wordpress历史漏洞排名

WordPress历史漏洞排名：揭秘那些曾威胁网站安全的漏洞

WordPress作为全球最受欢迎的内容管理系统，其安全性一直备受关注。本文将对WordPress历史上的知名漏洞进行排名，帮助广大用户了解漏洞的危害及防范措施。



一、WordPress历史漏洞排名

1. WordPress 5.0.0远程代码执行漏洞（CVE-2019-6977）

该漏洞于2019年12月12日发布，存在于5.0.0版本及之前。攻击者可利用该漏洞在默认设置下远程执行任意代码，威胁网站安全。该漏洞影响范围广泛，修复后仍有大量网站未及时更新。

1. WordPress 5.1.1 CSRF to RCE 漏洞（CVE-2019-6977）

2019年3月13日，RIPS团队公开了WordPress 5.1.1的CSRF to RCE漏洞。攻击者可利用该漏洞在特定条件下远程执行任意代码，对网站造成严重危害。

1. WordPress网站安全漏洞 98%由外挂引发

据安全厂商Imperva调查，98%的WordPress网站漏洞源于外挂程序。这些外挂程序往往存在安全漏洞，导致网站被攻击。

1. tagDiv插件漏洞（CVE-2023-3169）

该漏洞于2023年被发现，是一个跨站点脚本（XSS）漏洞。攻击者可利用该漏洞将恶意代码注入网页，对访问者进行诈骗。

二、漏洞危害及防范措施

1. 漏洞危害

（1）网站被攻击，数据泄露；

（2）网站被植入恶意代码，影响用户体验；

（3）网站被黑客控制，用于攻击其他网站。

1. 防范措施

（1）及时更新WordPress及插件，修复已知漏洞；

（2）加强对外挂程序的审查，避免使用存在安全漏洞的外挂；

（3）定期备份网站数据，以便在遭受攻击时快速恢复；

（4）使用安全防护工具，如防火墙、WAF等，提高网站安全性。

三、总结

WordPress作为全球最受欢迎的内容管理系统，其安全性至关重要。了解历史上的漏洞，有助于我们提高警惕，加强防范。广大用户应时刻关注WordPress安全动态，及时修复漏洞，确保网站安全稳定运行。

文章地址：<https://www.yyzq.team/post/434829.html>