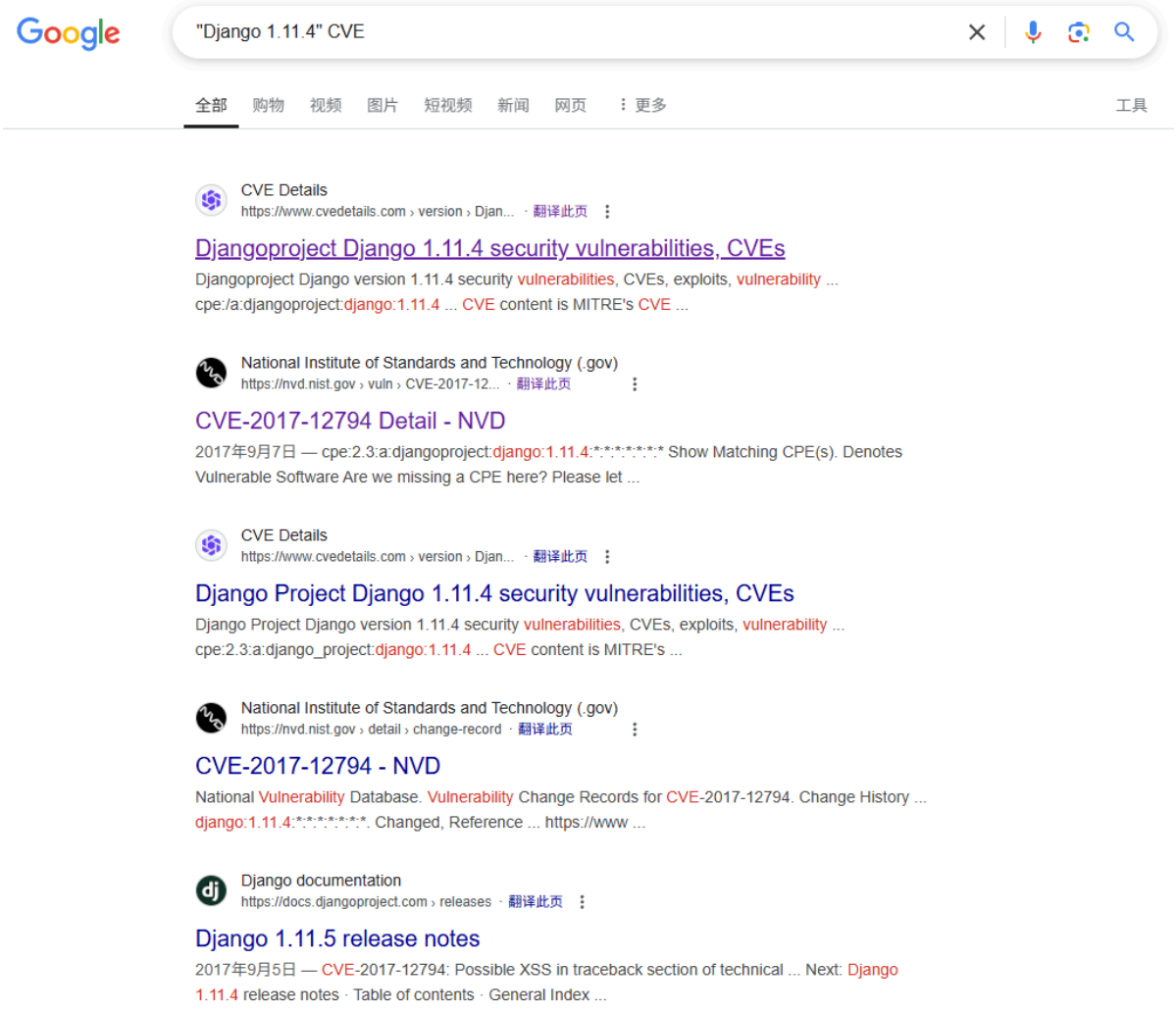
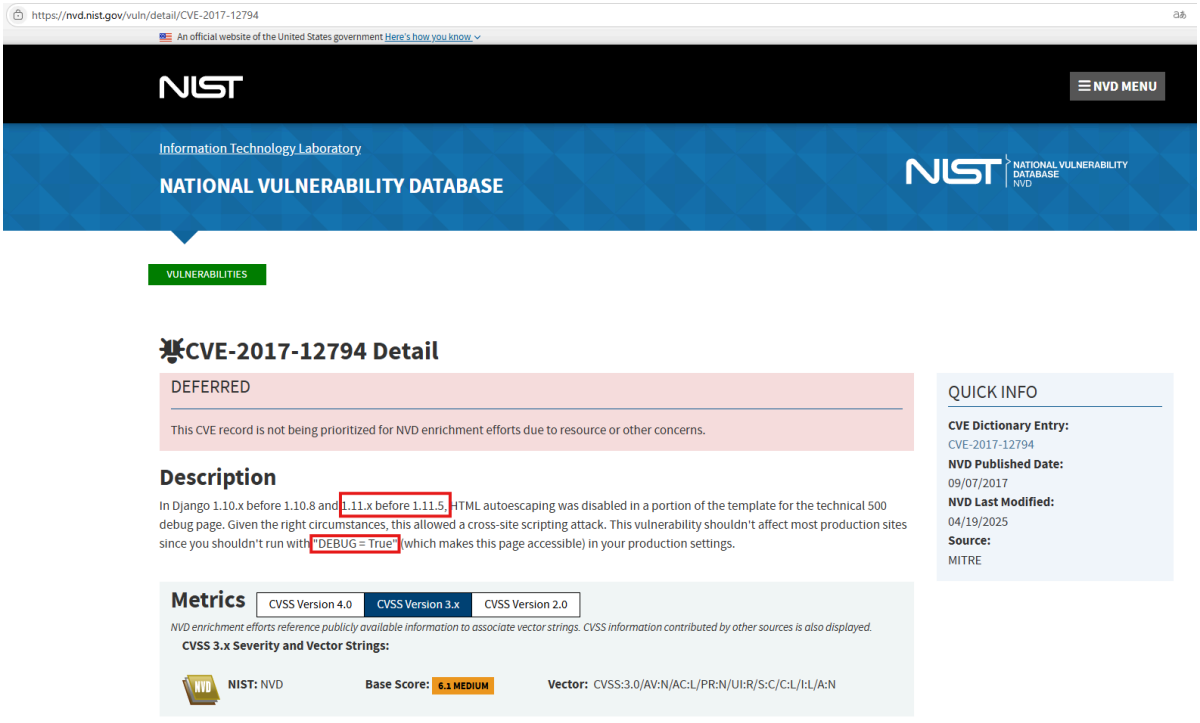
6月26日

```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'--'"
}
```

