‘Badsecrets’ Open Source Tool Detects Secrets in Many Web Frameworks

Cybersecurity company Black Lantern this week announced Badsecrets, an open source tool that can help identify known or weak cryptographic secrets across many web frameworks.

This pure Python library has a modular design and is currently offering ten modules, which are meant to be replacements of existing tools for finding known secrets.

In fact, Badsecrets itself is inspired by Blacklist3r, a NotSoSecure project for gathering secret keys related to publicly available web frameworks and auditing applications that might be using these pre-published keys.

The goal of Badsecrets, however, is to “expand on the supported platforms and remove language and operating system dependencies”.

The modules currently available with the library support scanning for Flask cookie signing passwords, bad/weak signing passwords in Peoplesoft PS_TOKEN, ASP.NET machine keys, and secret keys in Telerik UI, Django’s session cookies, Ruby on Rails signed or encrypted session cookies, JSON Web Token, Mojarra and Myfaces implementations of Java Server Faces (JSF), and Symfony ‘_fragment’ URLs.

“Knowing when a ‘bad secret’ was used is usually a matter of examining some cryptographic product in which the secret was used: for example, a cookie which is signed with a keyed hashing algorithm. Things can get complicated when you dive

into the individual implementation oddities each platform provides, which this library aims to alleviate," Black Lantern notes.

Badsecrets, the cybersecurity firm notes, was designed to identify known secrets that could be exploited for remote code execution (RCE) or privilege escalation, but does not help address these issues.

"It will help you find them, but you are generally on your own from there. Sometimes exploitation will be very straightforward, and in other cases it might require a lot of follow-on work or chaining with other vulnerabilities," Black Lantern explains.

However, there is currently no plan to change this aspect of Badsecrets, as that could lead to its abuse for the exploitation of identified misconfigurations.

Black Lantern hopes that the community will adopt Badsecrets as the standard for identifying such vulnerabilities and that contributions will help grow the available modules, to cover additional web frameworks and utilities.

Related: GitHub Secret Scanning Now Generally Available

Related: 'Secrets Sprawl' Haunts Software Supply Chain Security

Related: Thousands of Secret Keys Found in Leaked Samsung Source Code

https://www.securityweek.com/badsecrets-open-source-tool-detects-secrets-in-many-web-frameworks/