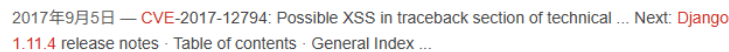


6月26日

```
```json
{
 "analysis": {
 "8000": {
 "service": "Django development server (WSGIServer/0.2 CPython/3.5.9)",
 "framework": "Django 1.11.4 (Python 3.5.9)",
 "vulnerabilities": {
 "confirmed": [
 "Unprotected user creation endpoint (GET request)",
 "XSS vulnerability (HTML/JS execution via username parameter)",
 "Debug mode enabled exposing sensitive information"
],
 "potential": [
 "SQL injection (payloads accepted without error)",
 "CSRF protection bypass",
 "Mass account creation vulnerability"
]
 },
 "exploitation": {
 "xss_confirmed": true,
 "sql_injection_status": "payloads accepted but impact unverified",
 "debug_exposure": "Full stack traces and configuration visible"
 }
 }
 },
 "next_step": [
 "Verify SQL injection impact by attempting to extract database information",
 "Check for CSRF protection bypass techniques",
 "Test for privilege escalation through created accounts",
 "Investigate if debug mode exposes additional sensitive endpoints"
],
 "executable": "curl -v 'http://192.168.18.128:8000/create_user/?username=admin' -- '"
}
```
```

上图为信息收集阶段的最终总结部分，根据上述信息在线检索对应的CVE



Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

OSCHINA

资讯 软件 博客 动弹 专区 问答 活动 工具 培训 APP Gitee 新媒体

大家都在搜...

开源资讯 / Django / 正文

6月28日晚8点
直播带榜首播

阿里云 领1728元优惠券 享百款产品折上折
云服务器 限时抢购 38元/年起
AI 大模型 免费体验 超7000万token
立即抢购

热门资讯
1. 尤雨溪创业公司 VoidZero 推出 Oxlint 1.0 稳定版, 基于 Rust 的静态代码分析工具
2. Spring AI Alibaba 1.0 GA 正式发布, Java 智能体开发进入新时代
3. X.Org Server 项目回滚了大量代码
4. 华为自研仓颉编程语言将于 7 月 30 日开源

Django 1.11.4 发布, Python 的 Web 框架

来源: 投稿 2017-08-02 07:33:14 0

阿里云飞天发布时刻, 领先大模型限免, 超 7000 万 tokens 免费体验

Django 是一个高级的 Python Web 框架, 旨在快速开发和简单, 实用的设计。

Django 1.11.4 已发布, 该版本修复了 1.11.3 中的一些 bug, 具体如下:

- Fixed a regression in 1.11.3 on Python 2 where non-ASCII "format" values for date/time widgets results in an empty "value" in the widget's HTML
- Fixed "QuerySet.union()" and "difference()" when combining with a queryset raising "EmptyResultSet"
- Fixed a regression in pickling of "LazyObject" on Python 2 when the wrapped object doesn't have "__reduce__()"

0 评论

5 收藏

分享

https://blog.csdn.net/ml_1019/article/details/76941745

python1.11.4

Q 搜索 AI 搜索 登录 会员

VeeLe

博客等级 码龄10年

65 69 224 92

原创 点赞 收藏 粉丝

关注 私信

创作助手

大纲生成/代码生成/文章润色...

深度思考 (R1)

云服务器 限时38元/年起 | 至高领1728元

python3.6.1 django1.11.4 初探

原创 于 2017-08-08 20:33:05 发布 · 883 阅读 · 0 点赞 · 0 收藏 · CC 4.0 BY-SA 版权

文章标签: #django #python

django 专栏收录该内容

3 篇文章 订阅专栏

安装django

直接用pip 安装, 并在命令行查看版本号

```
1 import django
2 django.VERSION # (1, 11, 4, 'final', 0) 安装成功
```

配置django

- 1.在指定目录下运行一下命令
django -h -admin startproject website(项目名称)
- 2.在项目目录下运行:
django-admin startapp blog (app名称)
- 3.文件结构如下:

复制链接

诸如上述一些论坛博客等来源的信息对检索过程的帮助较小



cve django framework 1.11.4



全部 视频 图片 购物 短视频 新闻 网页 更多

工具

National Institute of Standards and Technology (.gov)
<https://nvd.nist.gov/vuln/CVE-2017-12794> · [翻译此页](#)

CVE-2017-12794 Detail - NVD

2017年9月7日 — In Django 1.10.x before 1.10.8 and 1.11.x before 1.11.5, HTML autoescaping was disabled in a portion of the template for the technical 500 debug page.

