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.

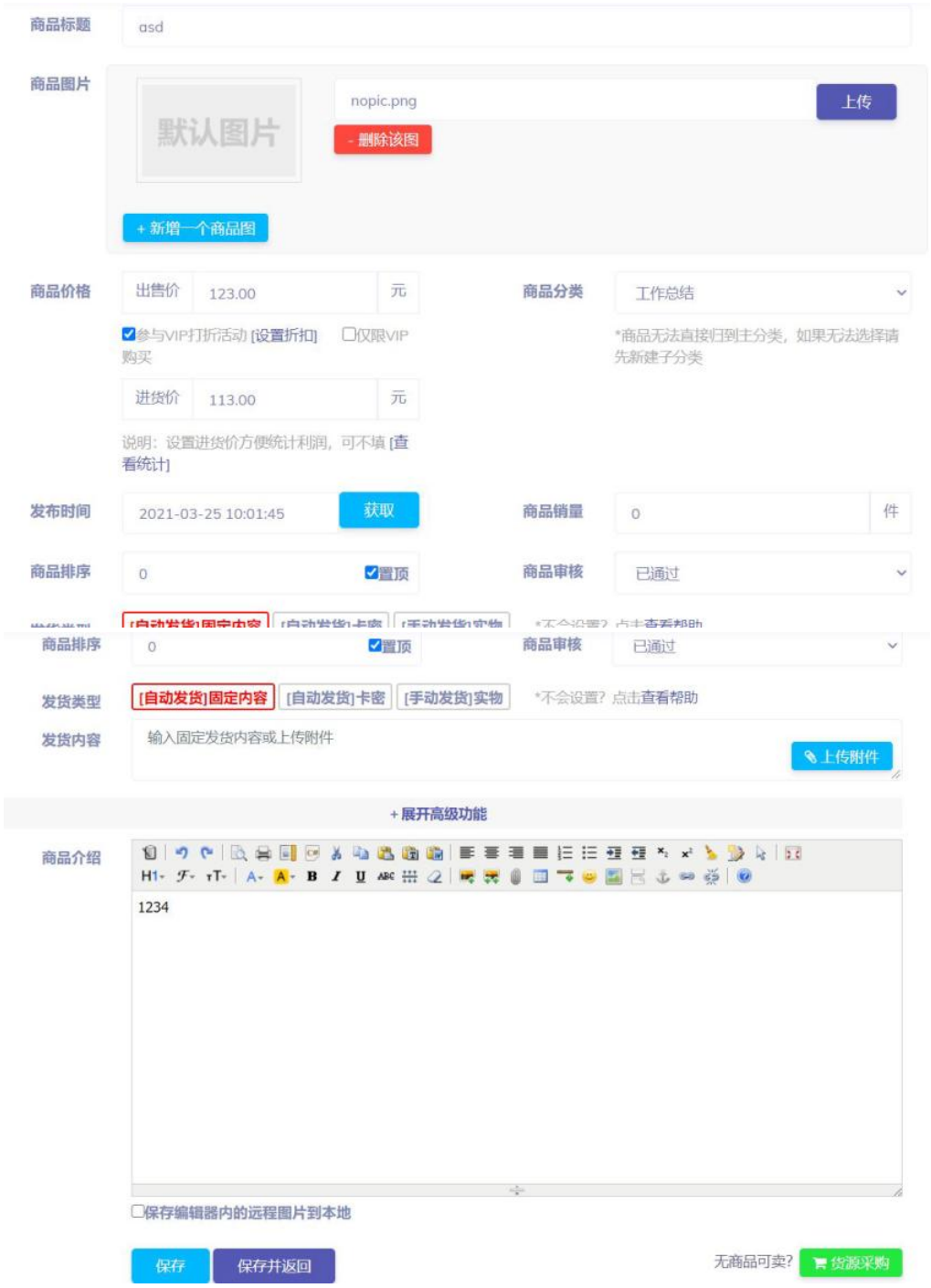
Reason: when getting user IP, there is no filtering.

/conn/function.php

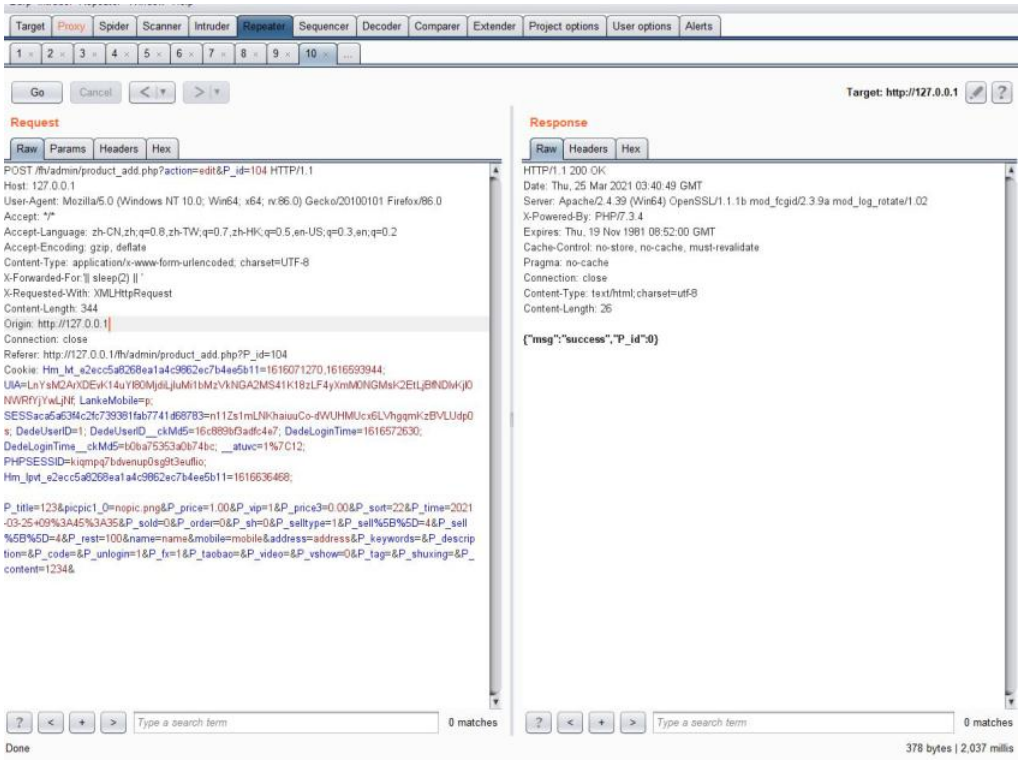
```php
function getip(){
    static $realip;
    if (isset($_SERVER)){
        if (isset($_SERVER["HTTP_X_FORWARDED_FOR"])){
            $realip = $_SERVER["HTTP_X_FORWARDED_FOR"];
        } else if (isset($_SERVER["HTTP_CLIENT_IP"])) {
            $realip = $_SERVER["HTTP_CLIENT_IP"];
        } else {
            $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;
}
```

visit /admin/product_add.php?

Modify the product information and click save



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



Successful injection!