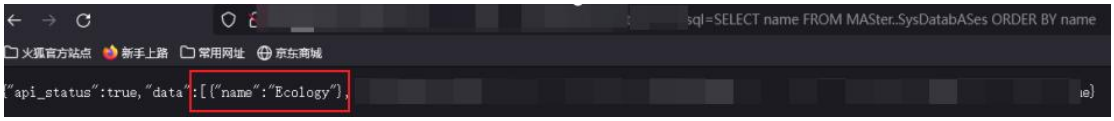
最近 weaver 出了补丁，看了下，审计了两个 1day。

利用链条是
mssql 注入拿账密+登录后台 upload 拿 shell

刚好有个项目正好遇到了，那就拿 1day 试试水吧。

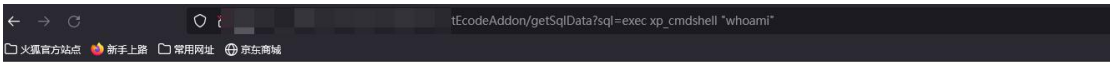
直接 select @@version 查询版本
发现是 2019，最新版的 mssql。

查询库中所有的表名
SELECT name FROM MASter..SysDatabASes ORDER BY name

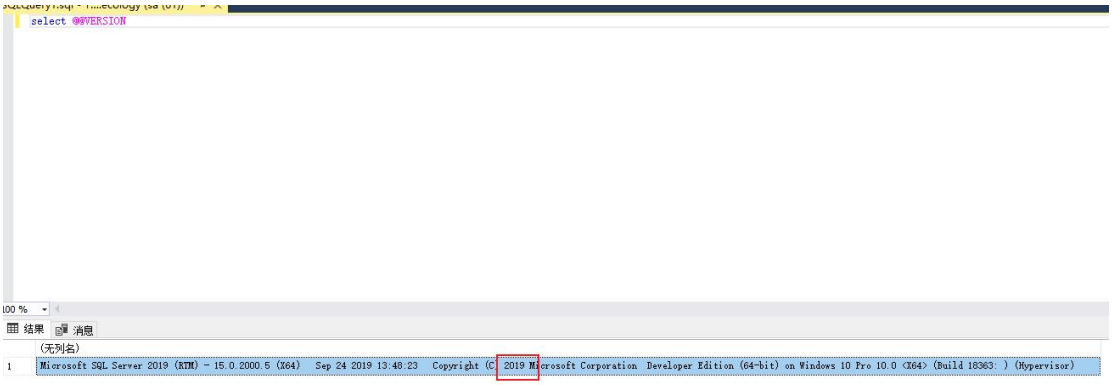


发现就是正常的 ecology 的数据库

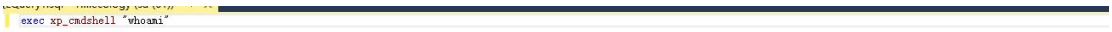
尝试 xp_cmdshell 执行命令



这里发现直接 404 了
一般不会直接 404，404 一般就是 waf
这里可以在本地搭建环境来测试
我这里同样选用 2019 版本



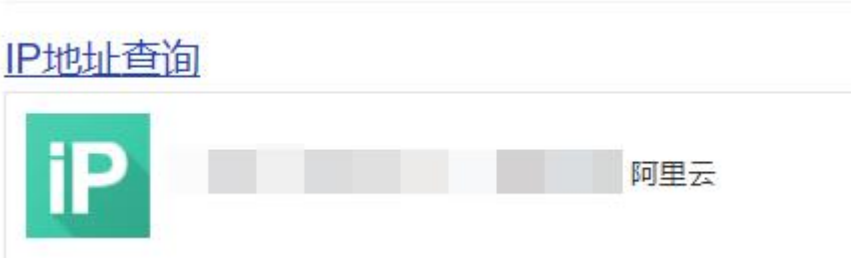
然后执行 exec xp_cmdshell “whoami”



