Archive of security issues ¶

Django's development team is strongly committed to responsible reporting and disclosure of security-related issues, as outlined in Django's security policies.

As part of that commitment, we maintain the following historical list of issues which have been fixed and disclosed. For each issue, the list below includes the date, a brief description, the CVE identifier if applicable, a list of affected versions, a link to the full disclosure and links to the appropriate patch(es).

Some important caveats apply to this information:

- Lists of affected versions include only those versions of Django which had stable, security-supported releases at the time of disclosure. This means older versions (whose security support had expired) and versions which were in pre-release (alpha/beta/RC) states at the time of disclosure may have been affected, but are not listed.
- The Django project has on occasion issued security advisories, pointing out potential security problems which can arise from improper configuration or from other issues outside of Django itself. Some of these advisories have received CVEs; when that is the case, they are listed here, but as they have no accompanying patches or releases, only the description, disclosure and CVE will be listed.

Issues under Django's security process ¶

All security issues have been handled under versions of Django's security process. These are listed below.

July 7, 2026 - CVE 2026-48588 ¶

Potential exposure of private data via cached **`Set-Cookie`** response. Full description

- Django 6.1 (patch)
- Django 6.0 (patch)
- Django 5.2 (patch)

July 7, 2026 - CVE 2026-53877 ¶

Heap buffer over-read in **`GDALRaster`**. Full description

- Django 6.1 (patch)
- Django 6.0 (patch)
- Django 5.2 (patch)

July 7, 2026 - CVE 2026-53878 ¶

Header injection possibility since **`DomainNameValidator`** accepted newlines in input. Full description

- Django 6.1 (patch)
- Django 6.0 (patch)
- Django 5.2 (patch)

June 3, 2026 - CVE 2026-6873 ¶

Signed cookie salt namespace collision in **`django.http.HttpRequest.get_signed_cookie`**. Full description

- Django 6.1 (patch)
- Django 6.0 (patch)
- Django 5.2 (patch)

June 3, 2026 - CVE 2026-7666 ¶

Potential unencrypted email transmission via **`STARTTLS`** in the SMTP backend. Full description

- Django 6.1 (patch)
- Django 6.0 (patch)

- Django 5.2 (patch)

June 3, 2026 - CVE 2026-8404 ¶

Potential exposure of private data via case-sensitive **`Cache-Control`** directives in **`UpdateCacheMiddleware`**. Full description

- Django 6.1 (patch)
- Django 6.0 (patch)
- Django 5.2 (patch)

June 3, 2026 - CVE 2026-35193 ¶

Potential exposure of private data via missing **`Vary: Authorization`** in **`UpdateCacheMiddleware`**. Full description

- Django 6.1 (patch)
- Django 6.0 (patch)
- Django 5.2 (patch)

June 3, 2026 - CVE 2026-48587 ¶

Potential exposure of private data via whitespace padding in **`Vary`** header. Full description

- Django 6.1 (patch)
- Django 6.0 (patch)
- Django 5.2 (patch)

May 5, 2026 - CVE 2026-5766 ¶

Potential denial-of-service vulnerability in ASGI requests via file upload limit bypass. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)

May 5, 2026 - CVE 2026-35192 ¶

Session fixation via public cached pages and **`SESSION_SAVE_EVERY_REQUEST`**. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)

May 5, 2026 - CVE 2026-6907 ¶

Potential exposure of private data due to incorrect handling of **`Vary: *`** in **`UpdateCacheMiddleware`**. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)

April 7, 2026 - CVE 2026-3902 ¶

ASGI header spoofing via underscore/hyphen conflation. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

April 7, 2026 - CVE 2026-4277 ¶

Privilege abuse in **`GenericInlineModelAdmin`**. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

April 7, 2026 - CVE 2026-4292 ¶

Privilege abuse in **`ModelAdmin.list_editable`**. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

April 7, 2026 - CVE 2026-33033 ¶

Potential denial-of-service vulnerability in **`MultiPartParser`** via base64-encoded file upload. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

April 7, 2026 - CVE 2026-33034 ¶

Potential denial-of-service vulnerability in ASGI requests via memory upload limit bypass. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

March 3, 2026 - CVE 2026-25673 ¶

Potential denial-of-service vulnerability in **`URLField`** via Unicode normalization on Windows. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

March 3, 2026 - CVE 2026-25674 ¶

Potential incorrect permissions on newly created file system objects. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

February 3, 2026 - CVE 2025-13473 ¶

Username enumeration through timing difference in mod_wsgi authentication handler. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

February 3, 2026 - CVE 2025-14550 ¶

Potential denial-of-service vulnerability via repeated headers when using ASGI. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

February 3, 2026 - CVE 2026-1207 ¶

Potential SQL injection via raster lookups on PostGIS. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

February 3, 2026 - CVE 2026-1285 ¶

Potential denial-of-service vulnerability in **`django.utils.text.Truncator`** HTML methods. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

February 3, 2026 - CVE 2026-1287 ¶

Potential SQL injection in column aliases via control characters. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)

- Django 4.2 (patch)

February 3, 2026 - CVE 2026-1312 ¶

Potential SQL injection via **`QuerySet.order_by`** and **`FilteredRelation`**. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 4.2 (patch)

December 2, 2025 - CVE 2025-13372 ¶

Potential SQL injection in **`FilteredRelation`** column aliases on PostgreSQL. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

December 2, 2025 - CVE 2025-64460 ¶

Potential denial-of-service vulnerability in XML serializer text extraction. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

November 5, 2025 - CVE 2025-64458 ¶

Potential denial-of-service vulnerability in **`HttpResponseRedirect`** and **`HttpResponsePermanentRedirect`** on Windows. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

