

Day 9 - Requests

Scenario

Task 14  [Day 9] Requests



McSkidy has been going keeping inventory of all the infrastructure but he finds a random web server running on port 3000. All he receives when accessing '/' is

```
{"value": "s", "next": "f"}
```

McSkidy needs to access the next page at /f(which is the value received from the data above) and keep track of the value at each step(in this case 's'). McSkidy needs to do this until the 'value' and 'next' data have the value equal to 'end'.

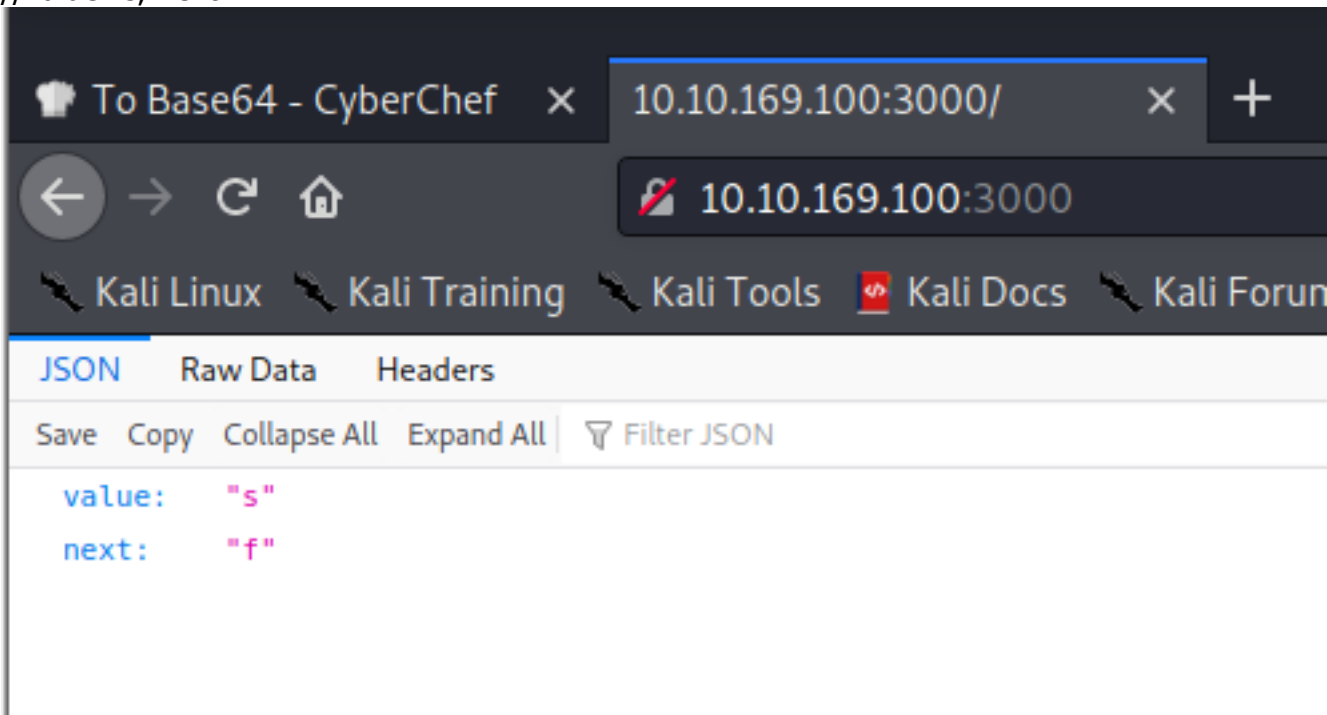
You can access the machines at the following IP:

- 10.10.169.100

Things to note about this challenge:

- The JSON object retrieved will need to be converted from unicode to ASCII(as shown in the supporting material)
- All the values retrieved until the 'end' will be the flag(end is not included in the flag)

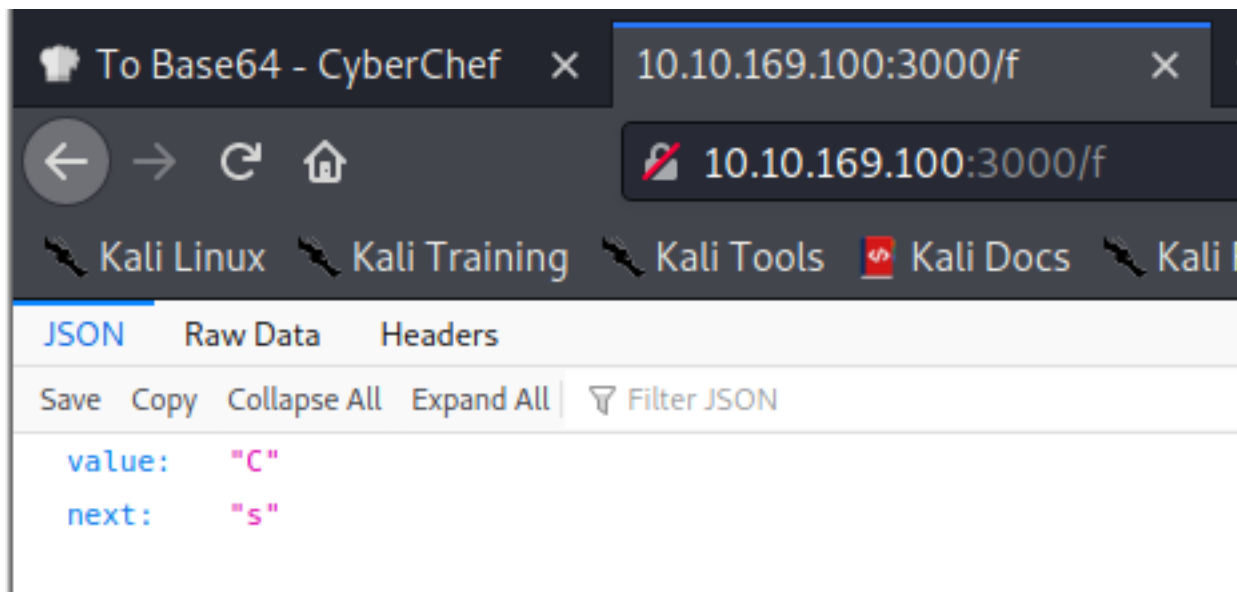
so let's check out the webpage
//value=s, next=f ?



