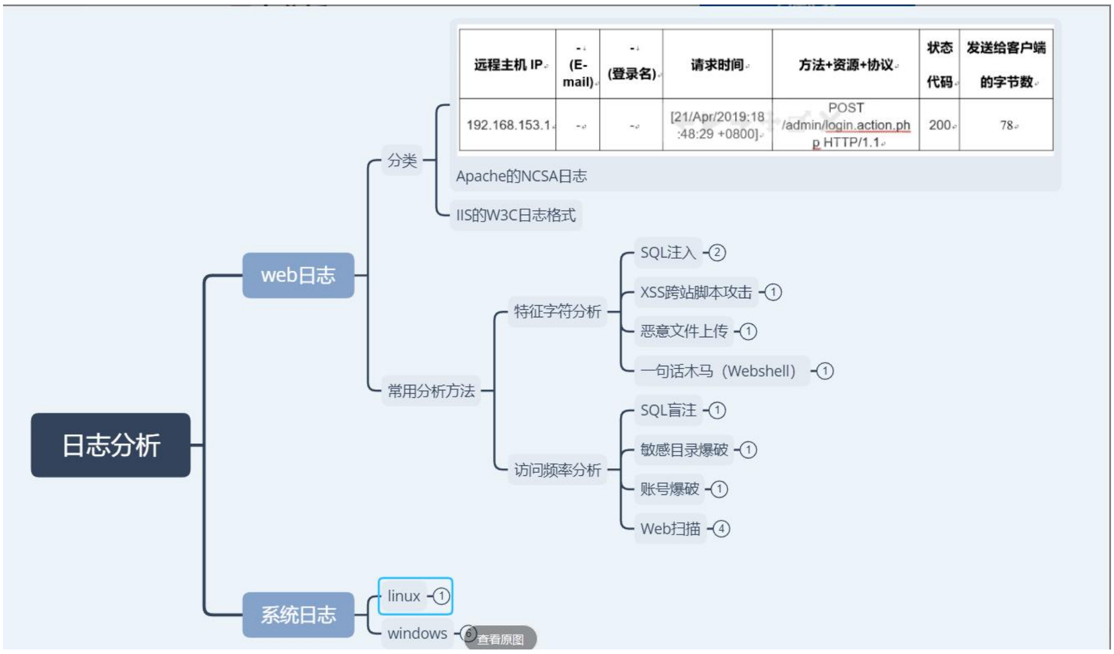
CTF-MISC-日志分析

总结——用于备忘和交流学习

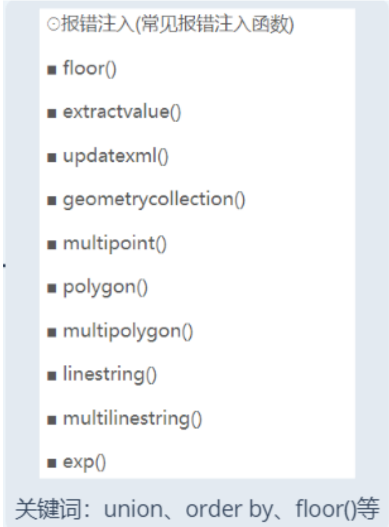


远程主机 IP	- (E-mail)	- (登录名)	请求时间	方法+资源+协议	状态代码	发送给客户端的字节数
192.168.153.1	-	-	[21/Apr/2019:18:48:29 +0800]	POST /admin/login.action.php HTTP/1.1	200	78

一.web 日志分析

（一）、特征字符分析

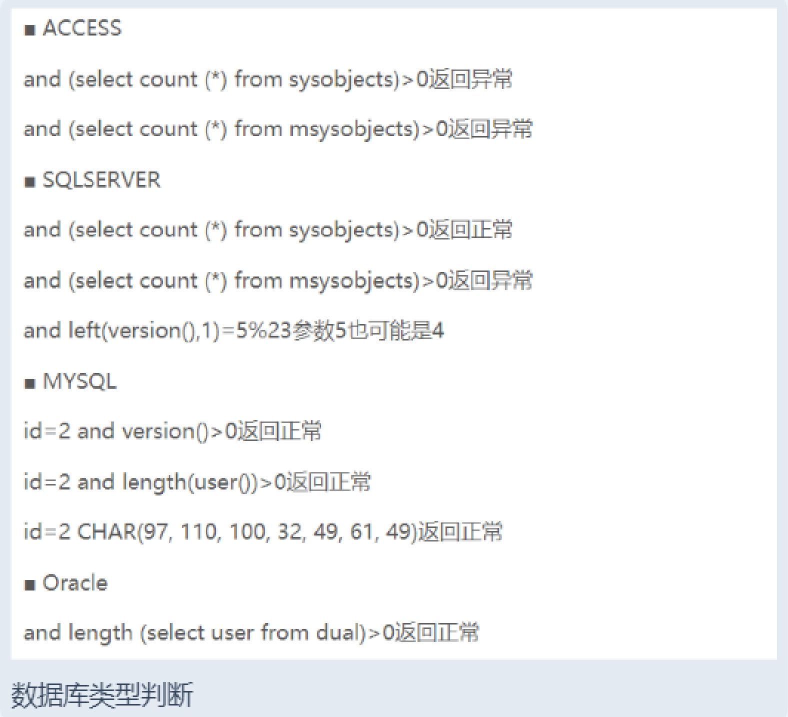
1. sql 注入



⊙报错注入(常见报错注入函数)