November 5, 2025 - CVE 2025-64459 ¶

Potential SQL injection via **`_connector`** keyword argument in **`QuerySet`** and **`Q`** objects. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

October 1, 2025 - CVE 2025-59681 ¶

Potential SQL injection in **`QuerySet.annotate()`**, **`alias()`**, **`aggregate()`**, and **`extra()`** on MySQL and MariaDB. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

October 1, 2025 - CVE 2025-59682 ¶

Potential partial directory-traversal via **`archive.extract()`**. Full description

- Django 6.0 (patch)
- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

September 3, 2025 - CVE 2025-57833 ¶

Potential SQL injection in **`FilteredRelation`** column aliases. Full description

- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

June 4, 2025 - CVE 2025-48432 ¶

Potential log injection via unescaped request path. Full description

- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

There was an additional hardening with new patch releases published on June 10, 2025. Full description

- Django 5.2.3 (patch)
- Django 5.1.11 (patch)
- Django 4.2.23 (patch)

May 7, 2025 - CVE 2025-32873 ¶

Denial-of-service possibility in **`strip_tags()`**. Full description

- Django 5.2 (patch)
- Django 5.1 (patch)
- Django 4.2 (patch)

April 2, 2025 - CVE 2025-27556 ¶

Potential denial-of-service vulnerability in **`LoginView`**, **`LogoutView`**, and **`set_language()`** on Windows. Full description

- Django 5.1 (patch)
- Django 5.0 (patch)

March 6, 2025 - CVE 2025-26699 ¶

Potential denial-of-service in **`django.utils.text.wrap()`**. Full description

- Django 5.1 (patch)
- Django 5.0 (patch)
- Django 4.2 (patch)

January 14, 2025 - CVE 2024-56374 ¶

Potential denial-of-service vulnerability in IPv6 validation. Full description

- Django 5.1 (patch)
- Django 5.0 (patch)
- Django 4.2 (patch)

December 4, 2024 - CVE 2024-53907 ¶

Potential denial-of-service in **`django.utils.html.strip_tags()`**. Full description

- Django 5.1 (patch)
- Django 5.0 (patch)
- Django 4.2 (patch)

December 4, 2024 - CVE 2024-53908 ¶

Potential SQL injection in **`HasKey(lhs, rhs)`** on Oracle. Full description

- Django 5.1 (patch)
- Django 5.0 (patch)
- Django 4.2 (patch)

September 3, 2024 - CVE 2024-45231 ¶

Potential user email enumeration via response status on password reset. Full description

- Django 5.1 (patch)

- Django 5.0 (patch)
- Django 4.2 (patch)

September 3, 2024 - CVE 2024-45230 ¶

Potential denial-of-service vulnerability in **`django.utils.html.urlize()`**. Full description

- Django 5.1 (patch)
- Django 5.0 (patch)
- Django 4.2 (patch)

August 6, 2024 - CVE 2024-42005 ¶

Potential SQL injection in **`QuerySet.values()`** and **`values_list()`**. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)

August 6, 2024 - CVE 2024-41991 ¶

Potential denial-of-service vulnerability in **`django.utils.html.urlize()`** and **`AdminURLFieldWidget`**. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)

August 6, 2024 - CVE 2024-41990 ¶

Potential denial-of-service vulnerability in **`django.utils.html.urlize()`**. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)

August 6, 2024 - CVE 2024-41989 ¶

Potential memory exhaustion in **`django.utils.numberformat.floatformat()`**. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)

July 9, 2024 - CVE 2024-39614 ¶

Potential denial-of-service in **`django.utils.translation.get_supported_language_variant()`**. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)

July 9, 2024 - CVE 2024-39330 ¶

Potential directory-traversal in **`django.core.files.storage.Storage.save()`**. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)

July 9, 2024 - CVE 2024-39329 ¶

Username enumeration through timing difference for users with unusable passwords. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)

July 9, 2024 - CVE 2024-38875 ¶

Potential denial-of-service in **`django.utils.html.urlize()`**. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)

March 4, 2024 - CVE 2024-27351 ¶

Potential regular expression denial-of-service in **`django.utils.text.Truncator.words()`**. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)
- Django 3.2 (patch)

February 6, 2024 - CVE 2024-24680 ¶

Potential denial-of-service in **`intcomma`** template filter. Full description

- Django 5.0 (patch)
- Django 4.2 (patch)
- Django 3.2 (patch)

November 1, 2023 - CVE 2023-46695 ¶

Potential denial of service vulnerability in **`UsernameField`** on Windows. Full description

- Django 4.2 (patch)
- Django 4.1 (patch)
- Django 3.2 (patch)

October 4, 2023 - CVE 2023-43665 ¶

Denial-of-service possibility in **`django.utils.text.Truncator`**. Full description

- Django 4.2 (patch)
- Django 4.1 (patch)
- Django 3.2 (patch)

September 4, 2023 - CVE 2023-41164 ¶

Potential denial of service vulnerability in **`django.utils.encoding.uri_to_iri()`**. Full description

- Django 4.2 (patch)
- Django 4.1 (patch)
- Django 3.2 (patch)

July 3, 2023 - CVE 2023-36053 ¶

Potential regular expression denial of service vulnerability in **`EmailValidator`**/**`URLValidator`**. Full description

- Django 4.2 (patch)
- Django 4.1 (patch)
- Django 3.2 (patch)

May 3, 2023 - CVE 2023-31047 ¶

Potential bypass of validation when uploading multiple files using one form field. Full description

- Django 4.2 (patch)
- Django 4.1 (patch)
- Django 3.2 (patch)

February 14, 2023 - CVE 2023-24580 ¶

Potential denial-of-service vulnerability in file uploads. Full description

- Django 4.1 (patch)
- Django 4.0 (patch)
- Django 3.2 (patch)

