CodeAssistant 报告

（由自动审查与测试生成系统输出）

Contents

---

1 代码审查（Review）

1.1 概览

- 问题总数：60
- 高/中/低：60 / 0 / 0
- 工具数：1
- DS 规则命中总数：0

1.2 严重性分布

- high：60

1.3 工具分布

- pip-audit：60

1.4 Top 20 问题

1. **[high] pip-audit VULN**
   说明：None None -> CVE-2024-27306 ### Summary A XSS vulnerability exists on index pages for static file handling. ### Details When using ‘web.static(..., show_index=True)‘, the resulting index pages do not escape file names. If users can upload files with arbitrary filenames to the static directory, the server is vulnerable to XSS attacks. ### Workaround We have always recommended using a reverse proxy server (e.g. nginx) for serving static files. Users following the recommendation are unaffected. Other users can disable ‘show_index‘ if unable to upgrade. — Patch: https://github.com/aio-libs/aiohttp/pull/8319/files

2. **[high] pip-audit VULN**
   说明：None None -> CVE-2024-30251 ### Summary An attacker can send a specially crafted POST (multipart/form-data) request. When the aiohttp server processes it, the server will enter an infinite loop and be unable to process any further requests. ### Impact An attacker can stop the application from serving requests after sending a single request. ——- For anyone needing to patch older versions of aiohttp, the minimum diff needed to resolve the issue is (located in '_read_chunk_from_length()'): "'diff diff –git a/aiohttp/multipart.py b/aiohttp/multipart.py index 227be605c..71fc2654a 100644 — a/aiohttp/multipart.py +++ b/aiohttp/multipart.py @@ -338,6 +338,8 @@ class BodyPartReader: assert self._length is not None, "Content-Length required for chunked read" chunk_size = min(size, self._length - self._read_bytes) chunk = await self._content.read(chunk_size) + if self._content.at_eof(): + self._at_eof = True return chunk async def _read_chunk_from_stream(self, size: int) -> bytes: "' This does however introduce some very minor issues with handling form data. So, if possible, it would be recommended to also backport the changes in: https://github.com/aio-libs/aiohttp/commit/cebe526b9c34dc3a3da9140409db63014bc4cf19 https://github.com/aio-libs/aiohttp/co https://github.com/aio-libs/aiohttp/commit/f21c6f2ca512a026ce7f0f6c6311f62d6a638866

3. **[high] pip-audit VULN**
   说明：None None -> CVE-2024-52304 ### Summary The Python parser parses newlines in chunk extensions incorrectly which can lead to request smuggling vulnerabilities under certain conditions. ### Impact If a pure Python version of aiohttp is installed (i.e. without the usual C extensions) or 'AIOHTTP_NO_EXTENSIONS' is enabled, then an attacker may be able to execute a request smuggling attack to bypass certain firewalls or proxy protections. —- Patch: https://github.com/aio-libs/aiohttp/commit/259edc369075de63e6f3a4eaade058c62af0df71

4. **[high] pip-audit VULN**
   说明：None None -> CVE-2025-53643 ### Summary The Python parser is vulnerable to a request smuggling vulnerability due to not parsing trailer sections of an HTTP request. ### Impact If a pure Python version of aiohttp is installed (i.e. without the usual C extensions) or AIOHTTP_NO_EXTENSIONS is enabled, then an attacker may be able to execute a request smuggling attack to bypass certain firewalls or proxy protections. —- Patch: https://github.com/aio-libs/aiohttp/commit/e8d774f635dc6d1cd3174d0e38891da5de0e2b6a

5. **[high] pip-audit VULN**
   说明：None None -> CVE-2025-6176 Scrapy versions up to 2.13.3 are vulnerable to a denial of service (DoS) attack due to a flaw in its brotli decompression implementation. The protection mechanism against decompression bombs fails to mitigate the brotli variant, allowing remote servers to crash clients with less than 80GB of available memory. This occurs because brotli can achieve extremely high compression ratios for zero-filled data, leading to excessive memory consumption during decompression. Mitigation for this vulnerability needs security enhancement added in brotli v1.2.0.

6. **[high] pip-audit VULN**
   说明：None None -> PYSEC-2024-225 cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. Starting in version 38.0.0 and prior to version 42.0.4, if 'pkcs12.serialize_key_and_certificates' is called with both a certificate whose public key did not match the provided private key and an 'encryption_algorithm' with 'hmac_hash' set (via 'PrivateFormat.PKCS12.encryption_builder().hmac_hash(...)', then a

NULL pointer dereference would occur, crashing the Python process. This has been resolved in version 42.0.4, the first version in which a 'ValueError' is properly raised.

7. **[high] pip-audit VULN**
   说明：None None -> GHSA-h4gh-qq45-vh27 pyca/cryptography's wheels include a statically linked copy of OpenSSL. The versions of OpenSSL included in cryptography 37.0.0-43.0.0 are vulnerable to a security issue. More details about the vulnerability itself can be found in https://openssl-library.org/news/secadv/20240903.txt. If you are building cryptography source ("sdist") then you are responsible for upgrading your copy of OpenSSL. Only users installing from wheels built by the cryptography project (i.e., those distributed on PyPI) need to update their cryptography versions.

