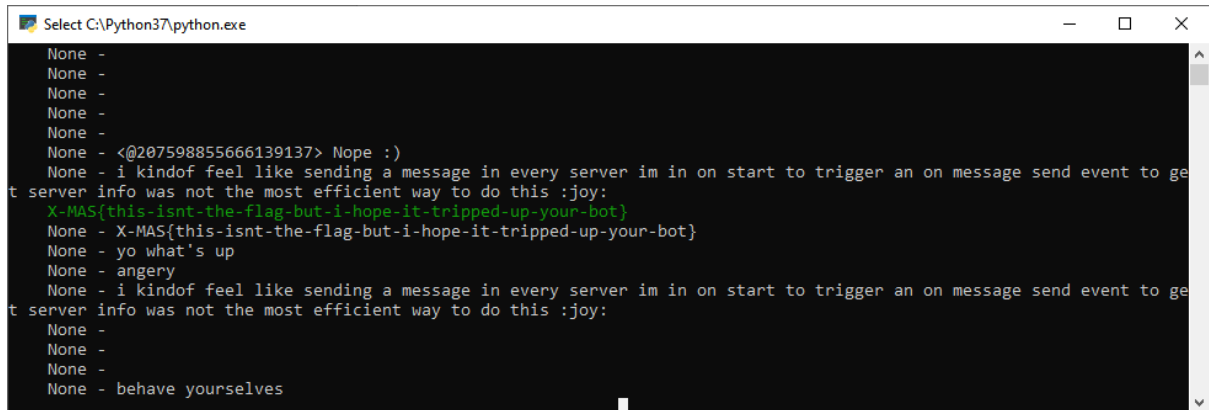
The brief specified we’ll have to make our own Discord bot, so I set about doing that first. It’s fairly simple to setup your own Discord bot - head to the My Applications section of the Discord Developer Portal, hit new application, give it a name, enable the bot feature, and you’re set. Note down the token.



To get your bot in the factory server, you have to make up an invite URL for it (see <https://discordapp.com/developers/docs/topics/oauth2#bot-authorization-flow>) and send that URL to the challenge author.

Once this has been done, you can begin writing your bot code. I used [Discord.Py](#) for this, but you could use [Discord.JS](#) if you wanted.

The code I wrote was simple - the bot would connect, check if it was a member of the target guild (in this case “*Toy Factory*”) and if it was, iterate over every channel and retrieve the last 200 messages. If a message that had “*X-MAS*” in it was found, that would be highlighted.

A screenshot of a Windows command prompt window titled "Select C:\Python37\python.exe". The window has a black background with white text. The text shows a series of messages from a bot, mostly starting with "None -". One message is highlighted in green: "X-MAS{this-isnt-the-flag-but-i-hope-it-tripped-up-your-bot}". Other messages include "Nope :)", "i kindof feel like sending a message in every server im in on start to trigger an on message send event to get server info was not the most efficient way to do this :joy:", "yo what's up", "angery", and "behave yourselves".

```
Select C:\Python37\python.exe
None -
None -
None -
None -
None -
None - <@207598855666139137> Nope :)
None - i kindof feel like sending a message in every server im in on start to trigger an on message send event to ge
t server info was not the most efficient way to do this :joy:
X-MAS{this-isnt-the-flag-but-i-hope-it-tripped-up-your-bot}
None - X-MAS{this-isnt-the-flag-but-i-hope-it-tripped-up-your-bot}
None - yo what's up
None - angry
None - i kindof feel like sending a message in every server im in on start to trigger an on message send event to ge
t server info was not the most efficient way to do this :joy:
None -
None -
None -
None - behave yourselves
```

Nice try