February 1, 2023 - CVE 2023-23969 ¶

Potential denial-of-service via **`Accept-Language`** headers. Full description

- Django 4.1 (patch)
- Django 4.0 (patch)
- Django 3.2 (patch)

October 4, 2022 - CVE 2022-41323 ¶

Potential denial-of-service vulnerability in internationalized URLs. Full description

- Django 4.1 (patch)
- Django 4.0 (patch)

- Django 3.2 (patch)

August 3, 2022 - CVE 2022-36359 ¶

Potential reflected file download vulnerability in FileResponse. Full description

- Django 4.0 (patch)
- Django 3.2 (patch)

July 4, 2022 - CVE 2022-34265 ¶

Potential SQL injection via **`Trunc(kind)`** and **`Extract(lookup_name)`** arguments. Full description

- Django 4.0 (patch)
- Django 3.2 (patch)

April 11, 2022 - CVE 2022-28346 ¶

Potential SQL injection in **`QuerySet.annotate()`**, **`aggregate()`**, and **`extra()`**. Full description

- Django 4.0 (patch)
- Django 3.2 (patch)
- Django 2.2 (patch)

April 11, 2022 - CVE 2022-28347 ¶

Potential SQL injection via **`QuerySet.explain(**options)`** on PostgreSQL. Full description

- Django 4.0 (patch)
- Django 3.2 (patch)
- Django 2.2 (patch)

February 1, 2022 - CVE 2022-22818 ¶

Possible XSS via **`{% debug %}`** template tag. Full description

Versions affected ¶

- Django 4.0 (patch)
- Django 3.2 (patch)
- Django 2.2 (patch)

February 1, 2022 - CVE 2022-23833 ¶

Denial-of-service possibility in file uploads. Full description

Versions affected ¶

- Django 4.0 (patch)
- Django 3.2 (patch)
- Django 2.2 (patch)

January 4, 2022 - CVE 2021-45452 ¶

Potential directory-traversal via **`Storage.save()`**. Full description

Versions affected ¶

- Django 4.0 (patch)
- Django 3.2 (patch)
- Django 2.2 (patch)

January 4, 2022 - CVE 2021-45116 ¶

Potential information disclosure in **`dictsort`** template filter. Full description

Versions affected ¶

- Django 4.0 (patch)
- Django 3.2 (patch)
- Django 2.2 (patch)

January 4, 2022 - CVE 2021-45115 ¶

Denial-of-service possibility in **`UserAttributeSimilarityValidator`**. Full description

Versions affected ¶

- Django 4.0 (patch)
- Django 3.2 (patch)
- Django 2.2 (patch)

December 7, 2021 - CVE 2021-44420 ¶

Potential bypass of an upstream access control based on URL paths. Full description

Versions affected ¶

- Django 3.2 (patch)
- Django 3.1 (patch)
- Django 2.2 (patch)

July 1, 2021 - CVE 2021-35042 ¶

Potential SQL injection via unsanitized **`QuerySet.order_by()`** input. Full description

Versions affected ¶

- Django 3.2 (patch)
- Django 3.1 (patch)

June 2, 2021 - CVE 2021-33203 ¶

Potential directory traversal via **`admindocs`**. Full description

Versions affected ¶

- Django 3.2 (patch)
- Django 3.1 (patch)
- Django 2.2 (patch)

June 2, 2021 - CVE 2021-33571 ¶

Possible indeterminate SSRF, RFI, and LFI attacks since validators accepted leading zeros in IPv4 addresses. Full description

Versions affected ¶

- Django 3.2 (patch)
- Django 3.1 (patch)
- Django 2.2 (patch)

May 6, 2021 - CVE 2021-32052 ¶

Header injection possibility since **`URLValidator`** accepted newlines in input on Python 3.9.5+. Full description

Versions affected ¶

- Django 3.2 (patch)
- Django 3.1 (patch)
- Django 2.2 (patch)

May 4, 2021 - CVE 2021-31542 ¶

Potential directory-traversal via uploaded files. Full description

Versions affected ¶

- Django 3.2 (patch)
- Django 3.1 (patch)
- Django 2.2 (patch)

April 6, 2021 - CVE 2021-28658 ¶

Potential directory-traversal via uploaded files. Full description

Versions affected ¶

- Django 3.2 (patch)
- Django 3.1 (patch)
- Django 3.0 (patch)
- Django 2.2 (patch)

February 19, 2021 - CVE 2021-23336 ¶

Web cache poisoning via **`django.utils.http.limited_parse_qsl()`**. Full description

Versions affected ¶

- Django 3.2 (patch)
- Django 3.1 (patch)
- Django 3.0 (patch)
- Django 2.2 (patch)

February 1, 2021 - CVE 2021-3281 ¶

Potential directory-traversal via **`archive.extract()`**. Full description

Versions affected ¶

- Django 3.1 (patch)
- Django 3.0 (patch)
- Django 2.2 (patch)

September 1, 2020 - CVE 2020-24584 ¶

Permission escalation in intermediate-level directories of the file system cache on Python 3.7+. Full description

Versions affected ¶

- Django 3.1 (patch)
- Django 3.0 (patch)
- Django 2.2 (patch)

September 1, 2020 - CVE 2020-24583 ¶

Incorrect permissions on intermediate-level directories on Python 3.7+. Full description

Versions affected ¶

- Django 3.1 (patch)
- Django 3.0 (patch)
- Django 2.2 (patch)

June 3, 2020 - CVE 2020-13596 ¶

Possible XSS via admin **`ForeignKeyRawIdWidget`**. Full description

Versions affected ¶

- Django 3.0 (patch)
- Django 2.2 (patch)

June 3, 2020 - CVE 2020-13254 ¶

Potential data leakage via malformed memcached keys. Full description

Versions affected ¶

- Django 3.0 (patch)
- Django 2.2 (patch)

