BugCatcher Report on Project: Pull Request 33

Introduction

We've performed static analysis tests on your codebase. This reports highlights the potential issues that were found after running these tests on your codebase. Note that static analysis can only flag sections of code for review. Static analysis tests do not confirm the existence of any given vulnerability! A developer with security expertise can use this report to assess which sections of the codebase are most likely to have potential issues, and to give those sections special attention during a code review. Please use our "Annotation" feature to make notes about which issues require fixes, and which error messages are not applicable and can be safely ignored

High Severity

These are the highest severity issues that can be detected by our tool. When present, high severity issues could have a significant impact on the security of your codebase.

No items of this type were found by our scan.

Medium Severity

Medium severity issues can potentially be exploited by third parties, and are recommended to fix

blacklist

By default, Python will create a secure, verified ssl context for use in such classes as HTTPSConnection. However, it still allows using an insecure context via the _create_unverified_context that reverts to the previous behavior that does not validate certificates or perform hostname checks.

File: google_images_download.py {instance.start_line} - {instance.end_line}

blacklist

Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.

This is not an issue because...

File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}
File: google_images_download.py {instance.start_line} - {instance.end_line}

Low Severity

Low severity issues may violate best practices but be difficult to exploit. Formatting issues and other non-security concerns also are in this category

No items of this type were found by our scan.

Informational

These items are purely informational items about best practices and are not security issues.

No items of this type were found by our scan.