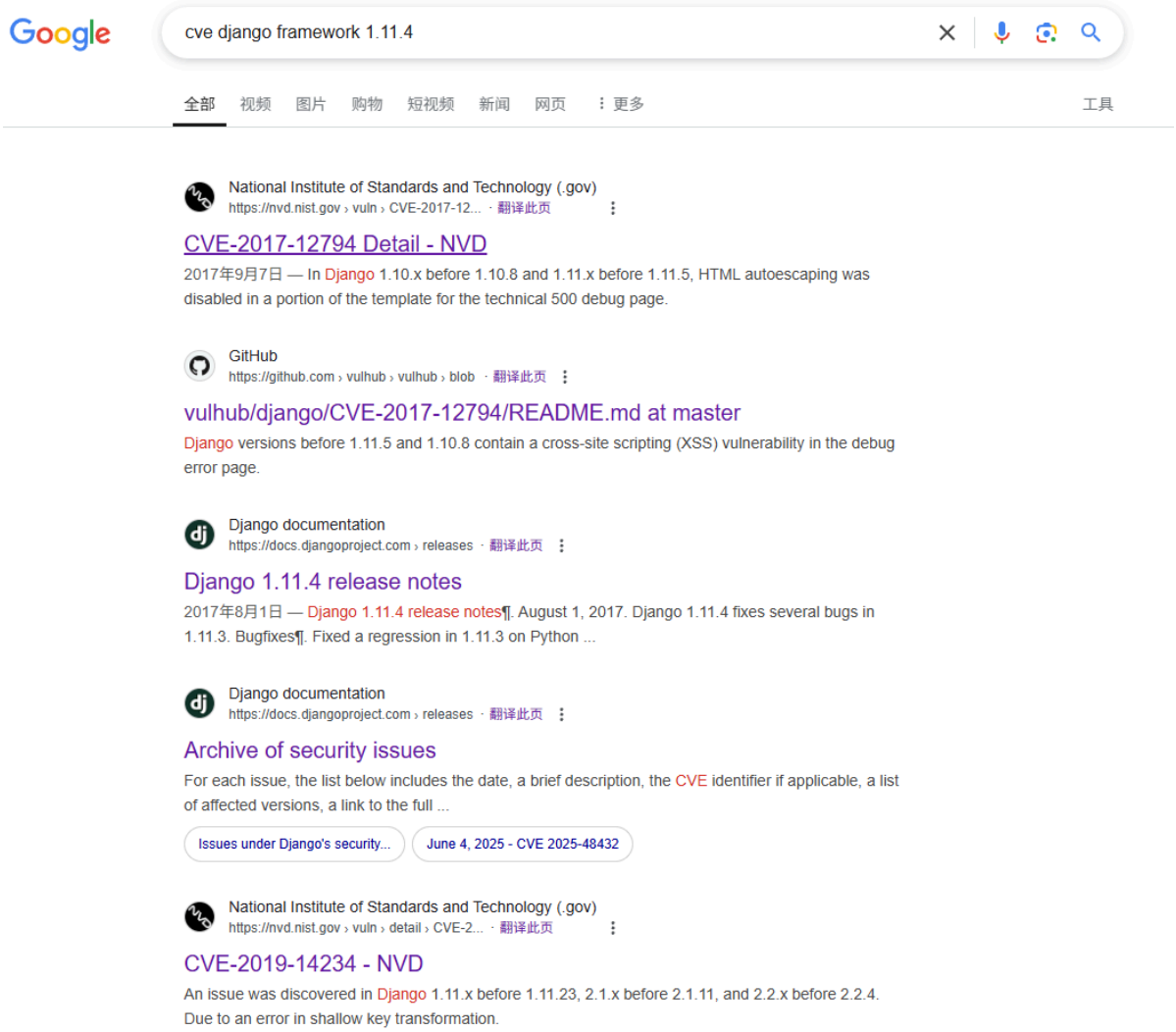
上图为信息收集阶段的最终总结部分，根据上述信息在线检索对应的CVE


Google
"Django 1.11.4" CVE
全部 购物 视频 图片 短视频 新闻 网页 更多 工具
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 ...
cpe:/a:djangoproject:django:1.11.4 ... CVE content is MITRE's CVE ...
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 — cpe:2.3:a:djangoproject:django:1.11.4:*:*:*:*:*:*:* Show Matching CPE(s). Denotes Vulnerable Software Are we missing a CPE here? Please let ...
CVE Details
https://www.cvedetails.com › version › Djan... · 翻译此页
Django Project Django 1.11.4 security vulnerabilities, CVEs
Django Project Django version 1.11.4 security vulnerabilities, CVEs, exploits, vulnerability ...
cpe:2.3:a:django_project:django:1.11.4 ... CVE content is MITRE's ...
National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › detail › change-record · 翻译此页
CVE-2017-12794 - NVD
National Vulnerability Database. Vulnerability Change Records for CVE-2017-12794. Change History ...
django:1.11.4:*:*:*:*:*:*:*. Changed, Reference ... https://www ...
Django documentation
https://docs.djangoproject.com › releases · 翻译此页
Django 1.11.5 release notes
2017年9月5日 — CVE-2017-12794: Possible XSS in traceback section of technical ... Next: Django 1.11.4 release notes · Table of contents · General Index ...