March 4, 2020 - CVE 2020-9402 ¶

Potential SQL injection via **`tolerance`** parameter in GIS functions and aggregates on Oracle. Full description

Versions affected ¶

- Django 3.0 (patch)
- Django 2.2 (patch)

- Django 1.11 (patch)

February 3, 2020 - CVE 2020-7471 ¶

Potential SQL injection via **`StringAgg(delimiter)`**. Full description

Versions affected ¶

- Django 3.0 (patch)
- Django 2.2 (patch)
- Django 1.11 (patch)

December 18, 2019 - CVE 2019-19844 ¶

Potential account hijack via password reset form. Full description

Versions affected ¶

- Django 3.0 (patch)
- Django 2.2 (patch)
- Django 1.11 (patch)

December 2, 2019 - CVE 2019-19118 ¶

Privilege escalation in the Django admin. Full description

Versions affected ¶

- Django 3.0 (patch)
- Django 2.2 (patch)
- Django 2.1 (patch)

August 1, 2019 - CVE 2019-14235 ¶

Potential memory exhaustion in **`django.utils.encoding.uri_to_iri()`**. Full description

Versions affected ¶

- Django 2.2 (patch)
- Django 2.1 (patch)
- Django 1.11 (patch)

August 1, 2019 - CVE 2019-14234 ¶

SQL injection possibility in key and index lookups for **`JSONField`**/**`HStoreField`**. Full description

Versions affected ¶

- Django 2.2 (patch)
- Django 2.1 (patch)
- Django 1.11 (patch)

August 1, 2019 - CVE 2019-14233 ¶

Denial-of-service possibility in **`strip_tags()`**. Full description

Versions affected ¶

- Django 2.2 (patch)
- Django 2.1 (patch)
- Django 1.11 (patch)

August 1, 2019 - CVE 2019-14232 ¶

Denial-of-service possibility in **`django.utils.text.Truncator`**. Full description

Versions affected ¶

- Django 2.2 (patch)
- Django 2.1 (patch)
- Django 1.11 (patch)

July 1, 2019 - CVE 2019-12781 ¶

Incorrect HTTP detection with reverse-proxy connecting via HTTPS. Full description

Versions affected ¶

- Django 2.2 (patch)
- Django 2.1 (patch)
- Django 1.11 (patch)

June 3, 2019 - CVE 2019-12308 ¶

XSS via "Current URL" link generated by **`AdminURLFieldWidget`**. Full description

Versions affected ¶

- Django 2.2 (patch)
- Django 2.1 (patch)
- Django 1.11 (patch)

June 3, 2019 - CVE 2019-11358 ¶

Prototype pollution in bundled jQuery. Full description

Versions affected ¶

- Django 2.2 (patch)
- Django 2.1 (patch)

February 11, 2019 - CVE 2019-6975 ¶

Memory exhaustion in **`django.utils.numberformat.format()`**. Full description

Versions affected ¶

- Django 2.1 (patch)
- Django 2.0 (patch and correction)
- Django 1.11 (patch)

January 4, 2019 - CVE 2019-3498 ¶

Content spoofing possibility in the default 404 page. Full description

Versions affected ¶

- Django 2.1 (patch)
- Django 2.0 (patch)
- Django 1.11 (patch)

October 1, 2018 - CVE 2018-16984 ¶

Password hash disclosure to "view only" admin users. Full description

Versions affected ¶

- Django 2.1 (patch)

August 1, 2018 - CVE 2018-14574 ¶

Open redirect possibility in **`CommonMiddleware`**. Full description

Versions affected ¶

- Django 2.1 (patch)
- Django 2.0 (patch)
- Django 1.11 (patch)

March 6, 2018 - CVE 2018-7537 ¶

Denial-of-service possibility in **`truncatechars_html`** and **`truncatewords_html`** template filters. Full description

Versions affected ¶

- Django 2.0 (patch)
- Django 1.11 (patch)

- Django 1.8 (patch)

March 6, 2018 - CVE 2018-7536 ¶

Denial-of-service possibility in **`urlize`** and **`urlizetrunc`** template filters. Full description

Versions affected ¶

- Django 2.0 (patch)
- Django 1.11 (patch)
- Django 1.8 (patch)

February 1, 2018 - CVE 2018-6188 ¶

Information leakage in **`AuthenticationForm`**. Full description

Versions affected ¶

- Django 2.0 (patch)
- Django 1.11 (patch)

September 5, 2017 - CVE 2017-12794 ¶

Possible XSS in traceback section of technical 500 debug page. Full description

Versions affected ¶

- Django 1.11 (patch)
- Django 1.10 (patch)

April 4, 2017 - CVE 2017-7234 ¶

Open redirect vulnerability in **`django.views.static.serve()`**. Full description

Versions affected ¶

- Django 1.10 (patch)
- Django 1.9 (patch)
- Django 1.8 (patch)

April 4, 2017 - CVE 2017-7233 ¶

Open redirect and possible XSS attack via user-supplied numeric redirect URLs. Full description

Versions affected ¶

- Django 1.10 (patch)
- Django 1.9 (patch)
- Django 1.8 (patch)

November 1, 2016 - CVE 2016-9014 ¶

DNS rebinding vulnerability when **`DEBUG=True`**. Full description

Versions affected ¶

- Django 1.10 (patch)
- Django 1.9 (patch)
- Django 1.8 (patch)

November 1, 2016 - CVE 2016-9013 ¶

User with hardcoded password created when running tests on Oracle. Full description

Versions affected ¶

- Django 1.10 (patch)
- Django 1.9 (patch)
- Django 1.8 (patch)

