

首先得先装好泛微 ec9。

装好之后服务器目录有三个文件存在。



Ecology 是主程序目录

Jdk 是 java 的 jdk 目录

Resin 是中间件目录

把这三个文件从服务端拷贝到本地

如果是虚拟机环境，ecology 这个文件是没法直接拷出来的。

因为内部文件太多了，需要打成压缩包拷出来。

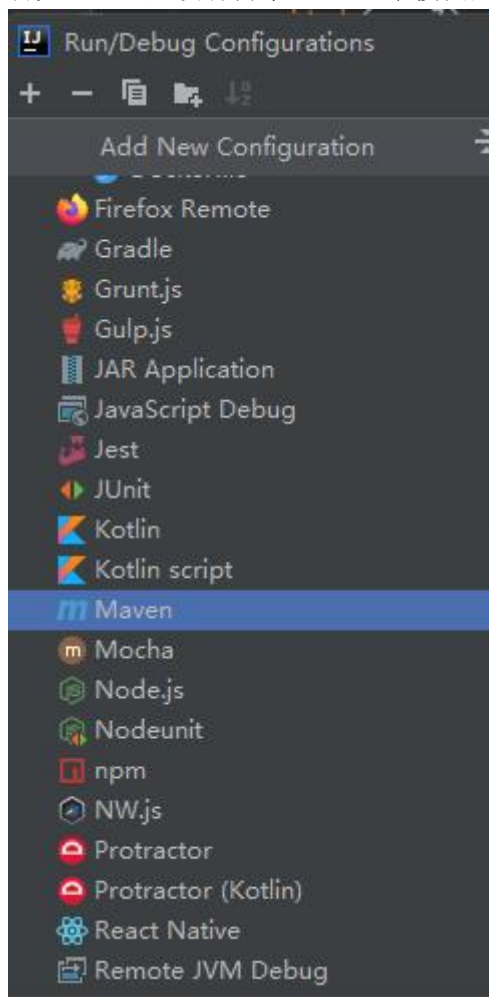
拷贝到本地之后，参考泛微官方进行环境搭建，按照官方步骤一步步来就好：

[//e-cloudstore.com/doc.html?appId=c6a9ae6e47b74d4da04c935ed51d177a&maxImgWidth](https://e-cloudstore.com/doc.html?appId=c6a9ae6e47b74d4da04c935ed51d177a&maxImgWidth)

