

Dedecms存在储存型跨站脚本漏洞

Dedecms是一款开源的PHP开源网站管理系统。

Dedecms会员功能carbuyaction.php中的address、des、email、postname参数存在存储型XSS漏洞，攻击者可利用漏洞获得管理员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 /plus/carbuyaction.php 文件 address、des、email、postname 参数过滤不严导致xss漏洞触发。

漏洞文件代码在 carbuyaction.php 第 111 行

```
$address = cn_substr(trim($address),200);
$des = cn_substr($des,100);
$postname = cn_substr(trim($postname),15);
$tel= preg_replace("#[^\d-9,\\/\| ]#", "", $tel);
$zip= preg_replace("#[^\d-9]#", "", $zip);
$email= cn_substr($email,255);
```

这里 \$postname 参数虽然做了长度限制，但是我们开始可以利用最短xss payload 触发xss漏洞。

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

```
if ( ! function_exists('cn_substr'))
{
    function cn_substr($str, $slen, $startdd=0)
    {
        $str = cn_substr(stripslashes($str), $slen, $startdd);
        return addslashes($str);
    }
}
```

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

漏洞利用

前台用户登录下单，在街道地址填写xss跨站代码。

```
`<svg/onload=alert(0)>`
```

确认订单信息	
街道地址	<input type="text" value="<svg/onload=alert(0)>"/> * 请填写街道地址，不能为空!
收货人	<input type="text" value="test"/> * 请填写收货人姓名
E-Mail	<input type="text"/> 可选，联系您的电子邮箱
手机/电话	<input type="text" value="18888888888"/> * 请填写可以联系到您的电话
邮编	<input type="text" value="000000"/> * 请填写格式如：300030
确认订单信息	
购买留言	<div><div></div><div>请在购买留言中填写您对商品的特殊要求，如“我要红色的小码”(100个字以内)</div></div>
验证码	<input type="text"/>  看不清换一张
<input type="button" value="确认下单"/>	

下单之后自己的消费中心页面可以看到 xss漏洞 触发

DEDECMS 会员中心

内容中心 我的织梦 系统设置

个人空间 我的好友 短消息 留言板 消费中心 随便踩踩

会员互动 我的收藏夹

会员升级/点卡充值 点卡/会员定单 我购买的文章 商品定单 我购买的商品

购买的商品

订单号: S-P1490

支付方式: 货到付款

单价(元/单位): 0元

数量: 1

配送: 费用:10.21元

总计: 10.21元

发生时间: 2017-03-30 14:06:55

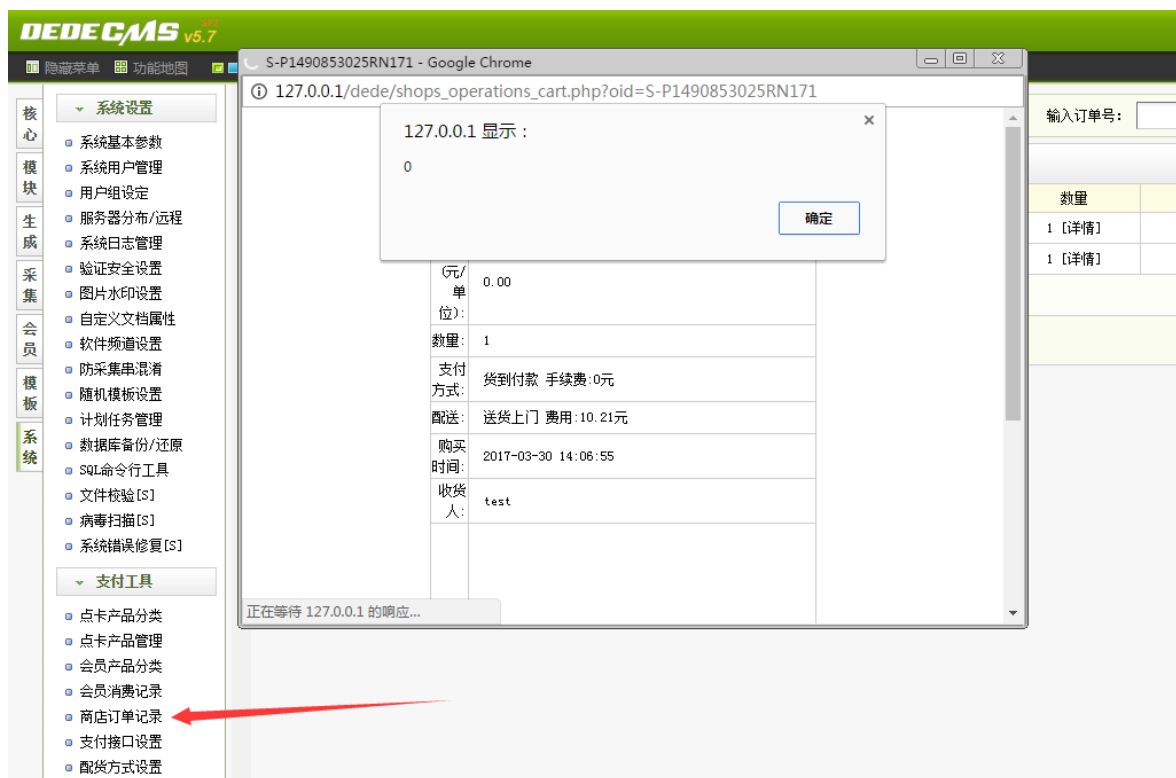
收货人: test

地址:

0

确定

同样在管理员后台也触发xss漏洞



利用此漏洞可以进一步获取管理员cookie。"