

W

人

作

SC



WordPress插件YITH WooCommerce Wishlist SQL注入漏洞

围观

WEB安全

在安全审计的一部分，我们发现了一个愿望清单插件[YITH WooCommerce Wishlist](#)，存目前至少已被50000+的wordpress站点安装使用。

受影响范围

关注我们 分享每日精选文章

这个漏洞主要出现在2.2.0版本以下，主要是因为该版本缺少对用户输入数据进行严格过滤措施。攻击者（至少有一用户帐户）可能会利用该缺陷盗取用户敏感数据，甚至通过某些配置项危害你整个的WordPress安装。

需要提醒的是在MySQL版本低于5.7的服务器中，该漏洞极易被利用。

这个漏洞有个非常有意思的地方，也是我们决定要发布该安全公告的原因，就是使用这个插件的站点通常会启用免费“用户注册”功能，以允许用户的偏好（例如愿望清单）被存储和访问，以便后续使用。

技术细节

产生漏洞的代码，可在2.1.2版本中的`includes/class.yith-wcwl-shortcode.php`的第523行中找到。这段代码是`get_products()`函数的一部分，用于返回特定用户的所有wishlist元素：





关注我们 分享每日精选文章

如果攻击者控制了`$limit`变量，就可以为其赋任意值。例如构建一个查询语句。这样攻击者将有可能直接获取走，服务器上的所有敏感数据。例如加密哈希和电子邮件等。

攻击者想要达到构建查询的目的必须满足以下条件：

分页值必须为“yes”

`count`变量必须大于1（此变量存储特定用户的wishlist元素数量）

`limit`变量必须被设置

攻击者可以通过 `includes/class.yith-wcwl-shortcode.php`中定义的短代码`yith_wcwl_wishlist`来满足所有这些条件：





关注我们 分享每日精选文章





关注我们 分享每日精选文章

攻击者唯一要做的就是创建一个用户帐户，并调用漏洞短代码（具体可以参考[我们此前的文章](#)）。

紧急措施

检查你的[插件版本](#)，并尽快将其更新到最新版！

如果由于某种原因你无法升级，我们建议你使用[Sucuri](#)或其它WAF来保障你的站点安全。

*参考来源：[sucuri](#)，FB小编 secist 编译，转载请注明来自FreeBuf.COM

上一篇：[ElastAlert监控日志告警Web攻击行为](#)

下一篇：[新手科普 | MySQL手工注入之基本注入流程](#)

选择文件

未选择任何文件

昵称

请输入昵称

必须

您当前尚未登录。[登陆?](#) [注册](#)

邮

请输入

表情

关注我们 分享每日精选文章

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



[secist](#)

每个人的心中都有一个梦。。

110

文章数

43

评论数

最近文章

- [Microsoft Office之DDE攻击](#)2018.01.22
- [WordPress插件YITH WooCommerce Wishlist SQL注入漏洞](#)2018.01.20
- [MITM6：用IPv6攻陷IPv4网络的工具](#)2018.01.18

浏览更多

- [ThinkPHP框架安全实现分析](#)
- [安全科普：SQLi Labs 指南 Part 1](#)
- [Joomla!3.7.0 SQL注入攻击漏洞分析](#)

如何搭建自己的安全博客

二

特



[RT注...](#)

关注我们 分享每日精选文章




揭秘：恶意软件是如何操纵ATM机的 Rabbit_Run 2014-10-09 漏洞预警：知名论坛系统vBulletin常用SEO插件VBSEO存在严重安全 dawner 2015-01-09	反击“猫眼电影”网站的反爬虫策略 数月亮的孩子 2017-07-26 【安全大咖说】FriedAppleTeam越狱团队创始人Max Bazaliy专访 Elaine_z 2017-07-17	
---	---	--



关注我们 分享每日精选文章



© 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务