- floor()
- extractvalue()
- updatexml()
- geometrycollection()
- multipoint()
- polygon()
- multipolygon()
- linestring()
- multilinestring()
- exp()

关键词：union、order by、floor()等



■ ACCESS

and (select count (*) from sysobjects)>0返回异常

and (select count (*) from msysobjects)>0返回异常

■ SQLSERVER

and (select count (*) from sysobjects)>0返回正常

and (select count (*) from msysobjects)>0返回异常

and left(version(),1)=5%23参数5也可能是4

■ MYSQL

id=2 and version()>0返回正常

id=2 and length(user())>0返回正常

id=2 CHAR(97, 110, 100, 32, 49, 61, 49)返回正常

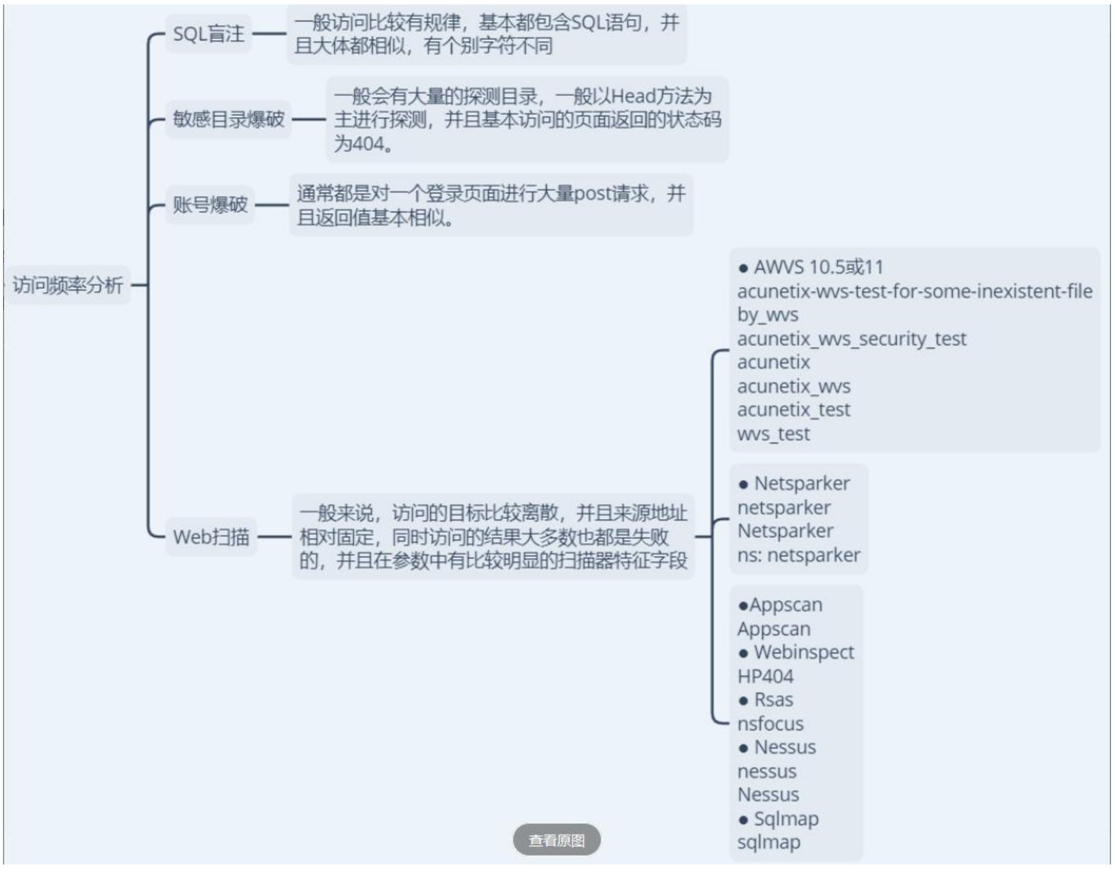
■ Oracle

and length (select user from dual)>0返回正常

数据库类型判断

有以上信息可以尝试判断是否为 sql 注入

（二）、访问频率分析

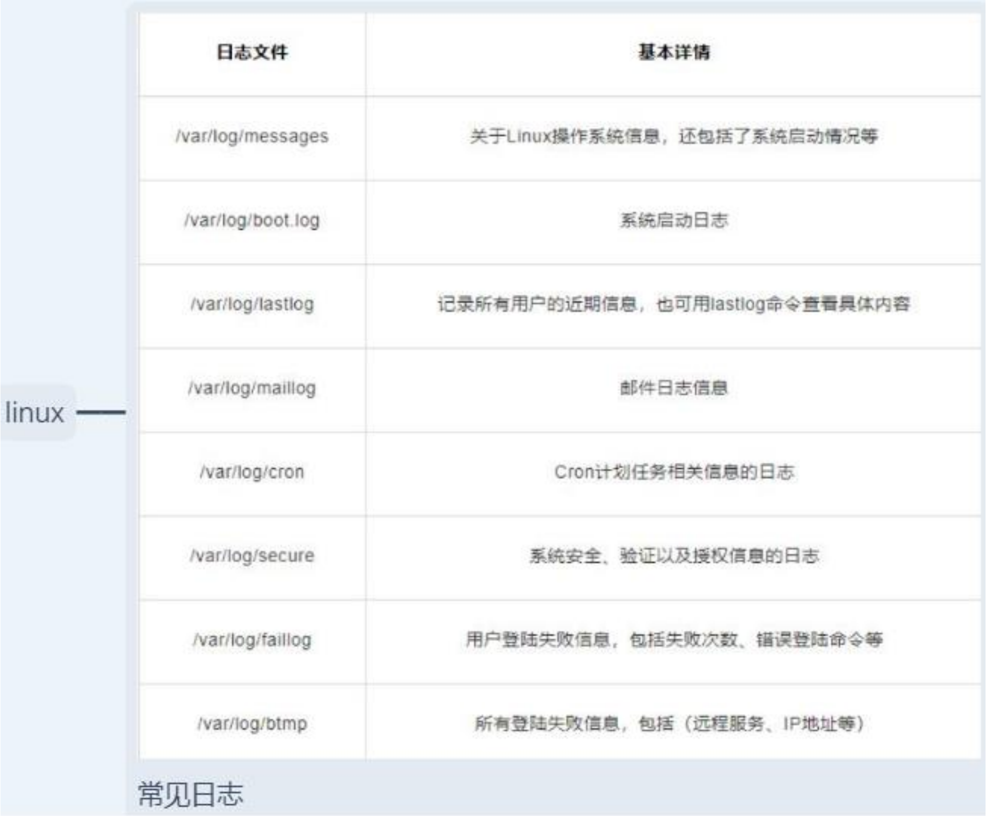


访问频率分析

- SQL盲注 — 一般访问比较有规律，基本都包含SQL语句，并且大体都相似，有个别字符不同
- 敏感目录爆破 — 一般会有大量的探测目录，一般以Head方法为主进行探测，并且基本访问的页面返回的状态码为404。
- 账号爆破 — 通常都是对一个登录页面进行大量post请求，并且返回值基本相似。