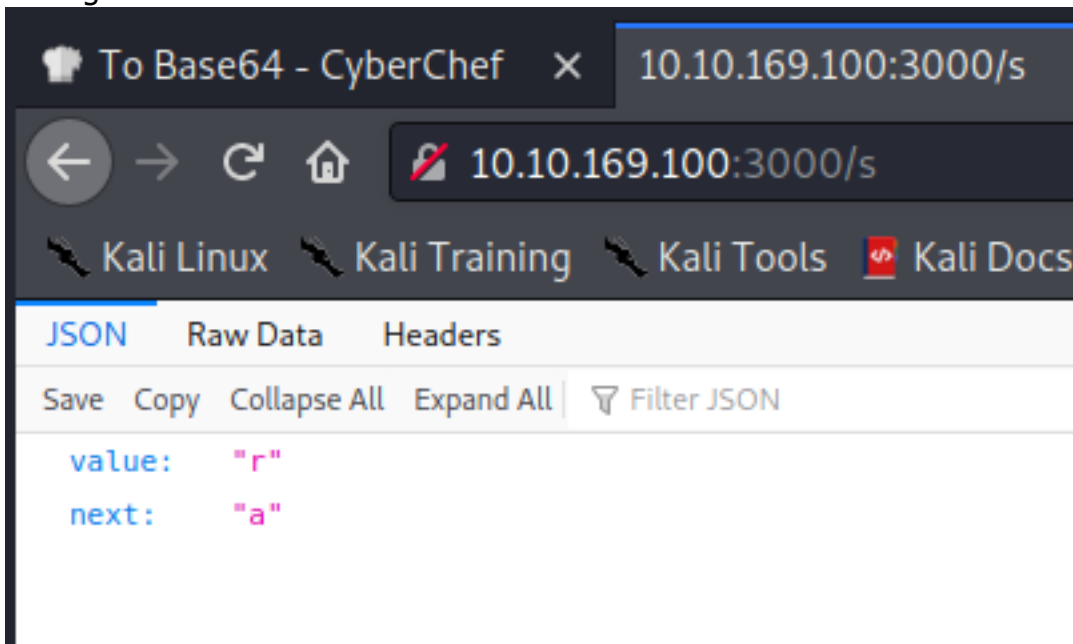
The screenshot shows a web browser window with the address bar displaying `10.10.169.100:3000/`. The browser's developer tools are open, showing the JSON response from the server. The response is a JSON object with two keys: `value` and `next`. The `value` key has a value of `"s"` and the `next` key has a value of `"f"`.

JSON	Raw Data	Headers
Save	Copy	Collapse All
Expand All	Filter JSON	
value:	"s"	
next:	"f"	

let's try out placing the next key value into the directory & it works!



testing the next value 's'



so it seems like we need to use the next value as the directory name to capture our flags by combining the value we get

we can do that by writing a simple python requests script

```

import requests

host = '10.10.169.100'
port = 3000

value = ''
url = 'http://' + host + ':' + str(port)

while(1):
    print("[*] Browsing url: " + url)

    req = requests.get(url)
    jsonValue = req.json()

    value += jsonValue['value']
    url = 'http://' + host + ':' + str(port) + '/' + jsonValue['next']

    if('end' in url):
        print("Value: " + value)
        break;

```

now let's capture our flag!

```

(nobodyata1@0xDEADBEEF) ~[~/Desktop/research
$ python3 day9Challenge.py
[*] Browsing url: http://10.10.169.100:3000
[*] Browsing url: http://10.10.169.100:3000/f
[*] Browsing url: http://10.10.169.100:3000/s
[*] Browsing url: http://10.10.169.100:3000/a
[*] Browsing url: http://10.10.169.100:3000/g
[*] Browsing url: http://10.10.169.100:3000/q
[*] Browsing url: http://10.10.169.100:3000/n
[*] Browsing url: http://10.10.169.100:3000/t
[*] Browsing url: http://10.10.169.100:3000/m
[*] Browsing url: http://10.10.169.100:3000/b
[*] Browsing url: http://10.10.169.100:3000/i
Value: sCrIPtKiDdend

```

Question: What is the value of the flag?
-sCrIPtKiDdend