X-MAS Helper (web)

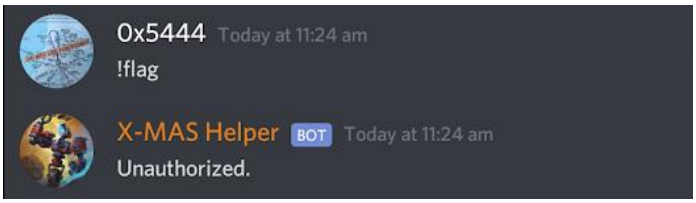
X-MAS CTF 2019

Written by Tom Pain (0x5444) for ProgPilot

X-MAS Helper was a web challenge as part of the 2019 X-MAS CTF organised by HTsP. X-MAS Helper is also the name of a Discord bot that resided in the event's Discord server. Quoting the challenge description:

> *"We have made this [Discord bot] to help us check the flags for various challenges by using the !flag command. This command is safe to use as it actively checks the user has the Organiser role assigned, so regular participants can't access the flags"*

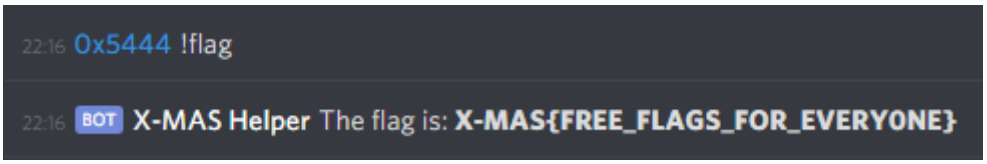
We are also provided with the section of the bot's source code that checks the user's role when the command is called. It shows exactly what the description said – if the user has the Organiser role it will give us the flag, otherwise it lets us know we are "Unauthorised." This is also reflected in the bot's actions in the main server.



The key to solving the challenge is getting the bot in your own Discord server.
Normally you invite a bot to a Discord server using a link provided by the bot creator which contains a bot ID and a permissions index (an integer that is based off the bot's required permissions).
This is an example invite link for the Pokécord bot:
https://discordapp.com/oauth2/authorize?client_id=365975655608745985&scope=bot&permissions=387072
We can get the client ID for the X-MAS Helper bot by going into the Discord client settings, the appearance tab and turning on "Developer mode". Right-click on the bot name, select "Copy ID" and paste that into the link. Leave the scope alone and set the permissions to 8 (which represents Administrator), after which you can invite the bot to one of your servers.

To obtain the flag, give yourself a role entitled “Organiser”, and run “!flag” in any channel, hopefully revealing the flag.

Note: The above method for adding a Discord bot to your server should work in all cases, except where the bot is not set to public by the developer. In this case, only they are able to add the bot to a server.



Challenge description