September 26, 2016 - CVE 2016-7401 ¶

CSRF protection bypass on a site with Google Analytics. Full description

Versions affected ¶

- Django 1.9 (patch)
- Django 1.8 (patch)

July 18, 2016 - CVE 2016-6186 ¶

XSS in admin's add/change related popup. Full description

Versions affected ¶

- Django 1.9 (patch)
- Django 1.8 (patch)

March 1, 2016 - CVE 2016-2513 ¶

User enumeration through timing difference on password hasher work factor upgrade. Full description

Versions affected ¶

- Django 1.9 (patch)
- Django 1.8 (patch)

March 1, 2016 - CVE 2016-2512 ¶

Malicious redirect and possible XSS attack via user-supplied redirect URLs containing basic auth. Full description

Versions affected ¶

- Django 1.9 (patch)
- Django 1.8 (patch)

February 1, 2016 - CVE 2016-2048 ¶

User with "change" but not "add" permission can create objects for **`ModelAdmin`**'s with **`save_as=True`**. Full description

Versions affected ¶

- Django 1.9 (patch)

November 24, 2015 - CVE 2015-8213 ¶

Settings leak possibility in **`date`** template filter. Full description

Versions affected ¶

- Django 1.8 (patch)
- Django 1.7 (patch)

August 18, 2015 - CVE 2015-5963 / CVE 2015-5964 ¶

Denial-of-service possibility in **`logout()`** view by filling session store. Full description

Versions affected ¶

- Django 1.8 (patch)
- Django 1.7 (patch)
- Django 1.4 (patch)

July 8, 2015 - CVE 2015-5145 ¶

Denial-of-service possibility in URL validation. Full description

Versions affected ¶

- Django 1.8 (patch)

July 8, 2015 - CVE 2015-5144 ¶

Header injection possibility since validators accept newlines in input. Full description

Versions affected ¶

- Django 1.8 (patch)
- Django 1.7 (patch)
- Django 1.4 (patch)

July 8, 2015 - CVE 2015-5143 ¶

Denial-of-service possibility by filling session store. Full description

Versions affected ¶

- Django 1.8 (patch)
- Django 1.7 (patch)
- Django 1.4 (patch)

May 20, 2015 - CVE 2015-3982 ¶

Fixed session flushing in the cached_db backend. Full description

Versions affected ¶

- Django 1.8 (patch)

March 18, 2015 - CVE 2015-2317 ¶

Mitigated possible XSS attack via user-supplied redirect URLs. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)
- Django 1.8 (patch)

March 18, 2015 - CVE 2015-2316 ¶

Denial-of-service possibility with **`strip_tags()`**. Full description

Versions affected ¶

- Django 1.6 (patch)
- Django 1.7 (patch)
- Django 1.8 (patch)

March 9, 2015 - CVE 2015-2241 ¶

XSS attack via properties in **`ModelAdmin.readonly_fields`**. Full description

Versions affected ¶

- Django 1.7 (patch)
- Django 1.8 (patch)

January 13, 2015 - CVE 2015-0222 ¶

Database denial-of-service with **`ModelMultipleChoiceField`**. Full description

Versions affected ¶

- Django 1.6 (patch)
- Django 1.7 (patch)

January 13, 2015 - CVE 2015-0221 ¶

Denial-of-service attack against **`django.views.static.serve()`**. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

January 13, 2015 - CVE 2015-0220 ¶

Mitigated possible XSS attack via user-supplied redirect URLs. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

January 13, 2015 - CVE 2015-0219 ¶

WSGI header spoofing via underscore/dash conflation. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

August 20, 2014 - CVE 2014-0483 ¶

Data leakage via querystring manipulation in admin. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

August 20, 2014 - CVE 2014-0482 ¶

`RemoteUserMiddleware` session hijacking. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

August 20, 2014 - CVE 2014-0481 ¶

File upload denial of service. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

August 20, 2014 - CVE 2014-0480 ¶

`reverse()` can generate URLs pointing to other hosts. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

May 18, 2014 - CVE 2014-3730 ¶

Malformed URLs from user input incorrectly validated. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

May 18, 2014 - CVE 2014-1418 ¶

Caches may be allowed to store and serve private data. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

April 21, 2014 - CVE 2014-0474 ¶

MySQL typecasting causes unexpected query results. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

April 21, 2014 - CVE 2014-0473 ¶

Caching of anonymous pages could reveal CSRF token. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

April 21, 2014 - CVE 2014-0472 ¶

Unexpected code execution using **`reverse()`**. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)
- Django 1.6 (patch)
- Django 1.7 (patch)

September 14, 2013 - CVE 2013-1443 ¶

Denial-of-service via large passwords. Full description

Versions affected ¶

- Django 1.4 (patch and Python compatibility fix)
- Django 1.5 (patch)

September 10, 2013 - CVE 2013-4315 ¶

Directory-traversal via **`ssi`** template tag. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)

August 13, 2013 - CVE 2013-6044 ¶

Possible XSS via unvalidated URL redirect schemes. Full description

Versions affected ¶

- Django 1.4 (patch)
- Django 1.5 (patch)

August 13, 2013 - CVE 2013-4249 ¶

XSS via admin trusting **`URLField`** values. Full description

Versions affected ¶

- Django 1.5 (patch)

February 19, 2013 - CVE 2013-0306 ¶

Denial-of-service via formset `max_num` bypass. Full description

Versions affected ¶

- Django 1.3 (patch)
- Django 1.4 (patch)

February 19, 2013 - CVE 2013-0305 ¶

Information leakage via admin history log. Full description

Versions affected ¶

- Django 1.3 (patch)
- Django 1.4 (patch)

February 19, 2013 - CVE 2013-1664 / CVE 2013-1665 ¶

Entity-based attacks against Python XML libraries. Full description

Versions affected ¶

- Django 1.3 (patch)
- Django 1.4 (patch)

