**Vulnerability scanner**

Vulnerability scanning is the process of identifying security weaknesses and flaws in systems and software running on them. This is an integral component of a [vulnerability management](https://www.balbix.com/insights/what-is-risk-based-vulnerability-management/) program, which has one overarching goal – to protect the organization from breaches and the exposure of sensitive data. These programs rely on assessment to gauge security readiness and minimize risk, and vulnerability scanning is a critical tool in the cybersecurity toolbox.

There are two big challenges related to traditional [vulnerability assessment](https://www.balbix.com/insights/vulnerability-assessments-drive-enhanced-security-and-cyber-resilience/) – knowing what to scan and knowing when to scan:

* Keeping an up-to-date asset inventory is an essential first step and requires its own set of tools and strategies.
* Making sure that your vulnerability scanning tools cover non-traditional assets such as BYOD devices, IoTs, mobile assets, and cloud services is essential.
* In a world where cyber threats can come from any direction and at any time, the ability to configure and perform continuous monitoring and scanning (as opposed to monthly or quarterly vulnerability scans) is key.

**How to use Vulnerability Scanner?**

Copy the given code in linux/termux software

nikto –h website(any website you want to vulnerability)

**Repository link:** [**https://github.com/Pragyesh1212/website-vulnerabiility.git**](https://github.com/Pragyesh1212/website-vulnerabiility.git)