=800

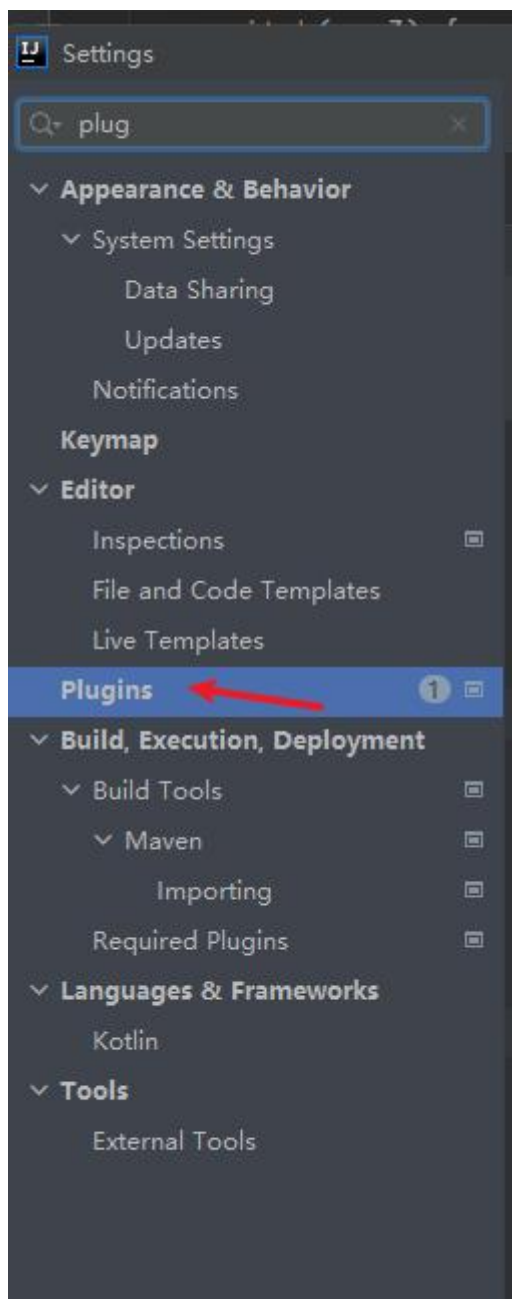
这里着重讲一下远程调试的部分，因为很坑

首先，idea 是没有自带 resin 这个模块的

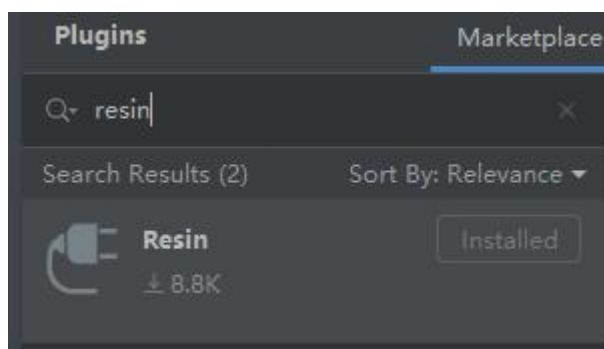


关注公众号：hack之道，回复关键词：2022，获取渗透工具、教程

Resin 模块需要自行下载  
这里 File-->Setting-->Plugins



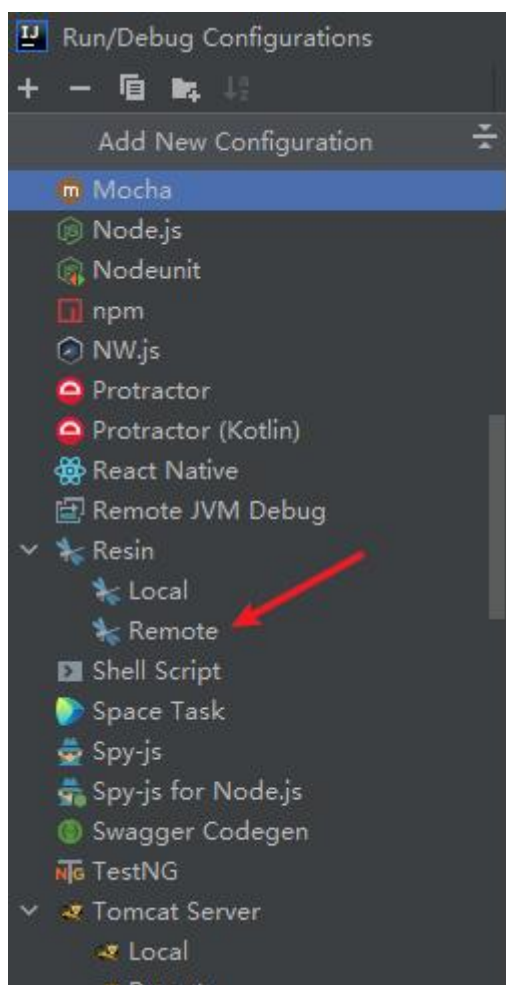
搜索并且安装好



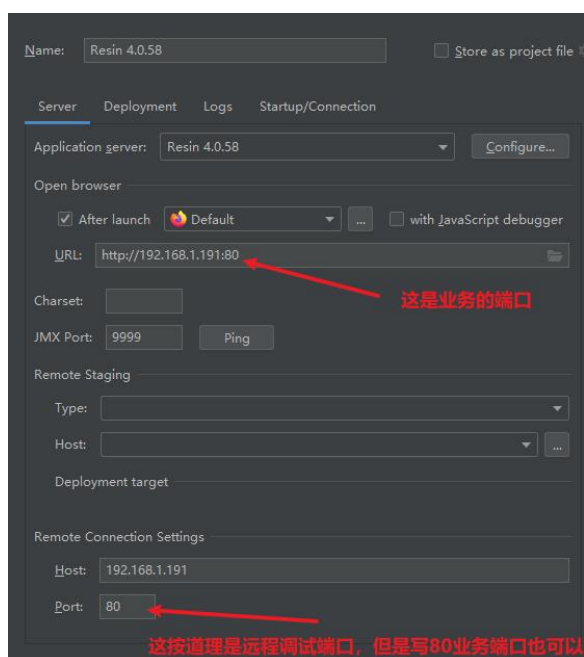
加我微信好友（stonefor345），拉你进2022护网微信交流群

关注公众号：hack之道，回复关键词：2022，获取渗透工具、教程

然后在 configuration 里面就可以选择了

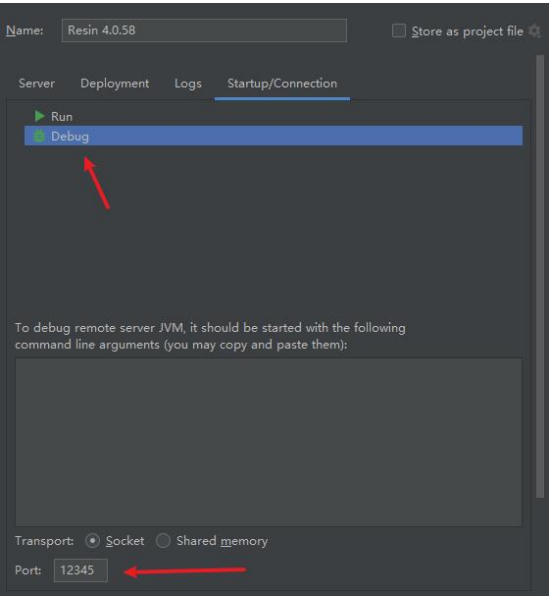


因为我这里配置的是远程调试环境，业务环境跑在了远端服务器上  
这里配置强调几个点，一个是端口的问题



加我微信好友（stonefor345），拉你进2022护网微信交流群

再一个是 debug 模式下的 jvm 端口问题



