

Learn > TryHack3M: Bricks Heist

## TryHack3M: Bricks Heist

Crack the code, command the exploit! Dive into the heart of the system with just an RCE CVE as your key.

3 MILLION USERS

Easy 60 min

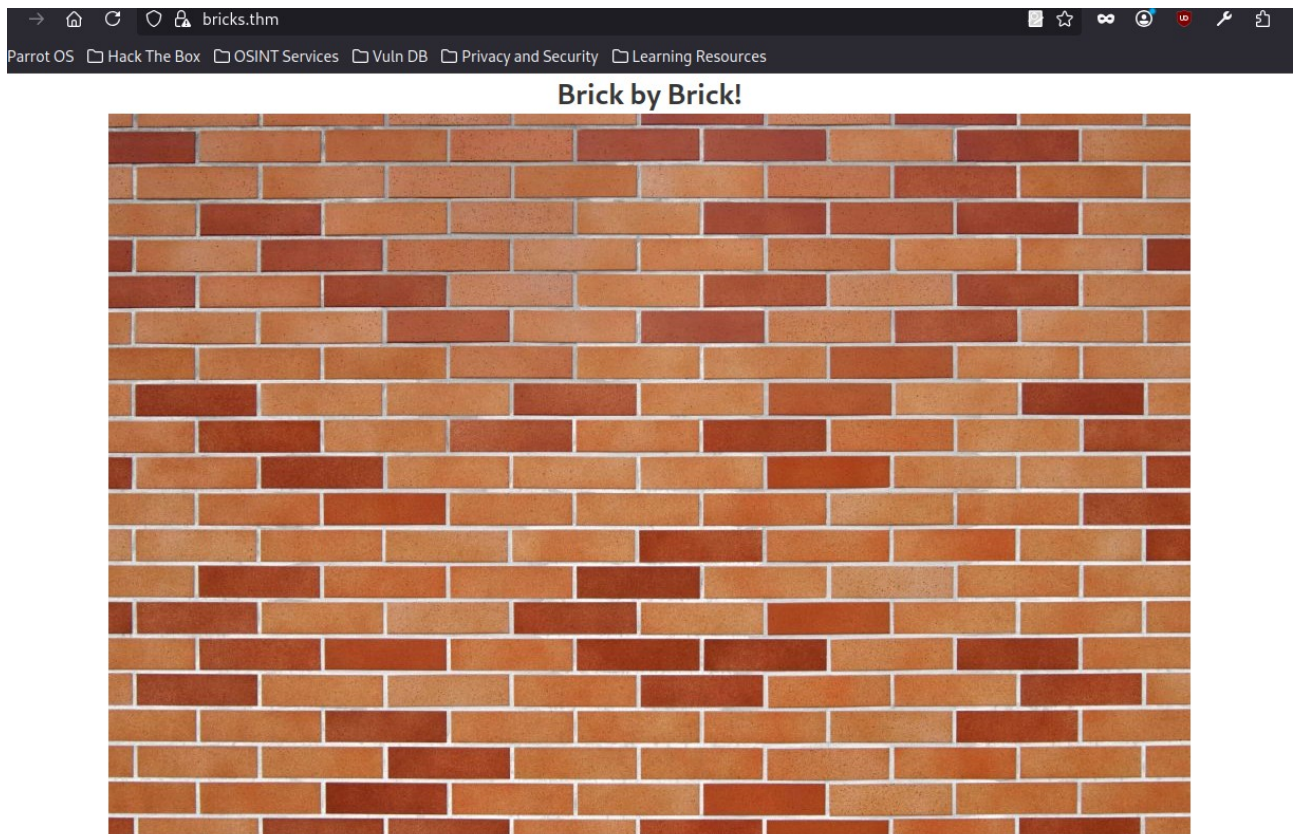
Share your achievement Start AttackBox Badge Help Save Room 655 Options

We start by adding the ip and host name to our hosts file

```
[x]-[parrot@parrot]-[~/tryhackme/3m bricks]
$ sudo nano /etc/hosts
[sudo] password for parrot:
[parrot@parrot]-[~/tryhackme/3m bricks]
$ sudo nano /etc/hosts
[parrot@parrot]-[~/tryhackme/3m bricks]
$
```

```
GNU nano 7.2
# Host addresses
127.0.0.1 localhost
127.0.1.1 parrot
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
# Others
10.10.188.222 bricks.thm
```

Next we navigate to the site:



The Site indicates that it is a wordpress site so we start with wpscan. We discover that it is running bricks 1.9.5 which is a vulnerable version. Searching in msfconsole for brick 1.9 yields an exploit. We run said exploit and get a meterpreter shell :).

What is the content of the hidden .txt file in the web folder?

THM{fl46\_650c844110baced87e1606453b93f22a}

To find the suspicious process I listed out all running processes using systemctl | grep running.

Find a service called ubuntu.service that's description is TRYHACKM3

What is the name of the suspicious process?

nm-inet-dialog

What is the service name affiliated with the suspicious process?

Ubuntu.service

What is the log file name of the miner instance?

Inet.conf

**What is the wallet address of the miner instance?**

**bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qa**

**The wallet address used has been involved in transactions between wallets belonging to which threat group?**

**LOCKBIT**