- Web扫描 — 一般来说，访问的目标比较离散，并且来源地址相对固定，同时访问的结果大多数也都是失败的，并且在参数中有比较明显的扫描器特征字段
  - ● AWVS 10.5或11
acunetix-wvs-test-for-some-inexistent-file
by_wvs
acunetix_wvs_security_test
acunetix
acunetix_wvs
acunetix_test
wvs_test
  - ● Netsparker
netsparker
Netsparker
ns: netsparker
  - ●Appscan
Appscan
● Webinspect
HP404
● Rsas
nsfocus
● Nessus
nessus
Nessus
● Sqlmap
sqlmap

二.系统日志分析

（一）、Linux

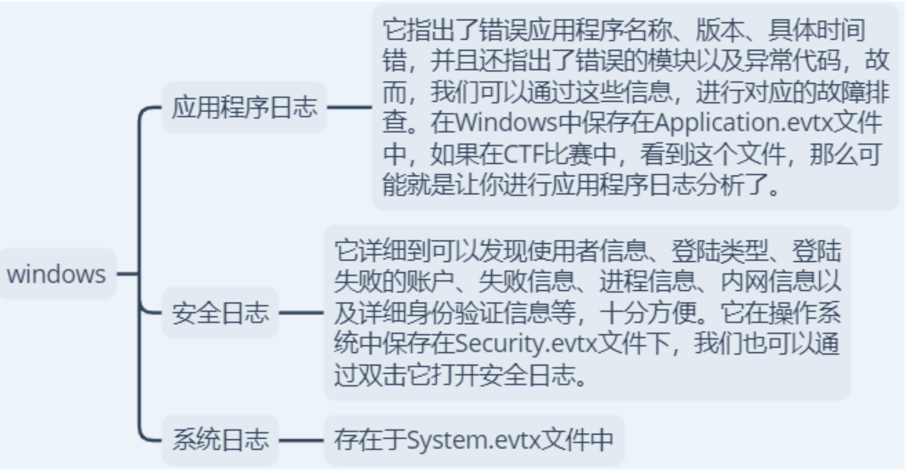


linux

日志文件	基本详情
/var/log/messages	关于Linux操作系统信息，还包括了系统启动情况等
/var/log/boot.log	系统启动日志
/var/log/lastlog	记录所有用户的近期信息，也可用lastlog命令查看具体内容
/var/log/maillog	邮件日志信息
/var/log/cron	Cron计划任务相关信息的日志
/var/log/secure	系统安全、验证以及授权信息的日志
/var/log/faillog	用户登陆失败信息，包括失败次数、错误登陆命令等
/var/log/btmp	所有登陆失败信息，包括（远程服务、IP地址等）

常见日志

（二）、Windows



windows

应用程序日志：它指出了错误应用程序名称、版本、具体时间错，并且还指出了错误的模块以及异常代码，故而，我们可以通过这些信息，进行对应的故障排查。在Windows中保存在Application.evtx文件中，如果在CTF比赛中，看到这个文件，那么可能就是让你进行应用程序日志分析了。