这个要和远程服务器配置的端口一致

```
# Arg passed directly to the JVM
jvm_args : -Xdebug -Xrunjdwp:transport=dt_socket,address=12345,server=y,suspend=n -Dcom.sun.management.jvm_mode=server
```

如果都配好了，一定要把服务器那台机器重启一次。  
注意，这里不是重启服务，而是重启服务器。  
因为不重启就会一直显示这个错

```
Error running 'Resin 4.0.58': Unable to open debugger port (192.168.1.191:12345): java.net.ConnectException "Connection timed out: connect"
```

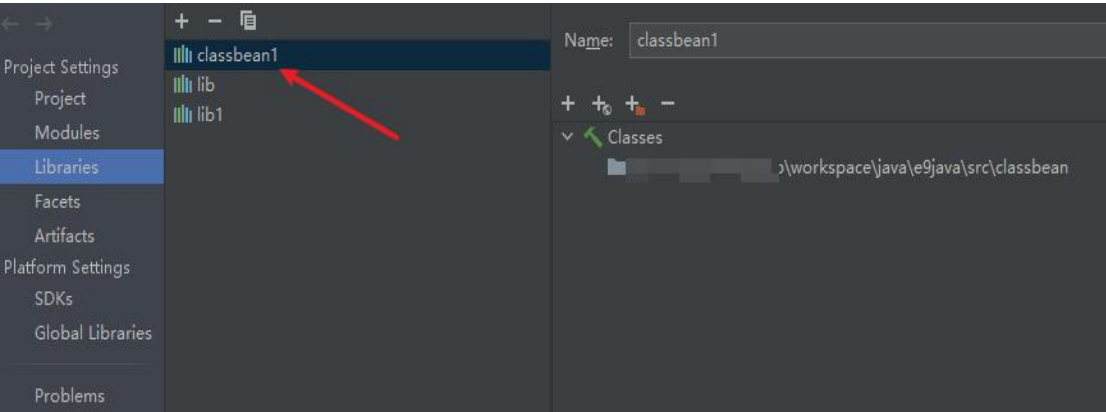
原因未知

如果服务器重启完毕，连接成功了会是这个样子

```
Connected to server
Connected to the target VM, address: '192.168.1.191:12345', transport: 'socket'
```

