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

```
$address = cn_substrR(trim($address),200);
$des = cn_substrR($des,100);
$postname = cn_substrR(trim($postname),15);
$tel= preg_replace(\"#[^-0-9,\\/\\| ]#\", \"\", $tel);
$zip= preg_replace(\"#[^0-9]#\", \"\", $zip);
$email= cn_substrR($email,255);
```

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

继续跟踪cn_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);
    }
}
```

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

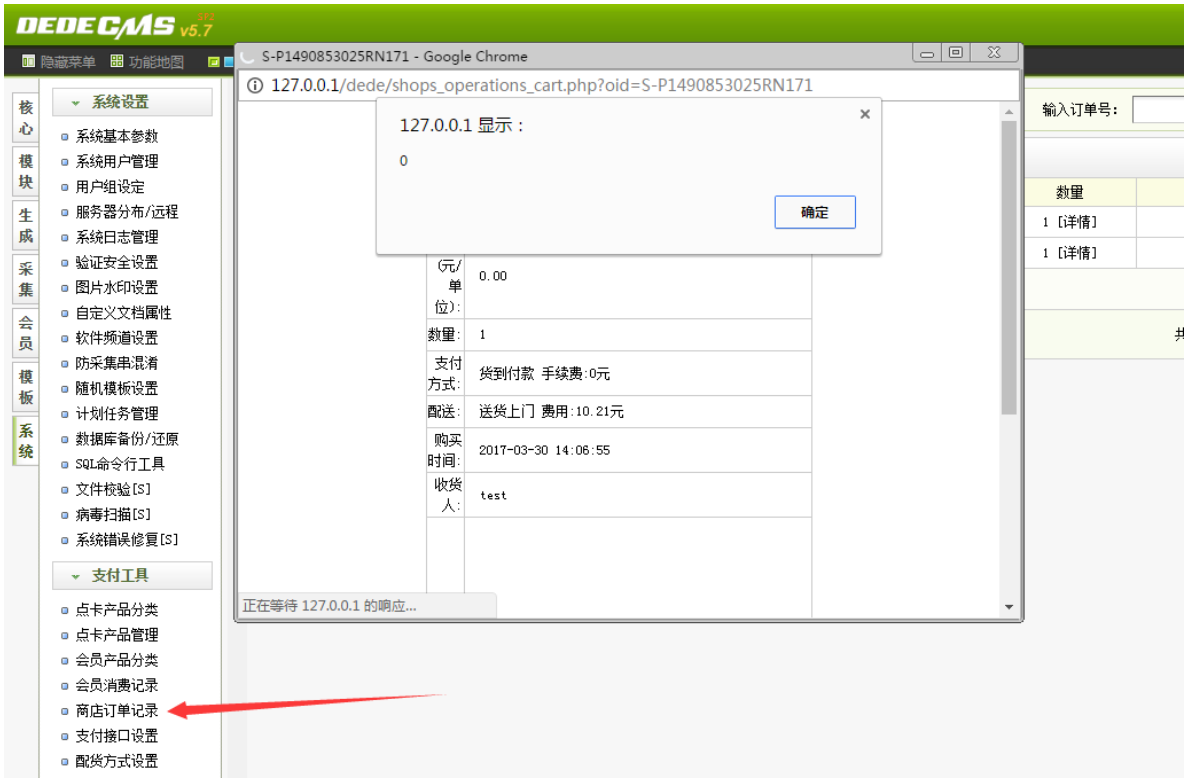
漏洞利用

前台用户登录下单，在街道地址填写xss跨站代码。

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

下单之后自己的消费中心页面可以看到 xss漏洞 触发

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。"