February 19, 2013 - No CVE ¶

Additional hardening of `Host` header handling. Full description

Versions affected ¶

- Django 1.3 (patch)
- Django 1.4 (patch)

December 10, 2012 - No CVE 2 ¶

Additional hardening of redirect validation. Full description

Versions affected ¶

- Django 1.3: (patch)
- Django 1.4: (patch)

December 10, 2012 - No CVE 1 ¶

Additional hardening of `Host` header handling. Full description

Versions affected ¶

- Django 1.3 (patch)
- Django 1.4 (patch)

October 17, 2012 - CVE 2012-4520 ¶

`Host` header poisoning. Full description

Versions affected ¶

- Django 1.3 (patch)
- Django 1.4 (patch)

July 30, 2012 - CVE 2012-3444 ¶

Denial-of-service via large image files. Full description

Versions affected ¶

- Django 1.3 (patch)
- Django 1.4 (patch)

July 30, 2012 - CVE 2012-3443 ¶

Denial-of-service via compressed image files. Full description

Versions affected ¶

- Django 1.3: (patch)

- Django 1.4: (patch)

July 30, 2012 - CVE 2012-3442 ¶

XSS via failure to validate redirect scheme. Full description

Versions affected ¶

- Django 1.3: (patch)
- Django 1.4: (patch)

September 9, 2011 - CVE 2011-4140 ¶

Potential CSRF via **`Host`** header. Full description

Versions affected ¶

This notification was an advisory only, so no patches were issued.

- Django 1.2
- Django 1.3

September 9, 2011 - CVE 2011-4139 ¶

`Host` header cache poisoning. Full description

Versions affected ¶

- Django 1.2 (patch)
- Django 1.3 (patch)

September 9, 2011 - CVE 2011-4138 ¶

Information leakage/arbitrary request issuance via **`URLField.verify_exists`**. Full description

Versions affected ¶

- Django 1.2: (patch)
- Django 1.3: (patch)

September 9, 2011 - CVE 2011-4137 ¶

Denial-of-service via **`URLField.verify_exists`**. Full description

Versions affected ¶

- Django 1.2 (patch)
- Django 1.3 (patch)

September 9, 2011 - CVE 2011-4136 ¶

Session manipulation when using memory-cache-backed session. Full description

Versions affected ¶

- Django 1.2 (patch)
- Django 1.3 (patch)

February 8, 2011 - CVE 2011-0698 ¶

Directory-traversal on Windows via incorrect path-separator handling. Full description

Versions affected ¶

- Django 1.1 (patch)
- Django 1.2 (patch)

February 8, 2011 - CVE 2011-0697 ¶

XSS via unsanitized names of uploaded files. Full description

Versions affected ¶

- Django 1.1 (patch)
- Django 1.2 (patch)

February 8, 2011 - CVE 2011-0696 ¶

CSRF via forged HTTP headers. Full description

Versions affected ¶

- Django 1.1 (patch)
- Django 1.2 (patch)

December 22, 2010 - CVE 2010-4535 ¶

Denial-of-service in password-reset mechanism. Full description

Versions affected ¶

- Django 1.1 (patch)
- Django 1.2 (patch)

December 22, 2010 - CVE 2010-4534 ¶

Information leakage in administrative interface. Full description

Versions affected ¶

- Django 1.1 (patch)
- Django 1.2 (patch)

September 8, 2010 - CVE 2010-3082 ¶

XSS via trusting unsafe cookie value. Full description

Versions affected ¶

- Django 1.2 (patch)

October 9, 2009 - CVE 2009-3695 ¶

Denial-of-service via pathological regular expression performance. Full description

Versions affected ¶

- Django 1.0 (patch)
- Django 1.1 (patch)

July 28, 2009 - CVE 2009-2659 ¶

Directory-traversal in development server media handler. Full description

Versions affected ¶

- Django 0.96 (patch)
- Django 1.0 (patch)

September 2, 2008 - CVE 2008-3909 ¶

CSRF via preservation of POST data during admin login. Full description

Versions affected ¶

- Django 0.91 (patch)
- Django 0.95 (patch)
- Django 0.96 (patch)

May 14, 2008 - CVE 2008-2302 ¶

XSS via admin login redirect. Full description

Versions affected ¶

- Django 0.91 (patch)
- Django 0.95 (patch)
- Django 0.96 (patch)

October 26, 2007 - CVE 2007-5712 ¶

Denial-of-service via arbitrarily-large `Accept-Language` header. Full description

Versions affected ¶

- Django 0.91 (patch)
- Django 0.95 (patch)

- Django 0.96 (patch)

Issues prior to Django's security process ¶

Some security issues were handled before Django had a formalized security process in use. For these, new releases may not have been issued at the time and CVEs may not have been assigned.

January 21, 2007 - CVE 2007-0405 ¶

Apparent "caching" of authenticated user. Full description

Versions affected ¶

- Django 0.95 (patch)

August 16, 2006 - CVE 2007-0404 ¶

Filename validation issue in translation framework. Full description

Versions affected ¶

- Django 0.90 (patch)
- Django 0.91 (patch)
- Django 0.95 (patch) (released January 21 2007)