这就代表已经连接上了

下一个坑点，源码调试部分。  
这里是需要把整个 classbean 加入到 lib 里面的，不然无法给 class 文件下断点。



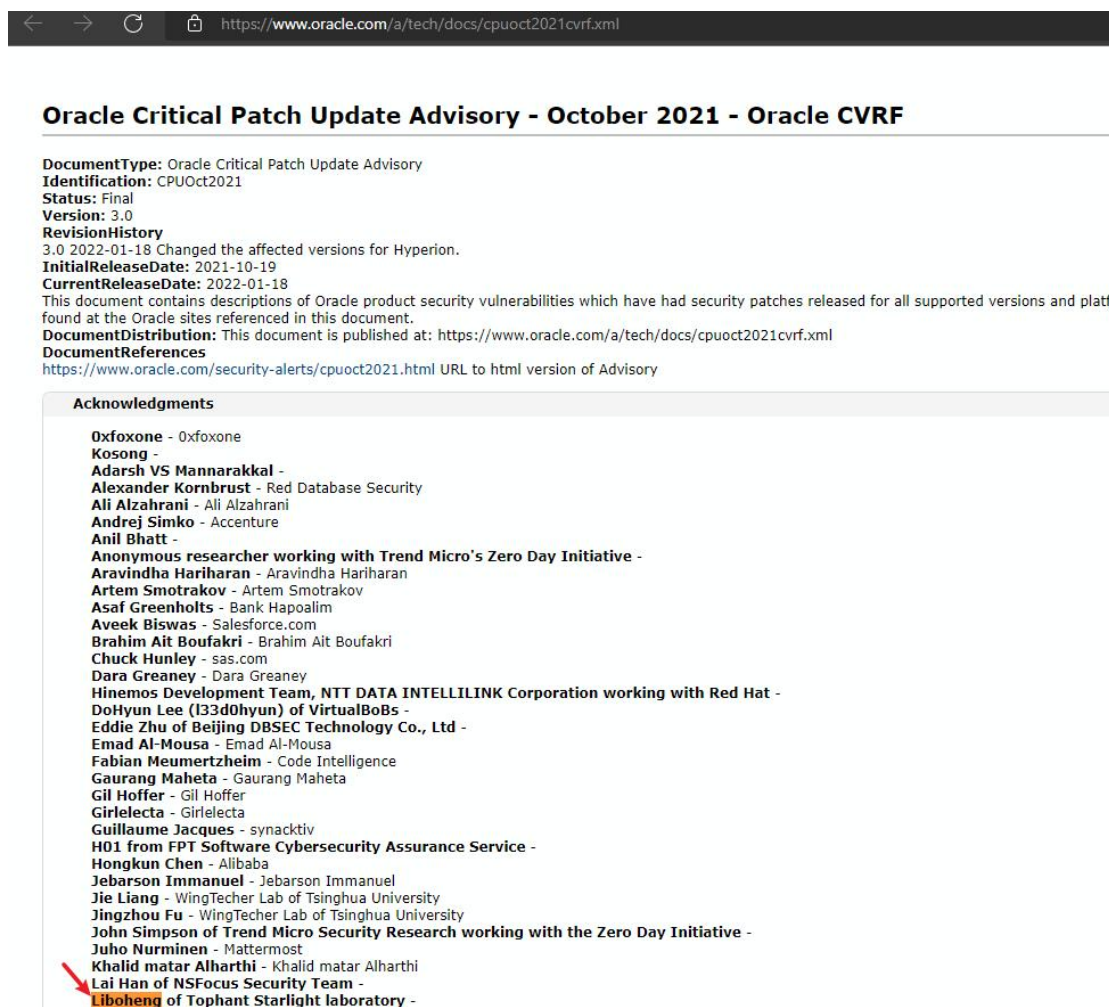
这一步其实在官方的步骤哪里有写的很明白，但是由于我第一次添加路径的时候添加到了别的 classbean（我本地放了好几个 ecology），因此一直不成功，排错排了半天，最后叫朋友 CVE 哥帮我看一下才整好了。

