Concerned about WordPress Security? Enter Acunetix

担心 WordPress 的安全？进入 Acunetix

WordPress is the most popular open source content management system (CMS). According to the latest W3Techs survey, almost 60% of all CMS instances use the platform and 32.5 of all the websites on the Internet are WordPress sites. From the standpoints of deployment and usage, this is exciting: given its popularity, WordPress is well-documented and full-featured. But it also means attackers are constantly looking to compromise vulnerable WordPress installations and the web servers behind them. To stay one step ahead, you need Acunetix: a WordPress vulnerability scanner that you can trust.

WordPress 是最流行的开源内容管理系统(CMS)。根据最新的 W3Techs 调查几乎有 60%的 CMS 实例使用该平台，互联网上的所有网站中有 32.5%是 WordPress 站点。从部署和使用的角度来看，这是令人振奋的：促使 WordPress 大受欢迎是因为 WordPress 有很好的存储系统和健全的功能。但这也意味着攻击者不断地试图破坏易受攻击的 WordPress 安装及其背后的 Web 服务器。为了领先一步抵御黑客攻击，您需要 Acunetix：一个令人信任的 WordPress 漏洞扫描仪。

Detect a Full Range of WordPress Vulnerabilities

检测到 WordPress 的全部漏洞

Acunetix is a full-featured WordPress security scanner. Vulnerabilities that Acunetix can discover include:

- Out-of-date WordPress versions, both WordPress core and plugins, that are missing critical security patches
- Malware disguised as 3rd party WordPress plugins and WordPress themes
- Weak passwords that can be used to launch a brute force attack
- Names of WordPress users that can be used to compromise accounts or perform social engineering
- Disclosure of publicly available wp-config.php files
- Susceptibility to XML-RPC brute force attacks

Acunetix 是一个功能齐全的 WordPress 安全扫描器.Acunetix 可以发现的漏洞包括：

- 过时的无论是 WordPress 核心还是插件，都缺少关键的安全补丁的 WordPress 版本
- 伪装成第三方 WordPress 插件和 WordPress 主题的恶意软件
- 可以用来发动暴力攻击的弱密码

- 可用于危害帐户或执行社会工程的 WordPress 用户名称
- 公开提供的 wp-config.php 文件
- 易受 xml-rpc 暴力攻击的影响

These results can be used by operations and development staff to update and secure existing WordPress installations. If out-of-date or unfamiliar plugins are detected, the team can quickly make educated decisions about whether to update the plugins or remove them from the site. Security teams can also use the findings as a basis for further penetration testing.

这些结果可供操作人员和开发人员使用，以更新和保护现有的 WordPress 安装。如果检测到过时或不熟悉的插件，团队可以迅速做出正确的决定，决定是更新插件还是从站点中删除插件。安全小组也可以利用调查结果作为进一步渗透试验做基础。

Up-to-Date WordPress Vulnerability Database

最新的 WordPress 漏洞数据库

When information about WordPress security vulnerabilities is released, attackers almost immediately begin to scan for sites with an outdated version of WordPress or with vulnerable plugins. Stopping attackers in their tracks requires both a strong ongoing WordPress security program as well as timely response when vulnerabilities are announced.

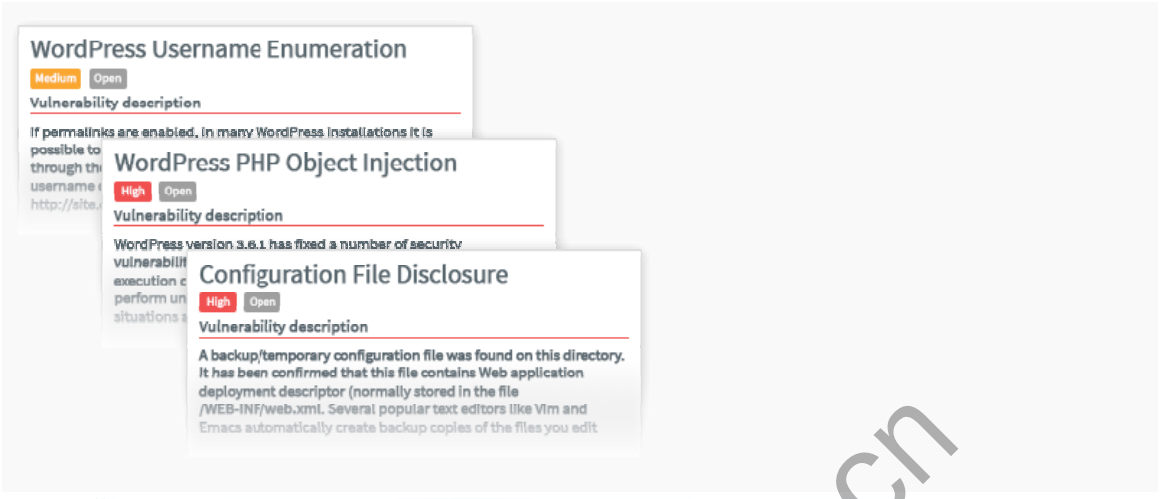
当有关 WordPress 安全漏洞的信息发布时，攻击者几乎立即开始扫描带有过时版本 WordPress 或带有易受攻击插件的站点。为了在中途就阻止攻击者，我们既需要一个强大的实时的 WordPress 安全程序，还想要漏洞被发现之后及时反应的程序。