Contents

- February 3, 2026 - **CVE 2025-14550**
- February 3, 2026 - **CVE 2026-1207**
- February 3, 2026 - **CVE 2026-1285**
- February 3, 2026 - **CVE 2026-1287**
- February 3, 2026 - **CVE 2026-1312**
- December 2, 2025 - **CVE 2025-13372**
- December 2, 2025 - **CVE 2025-64460**
- November 5, 2025 - **CVE 2025-64458**
- November 5, 2025 - **CVE 2025-64459**
- October 1, 2025 - **CVE 2025-59681**
- October 1, 2025 - **CVE 2025-59682**
- September 3, 2025 - **CVE 2025-57833**
- June 4, 2025 - **CVE 2025-48432**
- May 7, 2025 - **CVE 2025-32873**
- April 2, 2025 - **CVE 2025-27556**
- March 6, 2025 - **CVE 2025-26699**
- January 14, 2025 - **CVE 2024-56374**
- December 4, 2024 - **CVE 2024-53907**
- December 4, 2024 - **CVE 2024-53908**
- September 3, 2024 - **CVE 2024-45231**
- September 3, 2024 - **CVE 2024-45230**
- August 6, 2024 - **CVE 2024-42005**
- August 6, 2024 - **CVE 2024-41991**
- August 6, 2024 - **CVE 2024-41990**
- August 6, 2024 - **CVE 2024-41989**
- July 9, 2024 - **CVE 2024-39614**
- July 9, 2024 - **CVE 2024-39330**
- July 9, 2024 - **CVE 2024-39329**
- July 9, 2024 - **CVE 2024-38875**
- March 4, 2024 - **CVE 2024-27351**
- February 6, 2024 - **CVE 2024-24680**
- November 1, 2023 - **CVE 2023-46695**
- October 4, 2023 - **CVE 2023-43665**
- September 4, 2023 - **CVE 2023-41164**
- July 3, 2023 - **CVE 2023-36053**
- May 3, 2023 - **CVE 2023-31047**
- February 14, 2023 - **CVE 2023-24580**
- February 1, 2023 - **CVE 2023-23969**
- October 4, 2022 - **CVE 2022-41323**
- August 3, 2022 - **CVE 2022-36359**
- July 4, 2022 - **CVE 2022-34265**
- April 11, 2022 - **CVE 2022-28346**

Getting Help

- April 11, 2022 - **CVE 2022-28347**
- February 1, 2022 - **CVE 2022-22818**
  - Versions affected
- February 1, 2022 - **CVE 2022-23833**
  - Versions affected
- January 4, 2022 - **CVE 2021-45452**
  - Versions affected
- January 4, 2022 - **CVE 2021-45116**
  - Versions affected
- January 4, 2022 - **CVE 2021-45115**
  - Versions affected
- December 7, 2021 - **CVE 2021-44420**
  - Versions affected
- July 1, 2021 - **CVE 2021-35042**
  - Versions affected
- June 2, 2021 - **CVE 2021-33203**
  - Versions affected
- June 2, 2021 - **CVE 2021-33571**
  - Versions affected
- May 6, 2021 - **CVE 2021-32052**
  - Versions affected
- May 4, 2021 - **CVE 2021-31542**
  - Versions affected
- April 6, 2021 - **CVE 2021-28658**
  - Versions affected
- February 19, 2021 - **CVE 2021-23336**
  - Versions affected
- February 1, 2021 - **CVE 2021-3281**
  - Versions affected
- September 1, 2020 - **CVE 2020-24584**
  - Versions affected
- September 1, 2020 - **CVE 2020-24583**
  - Versions affected
- June 3, 2020 - **CVE 2020-13596**
  - Versions affected
- June 3, 2020 - **CVE 2020-13254**
  - Versions affected
- March 4, 2020 - **CVE 2020-9402**
  - Versions affected
- February 3, 2020 - **CVE 2020-7471**
  - Versions affected
- December 18, 2019 - **CVE 2019-19844**

- Versions affected
- December 2, 2019 - **CVE 2019-19118**
  - Versions affected
- August 1, 2019 - **CVE 2019-14235**
  - Versions affected
- August 1, 2019 - **CVE 2019-14234**
  - Versions affected
- August 1, 2019 - **CVE 2019-14233**
  - Versions affected
- August 1, 2019 - **CVE 2019-14232**
  - Versions affected
- July 1, 2019 - **CVE 2019-12781**
  - Versions affected
- June 3, 2019 - **CVE 2019-12308**
  - Versions affected
- June 3, 2019 - **CVE 2019-11358**
  - Versions affected
- February 11, 2019 - **CVE 2019-6975**
  - Versions affected
- January 4, 2019 - **CVE 2019-3498**
  - Versions affected
- October 1, 2018 - **CVE 2018-16984**
  - Versions affected
- August 1, 2018 - **CVE 2018-14574**
  - Versions affected
- March 6, 2018 - **CVE 2018-7537**
  - Versions affected
- March 6, 2018 - **CVE 2018-7536**
  - Versions affected
- February 1, 2018 - **CVE 2018-6188**
  - Versions affected
- September 5, 2017 - **CVE 2017-12794**
  - Versions affected
- April 4, 2017 - **CVE 2017-7234**
  - Versions affected
- April 4, 2017 - **CVE 2017-7233**
  - Versions affected
- November 1, 2016 - **CVE 2016-9014**
  - Versions affected
- November 1, 2016 - **CVE 2016-9013**
  - Versions affected
- September 26, 2016 - **CVE 2016-7401**