GitHub
<https://github.com/vulhub/vulhub/blob/master/vulhub/django/CVE-2017-12794/README.md> · [翻译此页](#)

vulhub/django/CVE-2017-12794/README.md at master

Django versions before 1.11.5 and 1.10.8 contain a cross-site scripting (XSS) vulnerability in the debug error page.

Django documentation
<https://docs.djangoproject.com/releases/1.11.4/> · [翻译此页](#)

Django 1.11.4 release notes

2017年8月1日 — Django 1.11.4 release notes¶. August 1, 2017. Django 1.11.4 fixes several bugs in 1.11.3. Bugfixes¶. Fixed a regression in 1.11.3 on Python ...

Django documentation
<https://docs.djangoproject.com/releases/1.11.4/> · [翻译此页](#)

Archive of security issues

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 ...

[Issues under Django's security...](#)

[June 4, 2025 - CVE 2025-48432](#)

National Institute of Standards and Technology (.gov)
<https://nvd.nist.gov/vuln/detail/CVE-2019-14234> · [翻译此页](#)

CVE-2019-14234 - NVD

An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. Due to an error in shallow key transformation.

构造其他检索词的检索结果如上所示,

An official website of the United States government [Here's how you know](#)

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2019-14234 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. Due to an error in shallow key transformation, key and index lookups for django.contrib.postgres.fields.JSONField, and key lookups for django.contrib.postgres.fields.HStoreField, were subject to **SQL Injection**. This could, for example, be exploited via crafted use of "OR 1=1" in a key or index name to return all records, using a suitably crafted dictionary, with dictionary expansion, as the **kwargs passed to the QuerySet.filter() function.

QUICK INFO

CVE Dictionary Entry:
CVE-2019-14234

NVD Published Date:
08/09/2019

NVD Last Modified:
11/20/2024

Source:
MITRE

下图是利用Django 1.11.4首先在数据库中匹配到其对应的CPE，然后利用CPE在线检索相关CVE，总结三次检索内容可知，CVE-2017-12794较符合信息收集阶段所收集到的内容



CVE Details

<https://www.cvedetails.com> › version › Djan... › 翻译此页

Djangoproject Django 1.11.4 security vulnerabilities, CVEs

Djangoproject Django version 1.11.4 security vulnerabilities, CVEs, exploits, vulnerability statistics, CVSS scores and references.



National Institute of Standards and Technology (.gov)

<https://nvd.nist.gov> › vuln › CVE-2017-12... › 翻译此页

CVE-2017-12794 Detail - NVD

2017年9月7日 — In Django 1.10.x before 1.10.8 and 1.11.x before 1.11.5, HTML autoescaping was disabled in a portion of the template for the technical 500 debug page.



CVE Details

<https://www.cvedetails.com> › version › Djan... › 翻译此页

Django Project Django 1.11.4 security vulnerabilities, CVEs

This page lists vulnerability statistics for CVEs published in the last ten years, if any, for Django Project » Django » 1.11.4 . Vulnerability statistics ...



National Institute of Standards and Technology (.gov)

<https://nvd.nist.gov> › detail › change-record › 翻译此页

CVE-2017-12794 - NVD

Initial Analysis by NIST 9/14/2017 2:06:04 PM ; Added, CPE Configuration, OR
cpe:2.3:a:django:django:1.10.0::*:*:*:* *cpe:2.3:a:django:django ...



Security Database

<https://www.security-database.com> › detail › 翻译此页

CVE-2024-45231 - Alert Detail

An issue was discovered in Django v5.1.1, v5.0.9, and v4.2.16. The
django.contrib.auth.forms.PasswordResetForm class, when used in a view implementing ...