CVE 哥很牛逼，人狠话不多，附上 github 地址。

//<https://github.com/coolboy0816>

天天抓着 weblogic 挖，被 oracle 致谢了 N 次。

- **Liboheng** of Tophant Starlight laboratory: CVE-2022-21420



Oracle Critical Patch Update Advisory - October 2021 - Oracle CVRF

**DocumentType:** Oracle Critical Patch Update Advisory  
**Identification:** CPUOct2021  
**Status:** Final  
**Version:** 3.0  
**RevisionHistory:**  
3.0 2022-01-18 Changed the affected versions for Hyperion.  
**InitialReleaseDate:** 2021-10-19  
**CurrentReleaseDate:** 2022-01-18  
This document contains descriptions of Oracle product security vulnerabilities which have had security patches released for all supported versions and platform found at the Oracle sites referenced in this document.  
**DocumentDistribution:** This document is published at: <https://www.oracle.com/a/tech/docs/cpuoct2021cvrf.xml>  
**DocumentReferences:**  
<https://www.oracle.com/security-alerts/cpuoct2021.html> URL to html version of Advisory

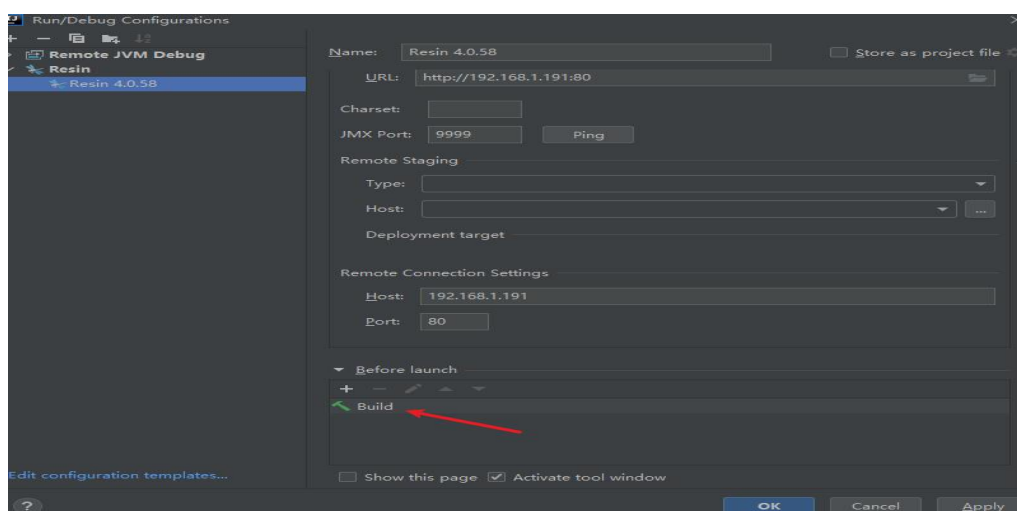
**Acknowledgments**

- Oxfoxone - Oxfoxone
- Kosong -
- Adarsh VS Mannarakkal -
- Alexander Kornbrust - Red Database Security
- Ali Alzahrani - Ali Alzahrani
- Andrej Simko - Accenture
- Anil Bhatt -
- Anonymous researcher working with Trend Micro's Zero Day Initiative -
- Aravindha Hariharan - Aravindha Hariharan
- Artem Smotrakov - Artem Smotrakov
- Asaf Greenholts - Bank Hapoalim
- Aveek Biswas - Salesforce.com
