白帽子昵称: 白袜子

漏洞描述

漏洞URL: 如果是Web就填写此项

https://api.v***.cc/druid/index.html

简要描述:漏洞说明、利用条件、危害等

https://api.v***.cc/druid/index.html

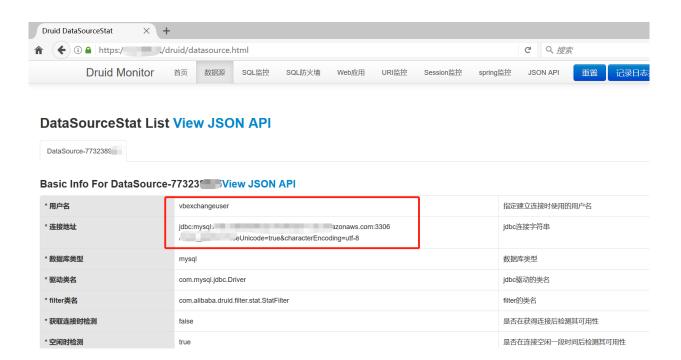
Druid未授权访问, 泄露部分敏感信息

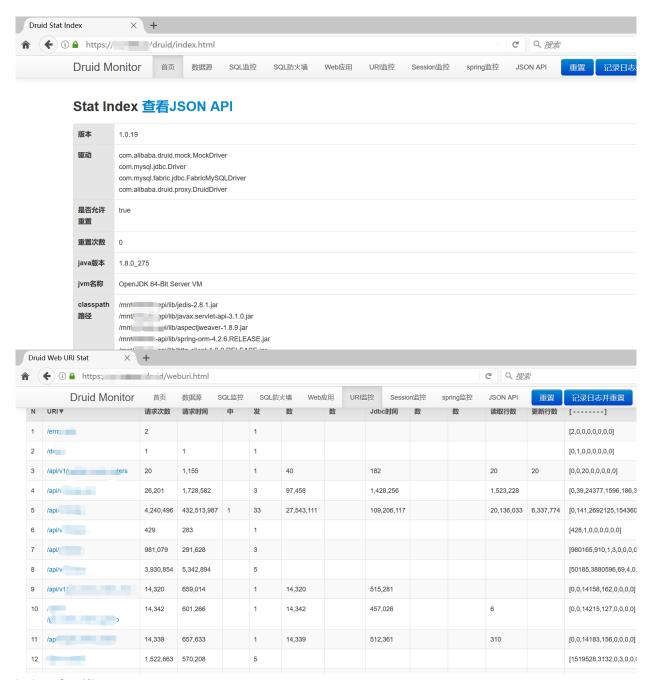
漏洞证明:

此处可找到找到api接口地址: https://api.****.cc/



存在Druid接口未做访问控制: https://api.****.cc/druid/index.html





漏洞利用代码:

https://api.**.cc/druid/index.html

修复方案:

做访问控制

漏洞总结

Druid是阿里巴巴出品,为监控而生的数据库连接池., Druid提供了监控功能, 如监控SQL的执行时间、监控Web URI的请求、Session监控, 当开发者配置不当时可能造成未授权访问

以下为druid常见的web路径,如果可直接访问到相关页面,说明存在Druid未授权访问/druid/websession.html/system/druid/websession.html/webpage/system/druid/websession.html