README

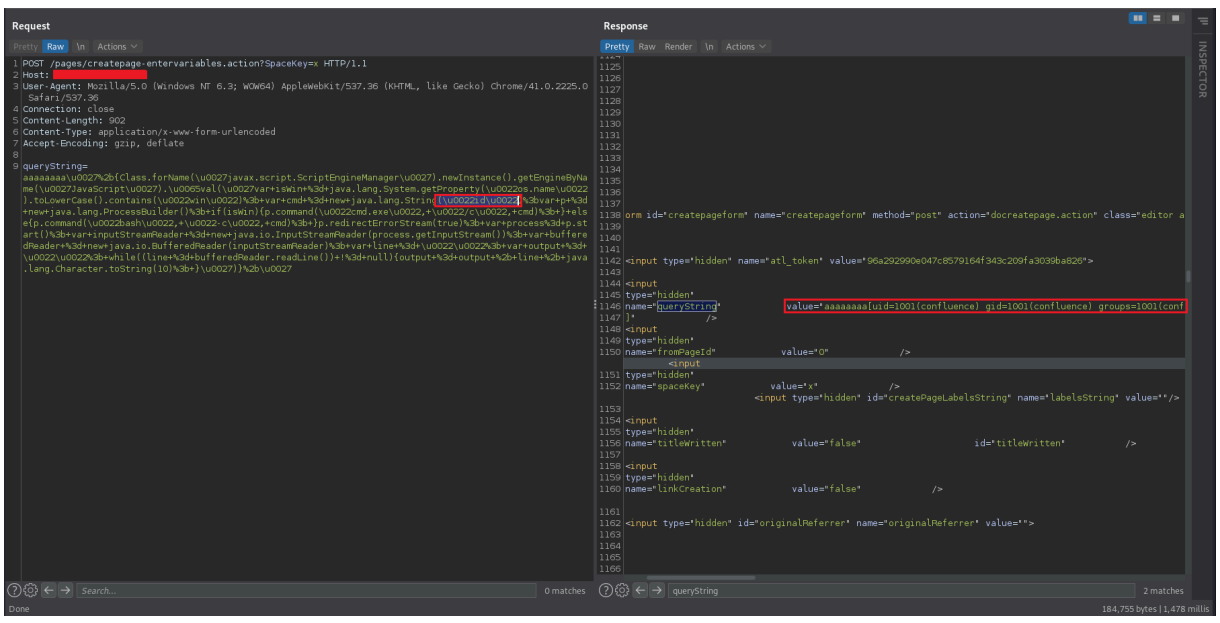
CVE-2021-26084 - Confluence Server Webwork OGNL injection

- 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

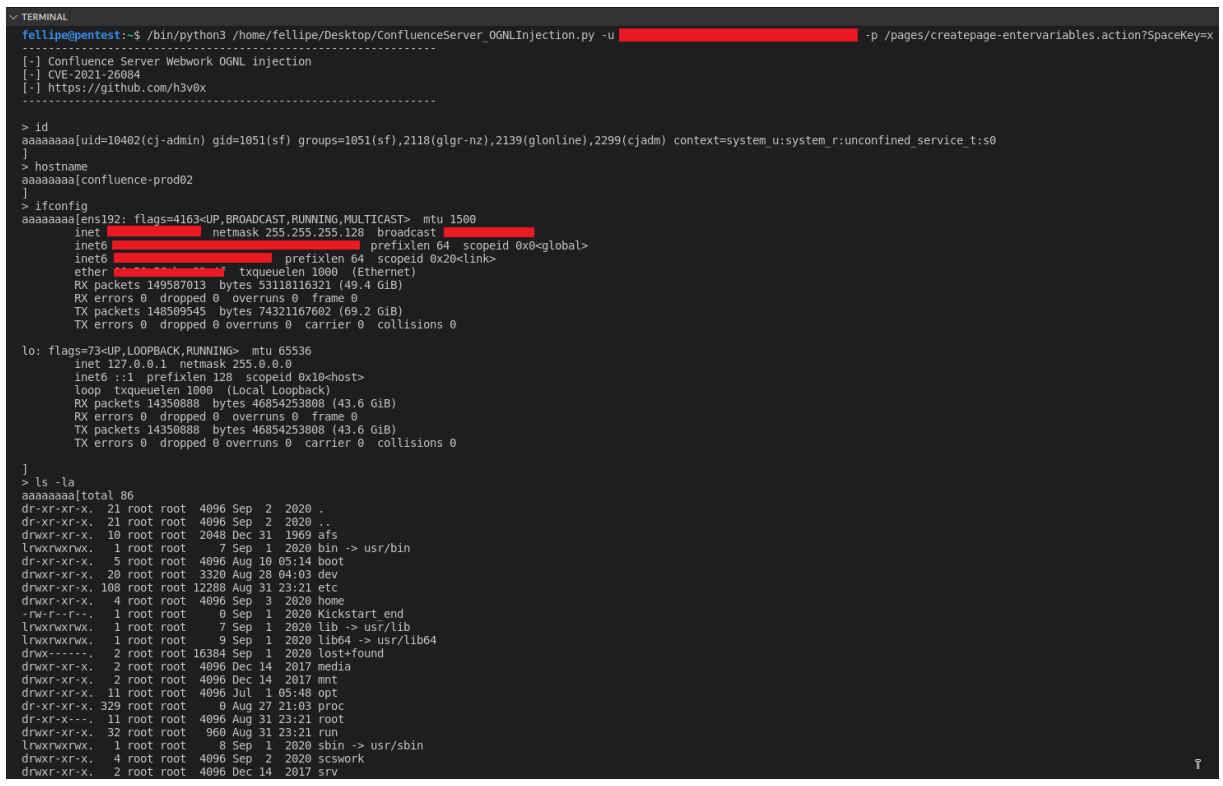
Commands:

```
$ 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**



- 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