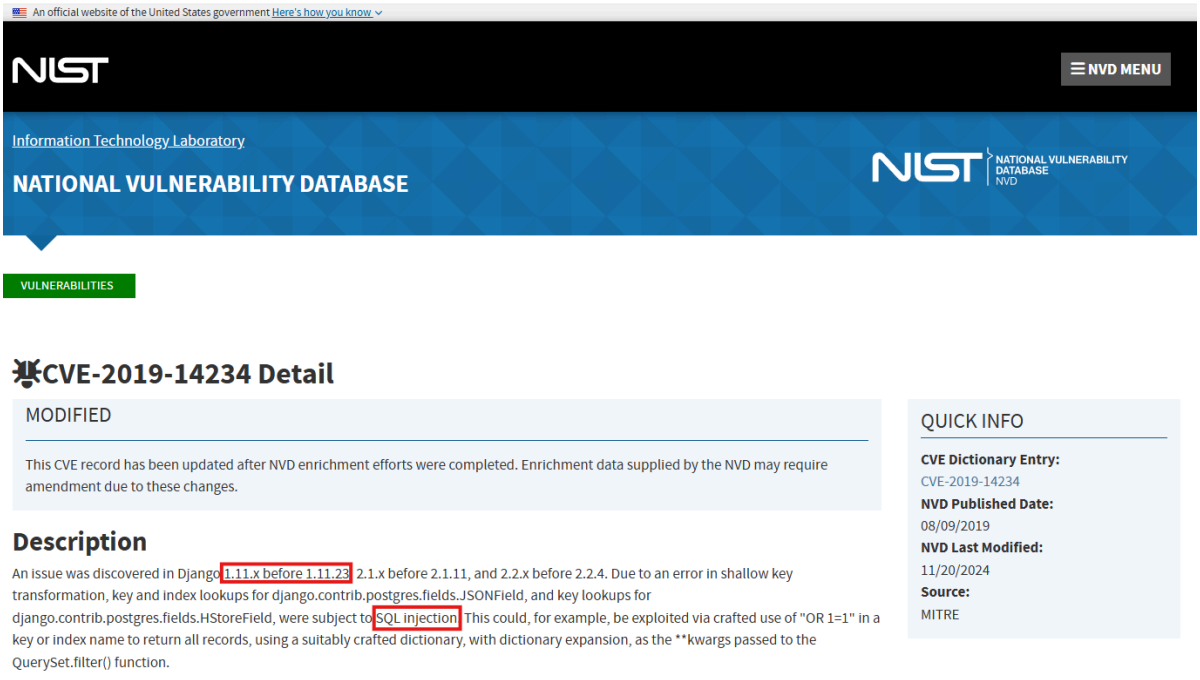
优先选择官方信息


https://nvd.nist.gov/vuln/detail/CVE-2017-12794
An official website of the United States government Here's how you know
NIST
NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES
CVE-2017-12794 Detail
DEFERRED
This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.
Description
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. Given the right circumstances, this allowed a cross-site scripting attack. This vulnerability shouldn't affect most production sites since you shouldn't run with "DEBUG = True" (which makes this page accessible) in your production settings.
QUICK INFO
CVE Dictionary Entry:
CVE-2017-12794
NVD Published Date:
09/07/2017
NVD Last Modified:
04/19/2025
Source:
MITRE
Metrics
CVSS Version 4.0
CVSS Version 3.x
CVSS Version 2.0
NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.
CVSS 3.x Severity and Vector Strings:
NIST: NVD
Base Score: 6.1 MEDIUM
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

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



构造其他检索词的检索结果如上所示，



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

Google cpe: cpe:2.3:a:djangoproject:django:1.11.4:*:*:*:*:*:*:* CVE

全部 购物 视频 短视频 图片 新闻 网页 更多 工具

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:djangoproject:django:1.10.0:*:*:*:*:*:*:* *cpe:2.3:a:djangoproject: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 ...