

# 某shop API接口前台注入(通杀3.X)

TheKingOfDuck (/u/12470) / 2019-06-13 08:22:00 / 浏览数 10922

## 0x01 前言

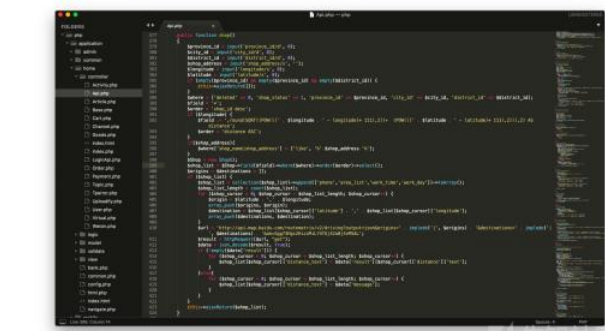
TPshop是国内应用范围大、覆盖面广的电商软件产品，基于此，历经5年的时间，而发展成为国内先进的具备成熟且标准化的电商平台技术方案提供商。“TPshop”的每一次新产品发布都引带头中国电商软件研发领域的潮流，持续为中国电子商务服务行业。同时公司建立了由多名科学家构成的行业及技术研究中心，对电商行业发展趋势、软件产品架构、技术性、新技术应用与创新等都做出了卓越贡献。

代码来源：

```
http://www.tp-shop.cn/download/
```

## 0x02 分析

跟踪到 /application/home/controller/Api.php 控制器中的 shop 方法：



(https://xzfile.aliyuncs.com/media/upload/picture/20190508175544-72108c04-7177-1.jpeg)

流程分析：

```
379~384 Line: 获取外部输入并赋值给变量
385~387 Line: $province_id, $district_id判断以上三个遍历是否为空，若成立返回空的json
388 Line: 将$province_id, $city_id, $district_id放入$where数组中以供SQL查询
389 Line: 定义变量$field并赋值为*
390 Line: 定义变量$order并赋值为shop_id desc
391 Line: 判断变量$longitude是否为真
392 Line: 将$longitude, $latitude拼接到SQL语句中并赋值到$field中
393 Line: 将$order赋值为distance ASC
395 Line: 判断$shop_address是否为真
396 Line: 将$shop_address放入$where数组中以供SQL查询
399 Line: 带入SQL查询
```

代码调试：

通过代码分析后发现 \$field 传入方法 field 中，并不会将这个变量中的值预编译，而是直接带入中执行，接着来调试！在399行后添加代码如下：

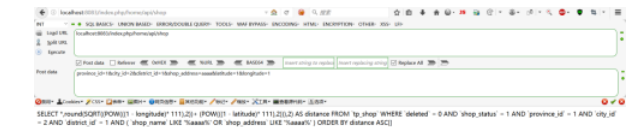
```
print Db::name('region')->getlastsql();
```

getlastsql 方法在tp框架中是返回SQL语句也可以说是监听，接着往下走，访问

```
http://localhost:8083/index.php/home/api/shop
```

POST包：

```
province_id=1&city_id=2&district_id=1&shop_address=aaaa&latitude=1&longitude=1
```



(https://xzfile.aliyuncs.com/media/upload/picture/20190508175603-7da3f8f8-7177-1.png)

为 longitude 参数赋值为 1'

先知社区

现在登录 (https://account.aliyun.com/)

社区小黑板 (/notice)

年度贡献榜	月度贡献榜
LeeH (/u/52868)	3
o°区 (/u/64530)	2
Youngmith (/u/56181)	2
000**** (/u/40035)	1
Bamboo (/u/13134)	1

## 目录

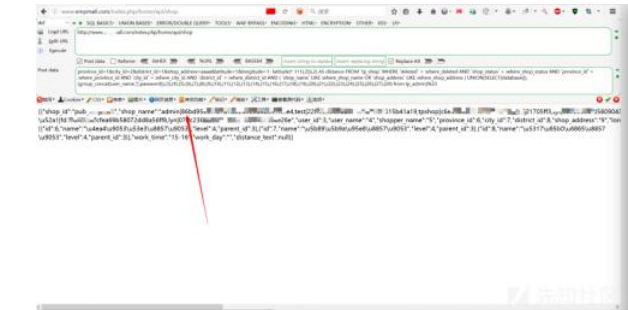
- 0x01 前言
- 0x02 分析
- 0x03 总结





(https://xzfile.aliyuncs.com/media/upload/picture/20190508180049-284df826-7178-1.png)

查用户：



(https://xzfile.aliyuncs.com/media/upload/picture/20190508180107-32dff2d0-7178-1.png)

(复现来源于互联网，如有打码不严还请手下留情。)

### 0x03 总结

贵州白马会头牌提醒您，代码千万行，安全第一条，开发(PDO)不规范，系统被插惨。



(https://xzfile.aliyuncs.com/media/upload/picture/20190508180425-a8d5933c-7178-1.jpeg)

关注 | 2    点击收藏 | 1

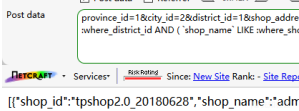
上一篇： PDF双重释放漏洞CVE-2018... (/t/5094)

下一篇： pwn return-to-di... (/t/5120)

8 条回复



IronHeart (u/11848)    2019-05-13 14:45:22



(https://xzfile.aliyuncs.com/media/upload/picture/20190513144507-a54d2fce-754a-1.png)

2.0貌似也存在

0    回复Ta



0o0\*\*\*\* (u/9750)    2019-05-14 10:14:16

这个可以直接get webshell

0    回复Ta



TheKingOfDuck (u/12470)    2019-05-14 13:29:21

@150\*\*\*\*1116 (u/11848) 2.x在此洞之前就有注入的 所以就懒得去测是否影响2.x了

0    回复Ta




TheKingOfDuck (u/12470)    2019-05-14 13:30:44

@0o0\*\*\*\* (u/9750) 能力有限 暂未挖掘到可以直接Getshell的 师傅手上有洞的话分享下咯 (一起投稿的还有这cms的其他两洞 敬请关注咯)

0    回复Ta

 postma\*\*\*@lanme (/u/9643) 2019-05-15 10:28:23  
@CoolCat (/u/12470) 有tp5和tp6的漏洞嘛


♡ 0 回复Ta

 TheKingOfDuck (/u/12470) 2019-05-15 23:20:57  
@postma\*\*\*@lanme (/u/9643) 啊哈? ?? 我去官网下载来审计时最新的也就不过3.x啊?




(<https://xfile.aliyuncs.com/media/upload/picture/20190515232037-fdeb28ee-7724-1.jpg>)

♡ 0 回复Ta

 影 (/u/18182) 2019-05-17 21:28:08  
进步很快啊,佩服

♡ 0 回复Ta

 Xm17 (/u/7245) 2020-01-30 19:17:14  
input 么有过滤? ?

♡ 0 回复Ta

登录 ([https://account.aliyun.com/login.htm?oauth\\_callback=https%3A%2F%2Fxx.aliyun.com%2F%2F5095&from\\_type=xianzhi](https://account.aliyun.com/login.htm?oauth_callback=https%3A%2F%2Fxx.aliyun.com%2F%2F5095&from_type=xianzhi)) 后跟帖