From an ongoing perspective, Acunetix allows you to schedule frequent scans of your company's web presence, enumerate WordPress websites, and focus on instances that need to be updated or decommissioned. The Acunetix Continuous Scanning feature is particularly helpful with WordPress sites. With Continuous Scanning, Acunetix performs a full scan of the website once every week as well as a daily scan for critical vulnerabilities, and sends you those findings immediately. As new vulnerabilities are added to the Acunetix vulnerability database, Continuous Scanning ensures that you are testing for those vulnerabilities as soon as they are known. This keeps you in front of attackers.

从持续的角度来看，Acunetix 可以让您频繁扫描公司的网络存在，枚举 WordPress 网站，并关注需要更新或退役的实例。Acunetix 连续扫描功能对 WordPress 站点特别有用。通过连续扫描，Acunetix 可以每周对网站进行一次全面扫描，并每天扫描一次关键漏洞，并立即将这些结果发送给您。随着新的漏洞被添加到 Acunetix 漏洞数据库中，持续扫描确保一旦知道这些漏洞，就会立即进行测试。这会让你永远快攻击者一步。

Scan reports can then be configured for different audiences to facilitate sharing vital security information and meet regulatory needs such as PCI DSS, HIPAA, or Sarbanes-Oxley. Our user interface allows security analysts to easily configure scans for individual vulnerabilities, allowing the team to quickly and easily identify WordPress sites that need immediate attention.

然后，可以为不同的受众配置扫描报告，以便于共享重要的安全信息，并满足监管需求，例如 PCI DSS, HIPAA，或者萨班斯-奥克斯利(Sarbanes-Oxley)。我们的用户界面可以让安全分析人员轻松地配置针对单个漏洞的扫描，使团队能够快速、轻松地识别需要立即关注的 WordPress 站点。



Content Management Systems and Beyond

内容管理系统及其之外的系统

Even if your business depends on WordPress websites, it may not be your only web platform now. If it is, it may not be your only one in the future. You may be considering a tool specific to WordPress, but Acunetix is more flexible. It is a full-featured web application security testing toolthat will evolve with your infrastructure. It detects security issues in any web application: from CMS platforms like WordPress, Joomla!, and Drupal to custom-built applications.

即使你的业务依赖于 WordPress 网站，但它很可能不是你现在唯一的网站平台。如果是的话，那它可不能是你未来唯一的一个。您可能正在考虑一个特定于 WordPress 的工具，但是 Acunetix 更灵活。这是一个功能齐全的 Web 应用程序安全测试工具这将随着您的基础设施的发展而发展。它检测任何 web 应用程序中的安全问题：从 WordPress 之类的 CMS 平台，乔姆拉！，和德鲁帕尔定制的应用程序。

Furthermore, Acunetix is technology-independent. Whether your web application is built using PHP, Ruby on Rails, Python, JavaScript, or any other language, you can trust Acunetix to enumerate the user input fields and find the vulnerabilities that the attackers are looking for. By choosing Acunetix now, you can ensure that your security team is using a full-featured web application vulnerability scanner, and that your business's web presence can remain secure through any future plans.

此外，Acunetix 是技术独立的。是否使用 PHP，Ruby on Rails，Python，JavaScript 或者任何其他语言，您都可以信任 Acunetix 枚举用户输入字段并查找攻击者正在寻找的漏洞。现在选择 Acunestx，您可以确保您的安全团队可以使用功能齐全的 web 应用程序漏洞扫描器，并且无论您未来计划如何，您的业务的网络存在可以一直保持安全。