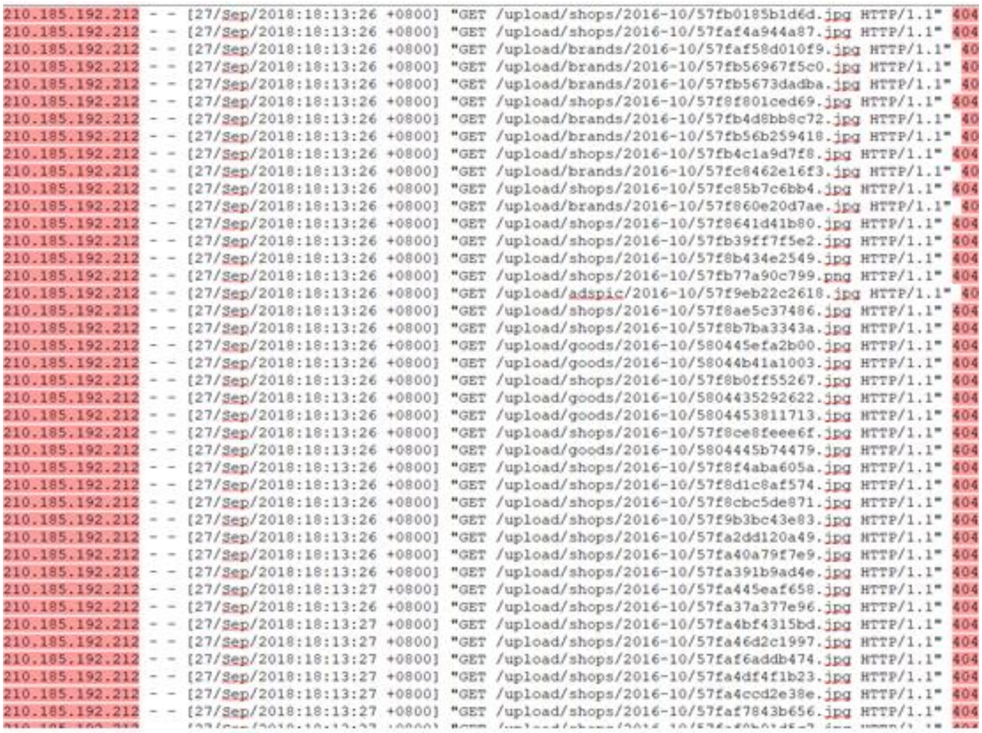
安全日志：它详细到可以发现使用者信息、登陆类型、登陆失败的账户、失败信息、进程信息、内网信息以及详细身份验证信息等，十分方便。它在操作系统中保存在Security.evtx文件下，我们也可以通过双击它打开安全日志。

系统日志：存在于System.evtx文件中

三.练习题

题目来源：墨者学院

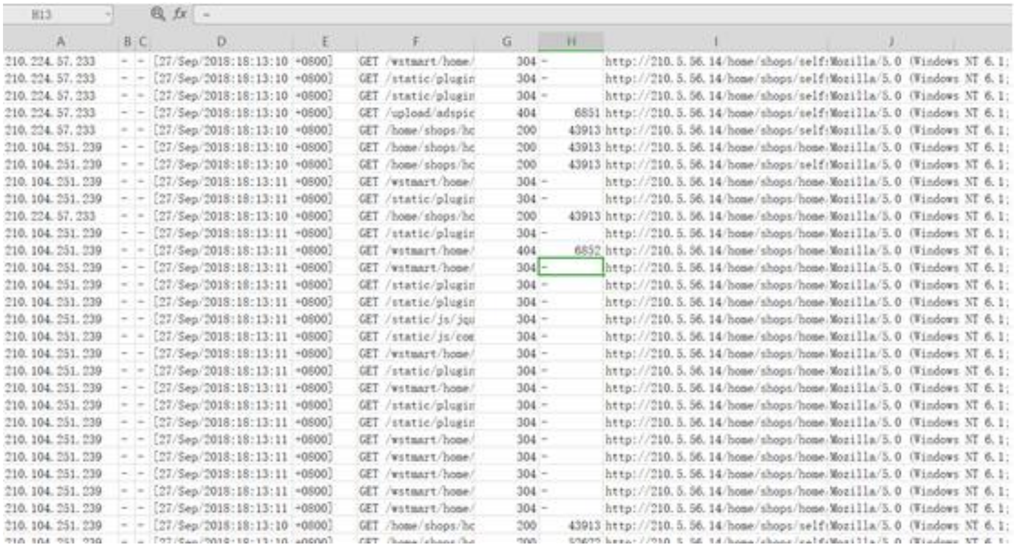
1.分析谷歌爬虫 IP



```
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fb0185b1d6d.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57faf4a944a87.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/brands/2016-10/57faf58d010f9.jpg HTTP/1.1" 40
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/brands/2016-10/57fb56967f5c0.jpg HTTP/1.1" 40
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/brands/2016-10/57fb5673dadba.jpg HTTP/1.1" 40
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8f801ced69.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/brands/2016-10/57fb4d8bb8c72.jpg HTTP/1.1" 40
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/brands/2016-10/57fb56b259418.jpg HTTP/1.1" 40
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fb4c1a9d7f8.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/brands/2016-10/57fc8462e16f3.jpg HTTP/1.1" 40
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fc85b7c6bb4.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/brands/2016-10/57f860e20d7ae.jpg HTTP/1.1" 40
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8641d41b80.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fb39ff7f5e2.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8b434e2549.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fb77a90c799.png HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/adspic/2016-10/57f9eb22c2618.jpg HTTP/1.1" 40
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8ae5c37486.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8b7ba3343a.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/goods/2016-10/580445efa2b00.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/goods/2016-10/58044b41a1003.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8b0ff55267.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/goods/2016-10/5804435292622.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/goods/2016-10/5804453811713.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8ce8feee6f.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/goods/2016-10/5804445b74479.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8f4aba605a.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8d1c8af574.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f8cbc5de871.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57f9b3bc43e83.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fa2dd120a49.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fa40a79f7e9.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fa391b9ad4e.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:27 +0800] "GET /upload/shops/2016-10/57fa445eaf658.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:26 +0800] "GET /upload/shops/2016-10/57fa37a377e96.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:27 +0800] "GET /upload/shops/2016-10/57fa4bf4315bd.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:27 +0800] "GET /upload/shops/2016-10/57fa46d2c1997.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:27 +0800] "GET /upload/shops/2016-10/57faf6addb474.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:27 +0800] "GET /upload/shops/2016-10/57fa4df4f1b23.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:27 +0800] "GET /upload/shops/2016-10/57fa4ccd2e38e.jpg HTTP/1.1" 404
210.185.192.212 - - [27/Sep/2018:18:13:27 +0800] "GET /upload/shops/2016-10/57faf7843b656.jpg HTTP/1.1" 404
```

