

ourphp存储型xss漏洞

漏洞简介：

OurPHP（傲派建站系统）是一款使用PHP语言开发的网站内容管理系统，开发商为哈尔滨伟成科技有限公司。

OurPHP 1.7.3版本存在存储型xss漏洞，可获取任意用户cookie

漏洞分析

OurPHP最新版 搜索框 过滤不严导致 存储型xss漏洞。

漏洞文件：www/function/ourphp_search.class.php 文件

第35行 `$content = dowith_sql($_REQUEST['content'])`；这里我们可以看到 `content` 参数用 `dowith_sql` 进行了过滤。继续跟进 `dowith_sql` 参数。在文件 `www/function/ourphp_function.class.php`

```
/*防注入函数*/
function dowith_sql($ourphpstr){
    $ourphpstr = addslashes($ourphpstr);
    $ourphpstr = str_ireplace(" and ", "", $ourphpstr);
    $ourphpstr = str_ireplace(" or ", "", $ourphpstr);
    $ourphpstr = str_ireplace("execute", "", $ourphpstr);
    $ourphpstr = str_ireplace("update", "", $ourphpstr);
    $ourphpstr = str_ireplace("count", "", $ourphpstr);
    $ourphpstr = str_ireplace("chr", "", $ourphpstr);
    $ourphpstr = str_ireplace("truncate", "", $ourphpstr);
    $ourphpstr = str_ireplace("char", "", $ourphpstr);
    $ourphpstr = str_ireplace("declare", "", $ourphpstr);
    $ourphpstr = str_ireplace("select", "", $ourphpstr);
    $ourphpstr = str_ireplace("create", "", $ourphpstr);
    $ourphpstr = str_ireplace("delete", "", $ourphpstr);
    $ourphpstr = str_ireplace("insert", "", $ourphpstr);
    $ourphpstr = str_ireplace("limit", "", $ourphpstr);
    $ourphpstr = str_ireplace("extractvalue", "", $ourphpstr);
    $ourphpstr = str_ireplace("concat", "", $ourphpstr);
    $ourphpstr = str_ireplace("&&", "", $ourphpstr);
    $ourphpstr = str_ireplace("||", "", $ourphpstr);
    $ourphpstr = str_ireplace("<script", "", $ourphpstr);
    $ourphpstr = str_ireplace("<iframe", "", $ourphpstr);
    $ourphpstr = str_ireplace("<embed", "", $ourphpstr);
    $ourphpstr = str_ireplace("*", "", $ourphpstr);
    $ourphpstr = str_ireplace("#", "", $ourphpstr);
    $ourphpstr = str_ireplace("'", "", $ourphpstr);
    $ourphpstr = str_ireplace("<", "&lt;", $ourphpstr);
    $ourphpstr = str_ireplace(">", "&gt;", $ourphpstr);
    $ourphpstr = str_ireplace("&", "&amp;", $ourphpstr);
    return $ourphpstr;
}
```

这里过滤了 单引号 尖括号 但是没有过滤双引号。

继续看 www/function/ourphp_search.class.php 文件

```
if ($query){
    $add = $db -> update("`ourphp_search`","`OP_Searchclick` = `OP_Searchclick`
+ 1","where `OP_Searchtext` = '". $content.'"");
}else{
    $add = $db -> insert("`ourphp_search`","`OP_Searchtext` =
'". $content.'"`,`OP_Searchclick` = 0`,`time` = '".date("Y-m-d H:i:s")."'");
}
```

这里把搜索关键字存入了数据库。

漏洞触发关键文件在，www/templates/default/cn/cn_shoptop.html 第40行

```
<p style=" padding-top:3px;">热门搜索:
[.sql mysql="SELECT * FROM `ourphp_search` order by OP_Searchclick desc limit
0,2" name="sql".]
<a href="search.php?cn-&content=[. $sql.OP_Searchtext.]&lang=cn&sid=product">
[. $sql.OP_Searchtext.]</a>
[./sql.]
</p>
```

这里我们看到 OP_Searchtext 从数据库读取之后，没有任何过滤直接展示在模板页面，导致xss漏洞触发。

漏洞复现

测试环境：chrome浏览器

在首页搜索框，输入关键字 1" onmouseover="alert(0)"，多搜索几次，使这个关键字成为热门搜索关键字。

OURPHP 建站演示

登录 - 注册
服务热线：400-626-0451



关于我们

查看更多 +

公司新闻

查看更多 +



01 世界，你好！
世界，你好！

[2014,12,07]

02 世界，你好！

[2014,12,07]

然后点击产品页面

[企业官网](#) [微信](#) [手机商城](#)

嗨，欢迎来到本网站

OURPHP 建站演示

ourphp
唯一官方商城

请输入搜索关键词

热门搜索: 1\ " onmouseover=\ "alert(0)\ " 1" onmouseover="alert(0)"

全场免运费

商品分类

商城首页

最新商品

特价商品

积分兑换

关于我们

联系我们

商城首页 >> 企业商城 >> 手机数码


客服中心

商品快捷分类

手机数码

男装女装

测试08



价格: ¥0.00

优惠价: **¥ 0.00**

货号: OP20141209155321

快递至: 本地IP 包邮

购买数量: 库存: 100

加入购物车

鼠标移动到搜索框下热门搜索，触发xss漏洞。

企业官网 微信 手机商城

OURPHP 建站演示 ourphp
唯一官方商城

10.9.1.31 显示:
0

确定

嗨，欢迎来到本网站

全场免运费

商品分类

商城首页

最新商品

特价商品

积分兑换

关于我们

联系我们


商城首页 >> 企业商城 >> 手机数码

客服中心

商品快捷分类

手机数码

测试08



价格: ¥0.00

优惠价: **¥ 0.00**

货号: OP20141209155321

快递至: 本地IP 包邮

购买数量: 库存: 100

加入购物车