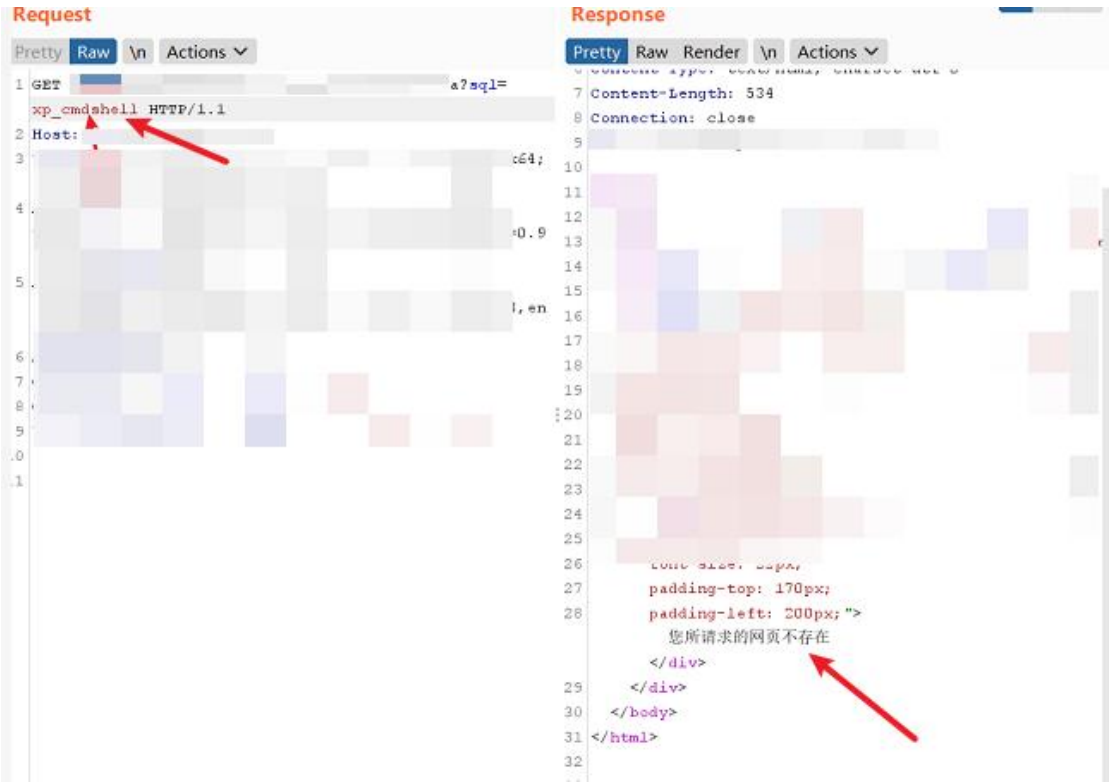
这里微软做了详细的说明，就是被关闭了。
那么即便在网页上的回显，也不应该是 404，因此判定被 waf 拦截了。

于是可以进一步推演两个思路
1、绕 waf 执行 xp_cmdshell 尝试落地 cs 马直接上线
2、Mssql 注出密码，后台 upload，利用 webshell 上线

这里先看看主机归属：



阿里云的 waf 一贯是盯着关键词搞，这里测试下：



这里只输入了 xp_cmdshell,直接被 404 了，可以证明确实是正则匹配了关键词。

而且绕 waf，听起来就费劲，拜拜。
先尝试 2 思路吧，如果 2 也被 waf 拦截了，再尝试 1。

这里还不死心，秉承着能偷懒就偷懒的情绪，用 sqlmap 试了下：

```
[CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
```

不行，还是被 waf 拦了，那么还是手工注入吧。

查询当前用户：

Dbo 权限

因为我是有源码的，也有数据库的 schema，这里直接查询密码：
这里只要是 weaver ecology 的站，其实都可以用这个语句来查密码：
select password as id from HrmResourceManager

是一串 md5，然后丢到 md5 查询站去查询

这里成功查询
然后直接登录
账号一般是 sysadmin

后面的 upload 部分过段时间再写出来吧，现在全网好像还没人放出这个洞。
枪打出头鸟，先稳一波。

其实现在不管是 weaver 也好，seeyon 也好，补丁都是要密码的，哈哈哈。
至于怎么获得密码，就各凭本事了。
我又不乱来，厂商为什么要防我一手呢，真是。。。
done