先标记 404，观察到其密集存在于 210.185.192.212 这个 IP，再同时标记上这个 IP，确实是一直在爬取网站的图片。输入 IP 即得到 key。

我最先使用的是 notepad++，后来想到用 excal 按空格分列显示，可以更直观和方便。

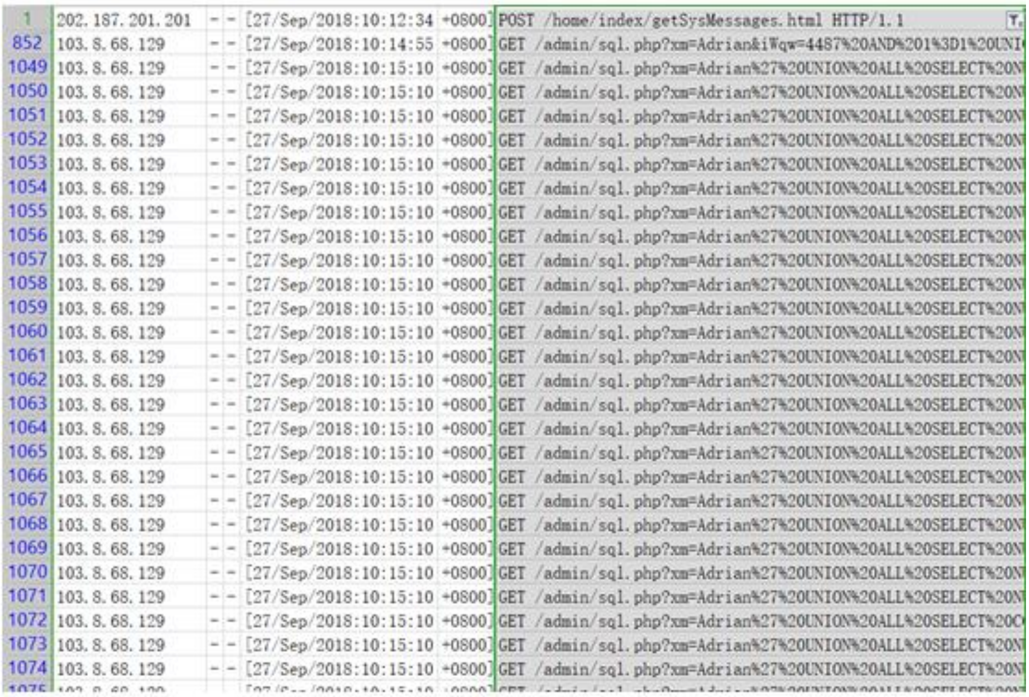


A	B	C	D	E	F	G	H	I	J
210.224.57.233	-	-	[27/Sep/2018:18:13:10	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/self	Mozilla/5.0 (Windows NT 6.1;
210.224.57.233	-	-	[27/Sep/2018:18:13:10	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/self	Mozilla/5.0 (Windows NT 6.1;
210.224.57.233	-	-	[27/Sep/2018:18:13:10	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/self	Mozilla/5.0 (Windows NT 6.1;
210.224.57.233	-	-	[27/Sep/2018:18:13:10	+0800]	GET /upload/adspic	404	6851	http://210.5.56.14/home/shops/self	Mozilla/5.0 (Windows NT 6.1;
210.224.57.233	-	-	[27/Sep/2018:18:13:10	+0800]	GET /home/shops/hc	200	43913	http://210.5.56.14/home/shops/self	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:10	+0800]	GET /home/shops/hc	200	43913	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:10	+0800]	GET /home/shops/hc	200	43913	http://210.5.56.14/home/shops/self	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.224.57.233	-	-	[27/Sep/2018:18:13:10	+0800]	GET /home/shops/hc	200	43913	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	404	6852	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/js/jqu	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/js/com	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /static/plugin	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:11	+0800]	GET /wstmart/home/	304	-	http://210.5.56.14/home/shops/home	Mozilla/5.0 (Windows NT 6.1;
210.104.251.239	-	-	[27/Sep/2018:18:13:10	+0800]	GET /home/shops/hc	200	43913	http://210.5.56.14/home/shops/self	Mozilla/5.0 (Windows NT 6.1;

2.分析 sql 注入 1

筛选相应的关键词如 union、select 等，或者筛选可能存在的 sql.php 这样的关键词（实际中不可能出现）

关键字：union all select



```
1     202.187.201.201  - - [27/Sep/2018:10:12:34 +0800] POST /home/index/getSysMessages.html HTTP/1.1
852   103.8.68.129     - - [27/Sep/2018:10:14:55 +0800] GET /admin/sql.php?xm=Adrian&iWqw=4487%20AND%201%3D1%20UNI
1049  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1050  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1051  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1052  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1053  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1054  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1055  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1056  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1057  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1058  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1059  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1060  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1061  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1062  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1063  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1064  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1065  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1066  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1067  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1068  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1069  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1070  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1071  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1072  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20C
1073  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
1074  103.8.68.129     - - [27/Sep/2018:10:15:10 +0800] GET /admin/sql.php?xm=Adrian%27%20UNION%20ALL%20SELECT%20N
```