- Versions affected
- July 18, 2016 - **CVE 2016-6186**
  - Versions affected
- March 1, 2016 - **CVE 2016-2513**
  - Versions affected
- March 1, 2016 - **CVE 2016-2512**
  - Versions affected
- February 1, 2016 - **CVE 2016-2048**
  - Versions affected
- November 24, 2015 - **CVE 2015-8213**
  - Versions affected
- August 18, 2015 - **CVE 2015-5963** / **CVE 2015-5964**
  - Versions affected
- July 8, 2015 - **CVE 2015-5145**
  - Versions affected
- July 8, 2015 - **CVE 2015-5144**
  - Versions affected
- July 8, 2015 - **CVE 2015-5143**
  - Versions affected
- May 20, 2015 - **CVE 2015-3982**
  - Versions affected
- March 18, 2015 - **CVE 2015-2317**
  - Versions affected
- March 18, 2015 - **CVE 2015-2316**
  - Versions affected
- March 9, 2015 - **CVE 2015-2241**
  - Versions affected
- January 13, 2015 - **CVE 2015-0222**
  - Versions affected
- January 13, 2015 - **CVE 2015-0221**
  - Versions affected
- January 13, 2015 - **CVE 2015-0220**
  - Versions affected
- January 13, 2015 - **CVE 2015-0219**
  - Versions affected
- August 20, 2014 - **CVE 2014-0483**
  - Versions affected
- August 20, 2014 - **CVE 2014-0482**
  - Versions affected
- August 20, 2014 - **CVE 2014-0481**
  - Versions affected
- August 20, 2014 - **CVE 2014-0480**

- Versions affected
- May 18, 2014 - **CVE 2014-3730**
  - Versions affected
- May 18, 2014 - **CVE 2014-1418**
  - Versions affected
- April 21, 2014 - **CVE 2014-0474**
  - Versions affected
- April 21, 2014 - **CVE 2014-0473**
  - Versions affected
- April 21, 2014 - **CVE 2014-0472**
  - Versions affected
- September 14, 2013 - **CVE 2013-1443**
  - Versions affected
- September 10, 2013 - **CVE 2013-4315**
  - Versions affected
- August 13, 2013 - **CVE 2013-6044**
  - Versions affected
- August 13, 2013 - **CVE 2013-4249**
  - Versions affected
- February 19, 2013 - **CVE 2013-0306**
  - Versions affected
- February 19, 2013 - **CVE 2013-0305**
  - Versions affected
- February 19, 2013 - **CVE 2013-1664** / **CVE 2013-1665**
  - Versions affected
- February 19, 2013 - No CVE
  - Versions affected
- December 10, 2012 - No CVE 2
  - Versions affected
- December 10, 2012 - No CVE 1
  - Versions affected
- October 17, 2012 - **CVE 2012-4520**
  - Versions affected
- July 30, 2012 - **CVE 2012-3444**
  - Versions affected
- July 30, 2012 - **CVE 2012-3443**
  - Versions affected
- July 30, 2012 - **CVE 2012-3442**
  - Versions affected
- September 9, 2011 - **CVE 2011-4140**
  - Versions affected
- September 9, 2011 - **CVE 2011-4139**

        - Versions affected
    - September 9, 2011 - **CVE 2011-4138**
        - Versions affected
    - September 9, 2011 - **CVE 2011-4137**
        - Versions affected
    - September 9, 2011 - **CVE 2011-4136**
        - Versions affected
    - February 8, 2011 - **CVE 2011-0698**
        - Versions affected
    - February 8, 2011 - **CVE 2011-0697**
        - Versions affected
    - February 8, 2011 - **CVE 2011-0696**
        - Versions affected
    - December 22, 2010 - **CVE 2010-4535**
        - Versions affected
    - December 22, 2010 - **CVE 2010-4534**
        - Versions affected
    - September 8, 2010 - **CVE 2010-3082**
        - Versions affected
    - October 9, 2009 - **CVE 2009-3695**
        - Versions affected
    - July 28, 2009 - **CVE 2009-2659**
        - Versions affected
    - September 2, 2008 - **CVE 2008-3909**
        - Versions affected
    - May 14, 2008 - **CVE 2008-2302**
        - Versions affected
    - October 26, 2007 - **CVE 2007-5712**
        - Versions affected
- Issues prior to Django's security process
    - January 21, 2007 - **CVE 2007-0405**
        - Versions affected
    - August 16, 2006 - **CVE 2007-0404**
        - Versions affected

Getting help

Getting Help

FAQ
Try the FAQ — it's got answers to many common questions.

Index, Module Index, or Table of Contents
Handy when looking for specific information.

Django Discord Server
Join the Django Discord Community.

Official Django Forum
Join the community on the Django Forum.

Ticket tracker
Report bugs with Django or Django documentation in our ticket tracker.

Download:

Offline (development version): HTML | PDF | ePub
Provided by Read the Docs.

Diamond and Platinum Members

Sentry

Monitor your Django Code Resolve performance bottlenecks and errors using monitoring, replays, logs and Seer an AI agent for debugging.

JetBrains

JetBrains delivers intelligent software solutions that make developers more productive by simplifying their challenging tasks, automating the routine, and helping them adopt the best development practices. PyCharm is the Python IDE for Professional Developers by JetBrains providing a complete set of tools for productive Python, Web and scientific development.

Kraken Tech

Kraken is the most-loved operating system for energy. Powered by our Utility-Grade AI™ and deep industry know-how, we help utilities transform their technology and operations so they can lead the energy transition. Delivering better outcomes from generation through distribution to supply, Kraken powers 70+ million accounts worldwide, and is on a mission to make a big, green dent in the universe.

Getting Help

PostHog

PostHog is an all-in-one developer platform for building successful products. We provide product analytics, web analytics, session replay, error tracking, feature flags, experiments, surveys, LLM observability, data warehouse, CDP, workflows, logs, and an AI product assistant to help debug your code, ship features faster, and keep all your usage and customer data in one stack.

Learn More

About Django

Getting Started with Django

Team Organization

Django Software Foundation

Code of Conduct

Diversity Statement

Get Involved

Join a Group

Contribute to Django

Submit a Bug

Report a Security Issue

Individual membership

Get Help

Getting Help FAQ

Django Discord

Official Django Forum

Getting Help

Follow Us

GitHub

X

Fediverse (Mastodon)

Bluesky

LinkedIn

News RSS

Support Us

Sponsor Django

Corporate membership

Official merchandise store

Benevity Workplace Giving Program

Getting Help