DedeCMS 存储型xss漏洞","## 漏洞简介：

Dedecms是一款开源的PHP开源网站管理系统。

Dedecms会员功能shops_delivery.php中的`des`参数存在存储型XSS漏洞，攻击者可利用漏洞获得用户cookie。

测试环境：DedeCMS-V5.7-UTF8-SP2

发布日期： 2017-03-15 官方最新版

漏洞利用条件：DedeCMS开启shop模块

漏洞分析

漏洞触发点在 /dede/shops_delivery.php 文件 `des` 参数过滤不严导致xss漏洞触发。

```
if($do=='add')
{
    if( empty($dname) || (strlen($dname) > 100) )
    {
        ShowMsg(\"请填写配送方式名称!\",\"-1\");
        exit();
    }
    $price     = preg_replace(\"#[^.0-9]#\", \"\", $price);
    if($price < 0.01)
    {
        $price = '0.00';
    }
    $des = cn_substrR($des,255);
    $InQuery = \"INSERT INTO #@__shops_delivery(`dname`,`price`,`des`) VALUES
('$dname','$price','$des');\";
    $result = $dsql->ExecuteNoneQuery($InQuery);
    if($result)
    {
        ShowMsg(\"成功添加一个配送方式!\",\"shops_delivery.php\");
    }
    else
    {
        ShowMsg(\"添加配送方式时发生SQL错误!\",\"-1\");
    }
    exit();
}
```

漏洞触发函数 `$des = cn_substrR($des,255);` des 参数 只用`cn_substrR` 做了过滤。

继续跟踪cn_substrR函数，在`/include/helpers/string.helper.php` 第24行

```
if ( ! function_exists('cn_substrR'))
{
    function cn_substrR($str, $slen, $startdd=0)
    {
        $str = cn_substr(stripslashes($str), $slen, $startdd);
        return addslashes($str); //删掉此处
        return htmlspecialchars(addslashes($str));//修改代码
    }
}
```

这里只用 stripslashes 和 addslashes 函数进行了过滤，但是没有过滤xss攻击函数，导致漏洞触发

继续看输出的文件代码。

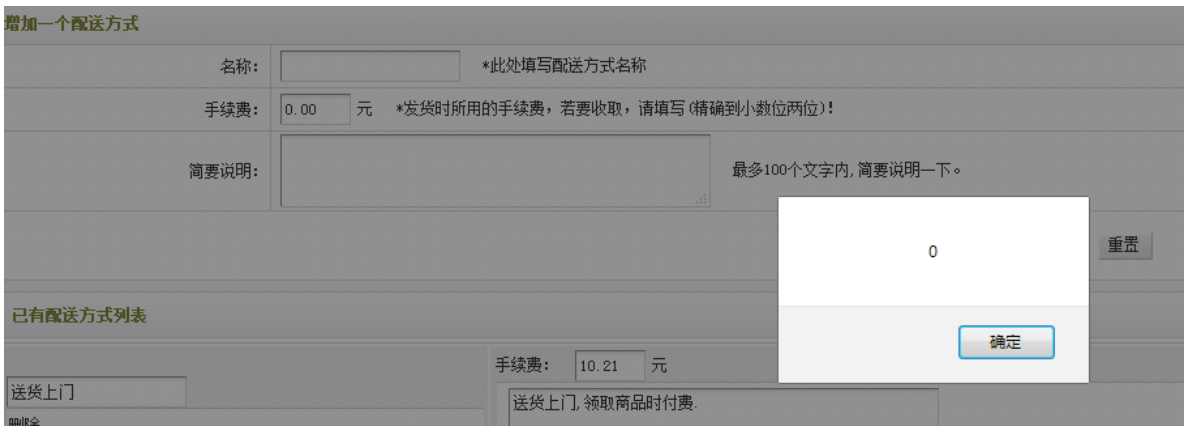
```
<td width=\"77%\" align=\"left\" valign=\"top\" bgcolor=\"#F0F0F0\"
style=\"BORDER-BOTTOM: #CCC 1px solid;padding-left:5px;\">
手续费:
<input name=\"m_price<?php echo $rs['pid'];?>\" type=\"text\" id=\"m_price<?php
echo $rs['pid'];?>\" style=\"margin-left:6px;\" value=\"<?php echo
$rs['price'];?>\" size=\"6\" maxlength=\"6\"/>
元
<div style=\"background-color:#FFFFFF; padding:3px;BORDER-TOP: #CCC 1px
solid;\"><textarea name=\"m_des<?php echo $rs['pid'];?>\" id=\"m_des<?php echo
$rs['pid'];?>\" style=\"margin-left:6px; width:320px;\"><?php echo $rs['des'];?>
</textarea></div>
</td>
```

可以看到这里 des没有做任何的过滤，从数据库读取之后，直接echo 输出 导致漏洞触发

漏洞利用

在管理员后台 系统 > 支付工具 >配送方式设置 增加一个配送方式。在简要说明输入 xss payload 即可触发漏洞。后台和前台都会触发。

后台触发



前台触发


下单购买
买家付款
确认收货
确认订单信息
订单编号 S-P1490927798RN143
订单价格 0.00 元
商品总数 1件
状态 下单
0
确定