3.分析 sql 注入 2

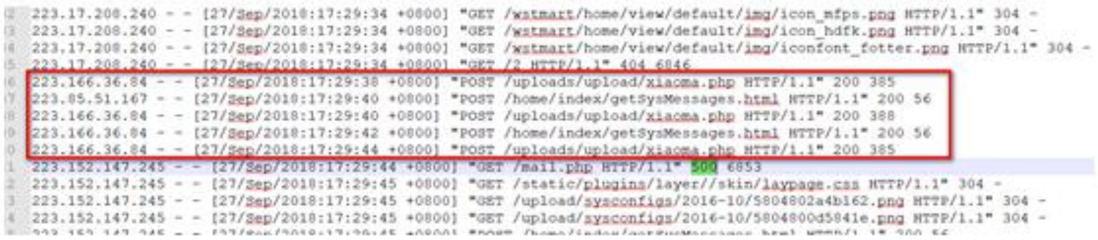
有两个文件：系统日志文件和 sql 日志文件

先分析 sql 文件，搜索 sql 相关语句，我搜索的是 admin，还有 order by、information_schema，union、table_name、and 1=2、and 1=1 即可

再根据这条命令对应的时间，在系统日志中匹配 IP 地址就可得到 key

4.中断 web 业务的 IP

根据 http 的状态码，500 为 web 服务中断，直接搜索字符串 500，找到在此之前有什么 post 之类的导致系统不能提供服务，得到 key

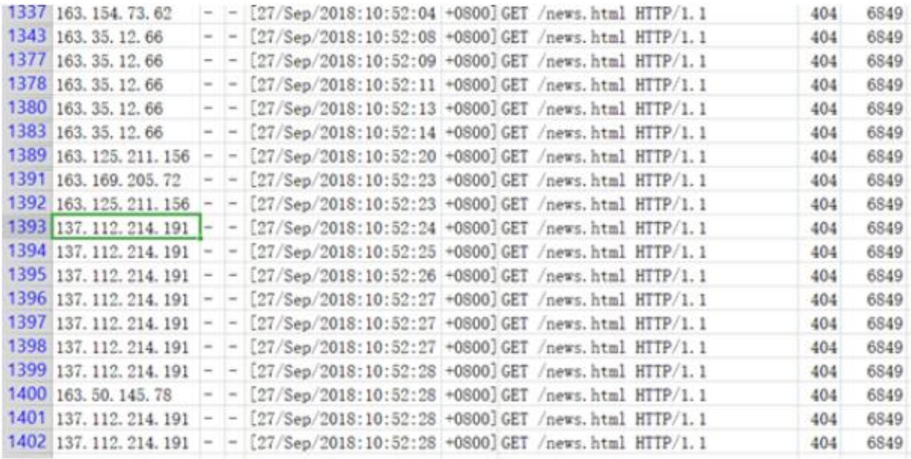


```
223.17.208.240 - - [27/Sep/2018:17:29:34 +0800] "GET /wstmart/home/view/default/img/icon_mfps.png HTTP/1.1" 304 -
223.17.208.240 - - [27/Sep/2018:17:29:34 +0800] "GET /wstmart/home/view/default/img/icon_hdfk.png HTTP/1.1" 304 -
223.17.208.240 - - [27/Sep/2018:17:29:34 +0800] "GET /wstmart/home/view/default/img/iconfont_fotter.png HTTP/1.1" 304 -
223.17.208.240 - - [27/Sep/2018:17:29:34 +0800] "GET /2 HTTP/1.1" 404 6846
223.166.36.84 - - [27/Sep/2018:17:29:38 +0800] "POST /uploads/upload/xiaoma.php HTTP/1.1" 200 385
223.85.51.167 - - [27/Sep/2018:17:29:40 +0800] "POST /home/index/getSysMessages.html HTTP/1.1" 200 56
223.166.36.84 - - [27/Sep/2018:17:29:40 +0800] "POST /uploads/upload/xiaoma.php HTTP/1.1" 200 388
223.166.36.84 - - [27/Sep/2018:17:29:42 +0800] "POST /home/index/getSysMessages.html HTTP/1.1" 200 56
223.166.36.84 - - [27/Sep/2018:17:29:44 +0800] "POST /uploads/upload/xiaoma.php HTTP/1.1" 200 385
223.152.147.245 - - [27/Sep/2018:17:29:44 +0800] "GET /mail.php HTTP/1.1" 500 6853
223.152.147.245 - - [27/Sep/2018:17:29:45 +0800] "GET /static/plugins/layer//skin/laypage.css HTTP/1.1" 304 -
223.152.147.245 - - [27/Sep/2018:17:29:45 +0800] "GET /upload/sysconfigs/2016-10/5804802a4b162.png HTTP/1.1" 304 -
223.152.147.245 - - [27/Sep/2018:17:29:45 +0800] "GET /upload/sysconfigs/2016-10/5804800d5841e.png HTTP/1.1" 304 -
223.152.147.245 - - [27/Sep/2018:17:29:45 +0800] "POST /home/index/getSysMessages.html HTTP/1.1" 200 56
```

5.境外 IP 攻击分析

背景：某网站遭到境外 ip 攻击，请通过 log，找到找到访问 news.html 最多的境外 IP 地址

筛选访问了 news.html 的所有 IP 地址，发现很多 404 的界面，猜测存在注入，根据其次数大小进行尝试，找到目的 IP。其实看 IP 的组成都能分析出 137 开头的 IP 为境外 IP



