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

```
/*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);</pre>
   $ourphpstr = str_ireplace("<iframe","",$ourphpstr);</pre>
   $ourphpstr = str_ireplace("<embed","",$ourphpstr);</pre>
   $ourphpstr = str_ireplace("*","",$ourphpstr);
   $ourphpstr = str_ireplace("#","",$ourphpstr);
   $ourphpstr = str_ireplace("'","",$ourphpstr);
   $ourphpstr = str_ireplace("<","&lt;",$ourphpstr);</pre>
   $ourphpstr = str_ireplace(">",">",$ourphpstr);
   $ourphpstr = str_ireplace("&","&",$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

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

```
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.]
```

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。

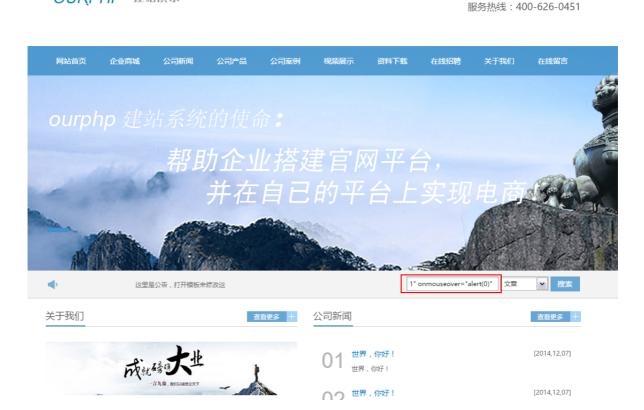
漏洞复现

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。

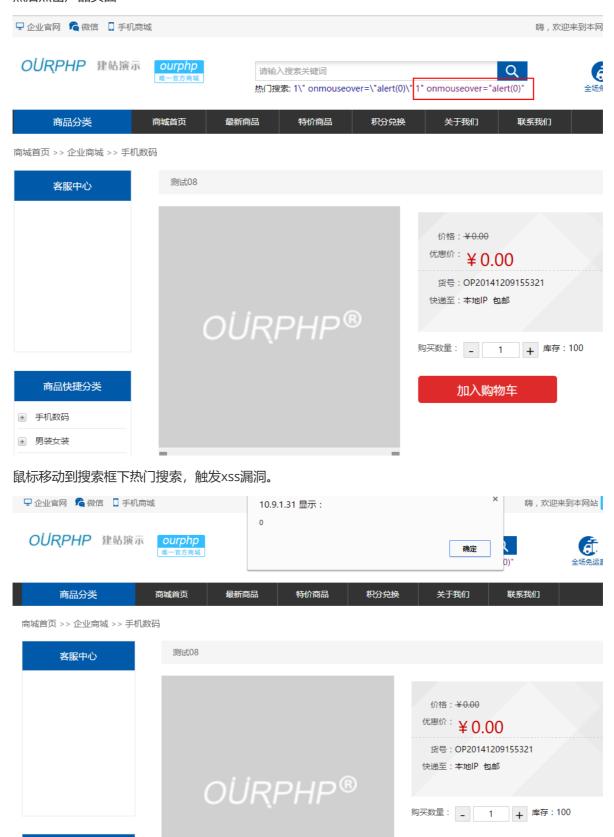
登录 - 注册

OURPHP 建站演示



商品快捷分类

- =±11 %/rZZ



加入购物车