登录

【PHP代码审计】TP****多个漏洞集合

phpoop / 2017-12-01 11:35:00 / 浏览数 5861 新手 入门资料 顶(0) 踩(0)

0x00 前言

这个系统的漏洞也是放了很久了，这几天逛T00ls发现给人家爆出来了。。爆出来了。我也一次性爆完把=-=，有和T00ls论坛的那个哥们重复的纯属正常。

防止说我是照抄的，引起不好影响，下面那图是我审计的时候上传的时间，来证明一下，引起误会就不好了。

百度云链接：https://pan.baidu.com/s/1o8MIOQI 密码：x83a

0x02 说明

TPshop开源商城系统(Thinkphp shop的简称
)，是深圳搜豹网络有限公司开发的一套多商家模式的商城系统。适合企业及个人快速构建个性化网上商城。包含PC+IOS客户端+Adroid客户端+微商城，系统PC+后台是基
MVC构架开发的跨平台开源软件，设计得非常灵活，具有模块化架构体系和丰富的功能，易于与第三方应用系统无缝集成，在设计上，包含相当全面，以模块化架构体系，
下载地址：http://www.tp-shop.cn/Index/Index/download.html

```
■■■■■■
   ■■index.php              ■■■■
   ■■Install                ■■■■ //■■■■■■sql■■ php■■■■■
   ■■Thinkphp               PHP■■■■
   ■■plugins                ■■■■■■■
   ■■vendor                 ■■■■■
   ■■Public                 ■■css,js■img■upload■■■
   ■■Template               ■■■■ //■■■■■■■■html■■■
   ■    ■■mobile                 ■■■■■■
   ■    ■■pc                     ■■■■■■
   ■■application            ■■■■■
   ■    ■■home                   ■■■■■■■ //■■■■■■■■■■■PHP■■
   ■    ■    ■■Controller             ■■■
   ■    ■    ■■lang                   ■■■
   ■    ■    ■■Logic                  ■■■■■(■■■■Services■■)
   ■    ■    ■■model                  ■■■
   ■    ■    ■■validate               ■■■
   ■    ■    ■■view                   ■■(■■■■■■■■■■■)
   ■    ■■admin                     ■■■■■■■ //■■■■■■■■■■■PHP■■■■
   ■    ■■mobile                    ■■■■■■■ //■■■■■■■■■■■PHP■■
   ■    ■■common                    ■■■■■■■■■(■■■■■■■■■■■■■■■model■■■)
   ■    ■■common.php                ■■■■■■■■
   ■    ■■config php                ■■■■■■■■
   ■    ■■database.php              ■■■■■■■
   ■    ■■function.php              ■■■■■■
   ■    ■■route.php                 ■■■■■■
   ■    ■■tags.php                  ■■■■■■■■■■
```

0x03 正文

注入篇

漏洞1：前台sql注入 order by注入
文件地址：application/home/controller/Goods.php
URL地址：http://xx.com/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/desc
问题函数：`goodsList()`
问题参数_1: `$sort = I('get.sort','goods_id');`// 排序
问题参数_2: `$sort_asc = I('get.sort_asc','asc');`// 排序

因为是order by 的注入所以要利用一些平时用不到的sql语句

爆当前库名：

```
http://127.0.0.1:8082/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/,(SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x2D2D2D
```

爆此mysql库的总数：

```
http://127.0.0.1:8082/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/,(SELECT 8138 FROM (SELECT 2*(IF((SELECT * FROM (SELE
```

爆某个库的名称：

```
http://127.0.0.1:8082/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/,(SELECT 4362 FROM (SELECT 2*(IF((SELECT * FROM (SELE
```

获取某个库表的总数：

```
http://127.0.0.1:8082/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/,(SELECT 8139 FROM (SELECT 2*(IF((SELECT * FROM (SELE
```

获取某个库每个表的表名：

```
http://127.0.0.1:8082/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/,(SELECT 3572 FROM (SELECT 2*(IF((SELECT * FROM (SELE
```

获取某个表的字段总数：

```
http://127.0.0.1:8082/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/,(SELECT 1965 FROM (SELECT 2*(IF((SELECT * FROM (SELE
```

获取某个表 某个字段名称：

```
http://127.0.0.1:8082/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/,(SELECT 3302 FROM (SELECT 2*(IF((SELECT * FROM (SELE
```

获取某库某表某字段数据：

```
http://127.0.0.1:8082/Home/Goods/goodsList/id/1/sort/shop_price/sort_asc/,(SELECT 2857 FROM (SELECT 2*(IF((SELECT * FROM (SELE
```

漏洞2：前台sql注入 order by注入

文件地址：application/home/controller/Goods.php
URL地址：http://xx.com/index.php/Home/Goods/search/q/a/sort/sales_sum
问题函数：search()
问题参数_1: $sort = I('get.sort','goods_id');// 排序
问题参数_2: $sort_asc = I('get.sort_asc','asc');// 排序

漏洞3：前台sql注入 order by注入

文件地址：application\mobile\controller\Goods.php
URL地址：http://xx.com/index.php/Mobile/Goods/goodsList/id/1/sort_asc/desc
问题函数：goodsList()
问题参数_1: $sort = I('get.sort','goods_id');// 排序
问题参数_2: $sort_asc = I('get.sort_asc','asc'); // 排序

漏洞3：前台sql注入 order by注入

文件地址：application\mobile\controller\Goods.php
URL地址：http://xx.com/index.php/Mobile/Goods/search/id/0/q/小米/sort/shop_price
问题函数：search()
问题参数_1: $sort = I('get.sort','goods_id'); // 排序
问题参数_2: $sort_asc = I('get.sort_asc','asc'); // 排序

前后台getshell篇

漏洞1：前台无限制getshell漏洞

文件地址：application/home/controller/Test.php
URL地址：http://xx.com/index.php/Home/test/dlfile
问题函数：dlfile()

漏洞2：前台无限制getshell漏洞

文件地址：application/home/controller/Uploadify.php
URL地址：http://xx.com/index.php/Home/Uploadify/preview
问题函数：preview()

漏洞3：后台有限制 命令注入 漏洞

文件地址：application\admin\controller\Plugin.php
URL地址：http://xx.com/index.php/Admin/Plugin/add_shipping
问题函数：add_shipping

点击收藏 | 2 关注 | 0

上一篇：伪全栈式安全研发：CVE监控 下一篇：最近还是有点闲的，想找点事情干，朋...

1. 2 条回复

hades 2017-12-01 12:44:50

@phpoop 纯手工注入 新手可以围观一下

0 回复Ta

chybeta 2017-12-05 12:47:29

感谢分享！

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板