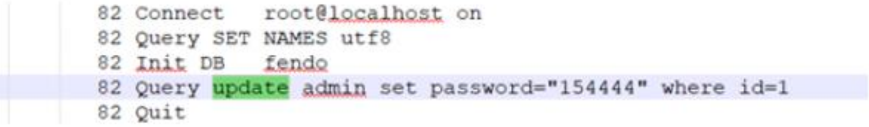
```
1337 163.154.73.62    - - [27/Sep/2018:10:52:04 +0800] GET /news.html HTTP/1.1   404  6849
1343 163.35.12.66     - - [27/Sep/2018:10:52:08 +0800] GET /news.html HTTP/1.1   404  6849
1377 163.35.12.66     - - [27/Sep/2018:10:52:09 +0800] GET /news.html HTTP/1.1   404  6849
1378 163.35.12.66     - - [27/Sep/2018:10:52:11 +0800] GET /news.html HTTP/1.1   404  6849
1380 163.35.12.66     - - [27/Sep/2018:10:52:13 +0800] GET /news.html HTTP/1.1   404  6849
1383 163.35.12.66     - - [27/Sep/2018:10:52:14 +0800] GET /news.html HTTP/1.1   404  6849
1389 163.125.211.156  - - [27/Sep/2018:10:52:20 +0800] GET /news.html HTTP/1.1   404  6849
1391 163.169.205.72   - - [27/Sep/2018:10:52:23 +0800] GET /news.html HTTP/1.1   404  6849
1392 163.125.211.156  - - [27/Sep/2018:10:52:23 +0800] GET /news.html HTTP/1.1   404  6849
1393 137.112.214.191  - - [27/Sep/2018:10:52:24 +0800] GET /news.html HTTP/1.1   404  6849
1394 137.112.214.191  - - [27/Sep/2018:10:52:25 +0800] GET /news.html HTTP/1.1   404  6849
1395 137.112.214.191  - - [27/Sep/2018:10:52:26 +0800] GET /news.html HTTP/1.1   404  6849
1396 137.112.214.191  - - [27/Sep/2018:10:52:27 +0800] GET /news.html HTTP/1.1   404  6849
1397 137.112.214.191  - - [27/Sep/2018:10:52:27 +0800] GET /news.html HTTP/1.1   404  6849
1398 137.112.214.191  - - [27/Sep/2018:10:52:27 +0800] GET /news.html HTTP/1.1   404  6849
1399 137.112.214.191  - - [27/Sep/2018:10:52:28 +0800] GET /news.html HTTP/1.1   404  6849
1400 163.50.145.78    - - [27/Sep/2018:10:52:28 +0800] GET /news.html HTTP/1.1   404  6849
1401 137.112.214.191  - - [27/Sep/2018:10:52:28 +0800] GET /news.html HTTP/1.1   404  6849
1402 137.112.214.191  - - [27/Sep/2018:10:52:28 +0800] GET /news.html HTTP/1.1   404  6849
```

在分析境外 IP 的时候还应该注意时区和时差

6. 更改管理员的密码

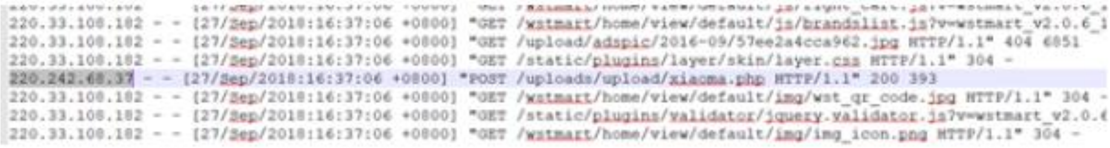
背景：某公司安全工程师发现公司有黑客入侵的痕迹，并更改了 admin 账户的密码，你能帮忙找一下更改 admin 账户密码的 IP 地址吗？

先对 sql 的日志搜索 update，在 16：37：06 时出现的修改



```
82 Connect    root@localhost on
82 Query SET NAMES utf8
82 Init DB    fendo
82 Query update admin set password="154444" where id=1
82 Quit
```