- Brahim Ait Boufakri - Brahim Ait Boufakri
- Chuck Hunley - sas.com
- Dara Greaney - Dara Greaney
- Hinemos Development Team, NTT DATA INTELLILINK Corporation working with Red Hat -
- DoHyun Lee (I33d0hyun) of VirtualBoBs -
- Eddie Zhu of Beijing DBSEC Technology Co., Ltd -
- Emad Al-Mousa - Emad Al-Mousa
- Fabian Meumertzheim - Code Intelligence
- Gaurang Maheta - Gaurang Maheta
- Gil Hoffer - Gil Hoffer
- Girlelecta - Girlelecta
- Guillaume Jacques - synacktiv
- H01 from FPT Software Cybersecurity Assurance Service -
- Hongkun Chen - Alibaba
- Jeberson Immanuel - Jeberson Immanuel
- Jie Liang - WingTecher Lab of Tsinghua University
- Jingzhou Fu - WingTecher Lab of Tsinghua University
- John Simpson of Trend Micro Security Research working with the Zero Day Initiative -
- Juho Nurminen - Mattermost
- Khalid matar Alharthi - Khalid matar Alharthi
- Lai Han of NSFfocus Security Team -
- Liboheng** of Tophant Starlight laboratory -

哈哈哈，CVE 哥 yyds。

言归正传，如果路径对了，就没啥大问题了。  
这里还有一些小细节。

关注公众号：hack之道，回复关键词：2022，获取渗透工具、教程



Resin 的 Configuration 这里默认是自带 build 的，记得直接给他干掉，调试不需要 build。

还有 ecology 的源码需要直接拷贝到 src 下面的文件夹，不要拷 idea 里面，会报错，因为太大了。

在拷贝完毕之后，会有很长的一段时间建立 index，需要等待。

最后如果一切都搞完了，就尝试下个断点，能够成功断下来，就说明环境搭建成功了。

Eg:



这里我在 getUsercheck 方法这里下断点。

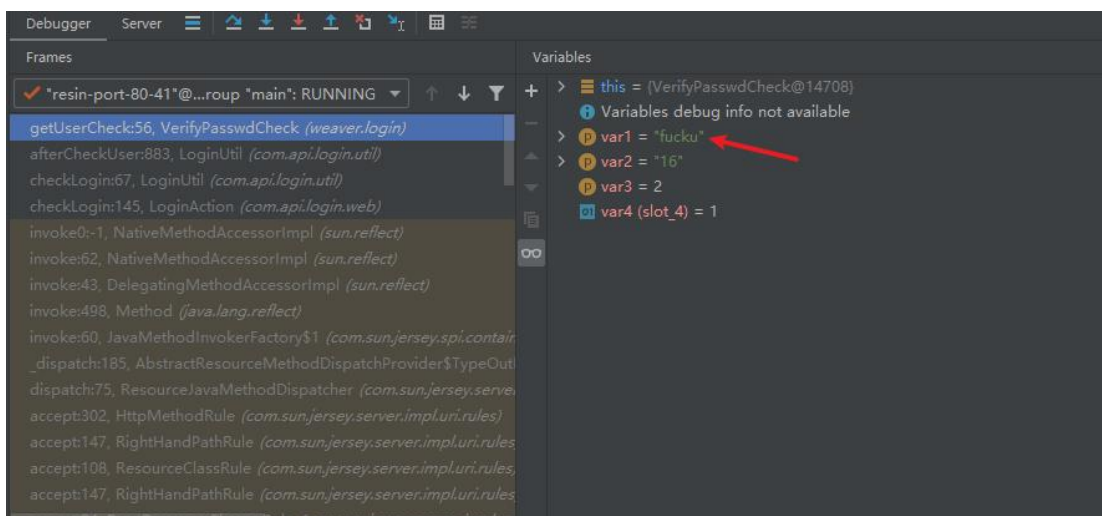
然后前端输入账号密码：



加我微信好友（stonefor345），拉你进2022护网微信交流群

关注公众号：hack之道，回复关键词：2022，获取渗透工具、教程

然后发现成功断下来了：



以上，测试通过，源码调试环境搭建成功。

Done

加我微信好友（stonefor345），拉你进2022护网微信交流群