8. **[high] pip-audit VULN**
   说明：None None -> CVE-2024-12797 pyca/cryptography's wheels include a statically linked copy of OpenSSL. The versions of OpenSSL included in cryptography 42.0.0-44.0.0 are vulnerable to a security issue. More details about the vulnerability itself can be found in https://openssl-library.org/news/secadv/20250211.txt. If you are building cryptography source ("sdist") then you are responsible for upgrading your copy of OpenSSL. Only users installing from wheels built by the cryptography project (i.e., those distributed on PyPI) need to update their cryptography versions.

9. **[high] pip-audit VULN**
   说明：None None -> PYSEC-2024-58 An issue was discovered in Django 5.0 before 5.0.7 and 4.2 before 4.2.14. Derived classes of the django.core.files.storage.Storage base class, when they override generate_filename() without replicating the file-path validations from the parent class, potentially allow directory traversal via certain inputs during a save() call. (Built-in Storage sub-classes are unaffected.)

10. **[high] pip-audit VULN**
    说明：None None -> PYSEC-2024-57 An issue was discovered in Django 5.0 before 5.0.7 and 4.2 before 4.2.14. The django.contrib.auth.backends.ModelBackend.authenticate() method allows remote attackers to enumerate users via a timing attack involving login requests for users with an unusable password.

11. **[high] pip-audit VULN**
    说明：None None -> PYSEC-2024-56 An issue was discovered in Django 4.2 before 4.2.14 and 5.0 before 5.0.7. urlize and urlizetrunc were subject to a potential denial of service attack via certain inputs with a very large number of brackets.

12. **[high] pip-audit VULN**
    说明：None None -> PYSEC-2024-59 An issue was discovered in Django 5.0 before 5.0.7 and 4.2 before 4.2.14. get_supported_language_variant() was subject to a potential denial-of-service attack when used with very long strings containing specific characters.

13. **[high] pip-audit VULN**
    说明：None None -> PYSEC-2024-69 An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The urlize and urlizetrunc template filters, and the AdminURLFieldWidget widget, are subject to a potential denial-of-service attack via certain inputs with a very large number of Unicode characters.

14. **[high] pip-audit VULN**
说明：None None -> PYSEC-2024-70 An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. QuerySet.values() and values_list() methods on models with a JSONField are subject to SQL injection in column aliases via a crafted JSON object key as a passed *arg.

15. **[high] pip-audit VULN**
说明：None None -> PYSEC-2024-68 An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The urlize() and urlizetrunc() template filters are subject to a potential denial-of-service attack via very large inputs with a specific sequence of characters.

16. **[high] pip-audit VULN**
说明：None None -> PYSEC-2024-67 An issue was discovered in Django 5.0 before 5.0.8 and 4.2 before 4.2.15. The floatformat template filter is subject to significant memory consumption when given a string representation of a number in scientific notation with a large exponent.

17. **[high] pip-audit VULN**
说明：None None -> PYSEC-2025-13 An issue was discovered in Django 5.1 before 5.1.7, 5.0 before 5.0.13, and 4.2 before 4.2.20. The django.utils.text.wrap() method and wordwrap template filter are subject to a potential denial-of-service attack when used with very long strings.

18. **[high] pip-audit VULN**
说明：None None -> PYSEC-2024-102 An issue was discovered in Django 5.1 before 5.1.1, 5.0 before 5.0.9, and 4.2 before 4.2.16. The urlize() and urlizetrunc() template filters are subject to a potential denial-of-service attack via very large inputs with a specific sequence of characters.

19. **[high] pip-audit VULN**
说明：None None -> PYSEC-2024-157 An issue was discovered in Django 5.1 before 5.1.4, 5.0 before 5.0.10, and 4.2 before 4.2.17. Direct usage of the django.db.models.fields.json.HasKey lookup, when an Oracle database is used, is subject to SQL injection if untrusted data is used as an lhs value. (Applications that use the jsonfield.has_key lookup via ___ are unaffected.)

20. **[high] pip-audit VULN**
说明：None None -> PYSEC-2024-156 An issue was discovered in Django 5.1 before 5.1.4, 5.0 before 5.0.10, and 4.2 before 4.2.17. The strip_tags() method and striptags template filter are subject to a potential denial-of-service attack via certain inputs containing large sequences of nested incomplete HTML entities.

2 测试生成（TestGen）

2.1 指标

- 写入测试文件数：3
- 覆盖函数数：4
- 输出目录：`D:/code/PythonWithPycharm/DataMining/CodeAssistant-v2/generated_tests`

2.2 覆盖率报告

Name	Stmts	Miss	Cover	Missing
N/A	0	0	0%	