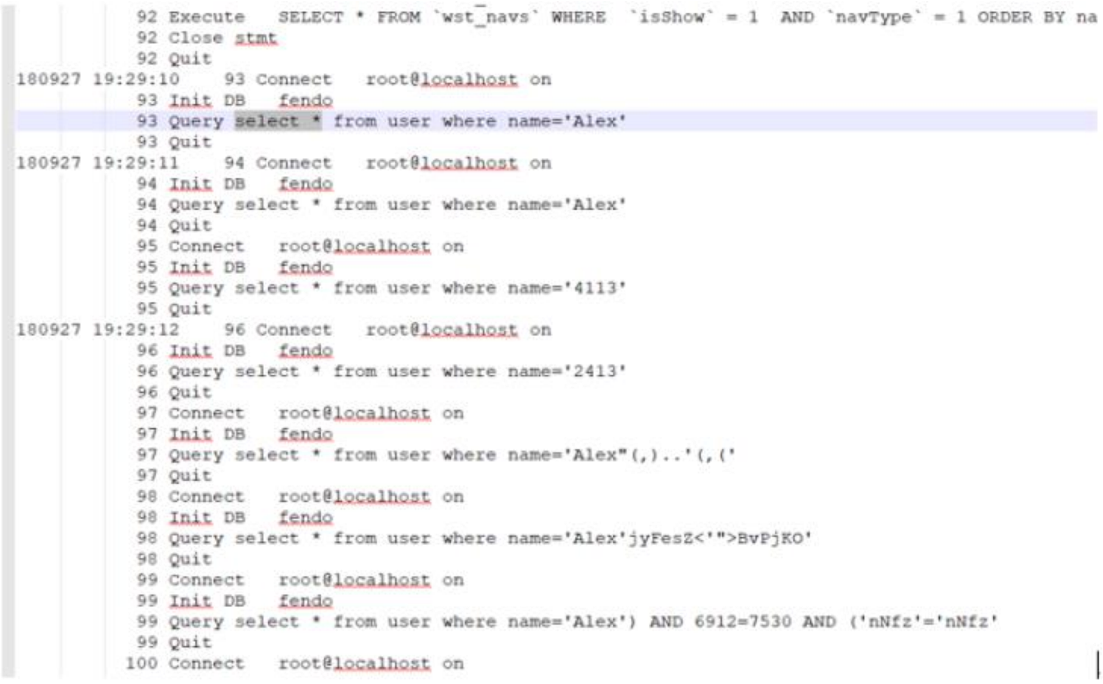
对应时间查找日志



```
220.33.108.182 - - [27/Sep/2018:16:37:06 +0800] "GET /wstmart/home/view/default/js/brandslist.js?v=wstmart_v2.0.6_1
220.33.108.182 - - [27/Sep/2018:16:37:06 +0800] "GET /upload/adspic/2016-09/57ee2a4cca962.jpg HTTP/1.1" 404 6851
220.33.108.182 - - [27/Sep/2018:16:37:06 +0800] "GET /static/plugins/layer/skin/layer.css HTTP/1.1" 304 -
220.242.68.37 - - [27/Sep/2018:16:37:06 +0800] "POST /uploads/upload/xiaoma.php HTTP/1.1" 200 393
220.33.108.182 - - [27/Sep/2018:16:37:06 +0800] "GET /wstmart/home/view/default/img/wst_qr_code.jpg HTTP/1.1" 304 -
220.33.108.182 - - [27/Sep/2018:16:37:06 +0800] "GET /static/plugins/validator/jquery.validator.js?v=wstmart_v2.0.6
220.33.108.182 - - [27/Sep/2018:16:37:06 +0800] "GET /wstmart/home/view/default/img/img_icon.png HTTP/1.1" 304 -
```

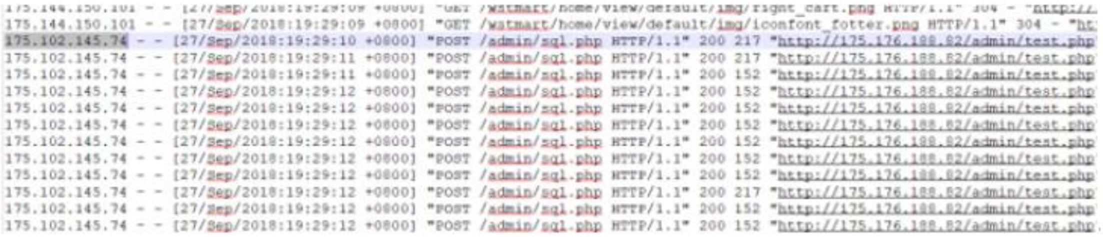
7. 拖库溯源

直接在 sql 日志里搜索“select *”，得到明显拖库痕迹



```
                92 Execute    SELECT * FROM `wst_navs` WHERE  `isShow` = 1  AND `navType` = 1 ORDER BY na
                92 Close stmt
                92 Quit
180927 19:29:10     93 Connect    root@localhost on
                93 Init DB    fendo
                93 Query select * from user where name='Alex'
                93 Quit
180927 19:29:11     94 Connect    root@localhost on
                94 Init DB    fendo
                94 Query select * from user where name='Alex'
                94 Quit
                95 Connect    root@localhost on
                95 Init DB    fendo
                95 Query select * from user where name='4113'
                95 Quit
180927 19:29:12     96 Connect    root@localhost on
                96 Init DB    fendo
                96 Query select * from user where name='2413'
                96 Quit
                97 Connect    root@localhost on
                97 Init DB    fendo
                97 Query select * from user where name='Alex"(,)..'(,('
                97 Quit
                98 Connect    root@localhost on
                98 Init DB    fendo
                98 Query select * from user where name='Alex'jyFesZ<'">BvPjKO'
                98 Quit
                99 Connect    root@localhost on
                99 Init DB    fendo
                99 Query select * from user where name='Alex') AND 6912=7530 AND ('nNfz'='nNfz'
                99 Quit
               100 Connect    root@localhost on
```

接着对应时间查找 IP，得到 key



```
175.144.150.101 - - [27/Sep/2018:19:29:09 +0800] "GET /wstmart/home/view/default/img/right_cart.png HTTP/1.1" 304 - "http://
175.144.150.101 - - [27/Sep/2018:19:29:09 +0800] "GET /wstmart/home/view/default/img/iconfont_fotter.png HTTP/1.1" 304 - "ht
175.102.145.74 - - [27/Sep/2018:19:29:10 +0800] "POST /admin/sql.php HTTP/1.1" 200 217 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:11 +0800] "POST /admin/sql.php HTTP/1.1" 200 217 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:11 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 217 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
175.102.145.74 - - [27/Sep/2018:19:29:12 +0800] "POST /admin/sql.php HTTP/1.1" 200 152 "http://175.176.188.82/admin/test.php
```

作者：Yilanere
链接：https://www.jianshu.com/p/bb5b4c31f4f5
来源：简书