Reporter:
Dhananjay Porwal
dporwal214@gmail.com

Title:
While working with git on a project, I understand how Git and GitHub work and found a critical vulnerability in it. We can create fake commit using username and user-email. We can found user-email easily by GitHub API.

Description:
Using GitHub API (https://api.github.com/users/USERNAME/events/public) we get email address of any user and using both we can create fake commit. Performing this action won’t send any message/notification to genuine user.

Reproduction:

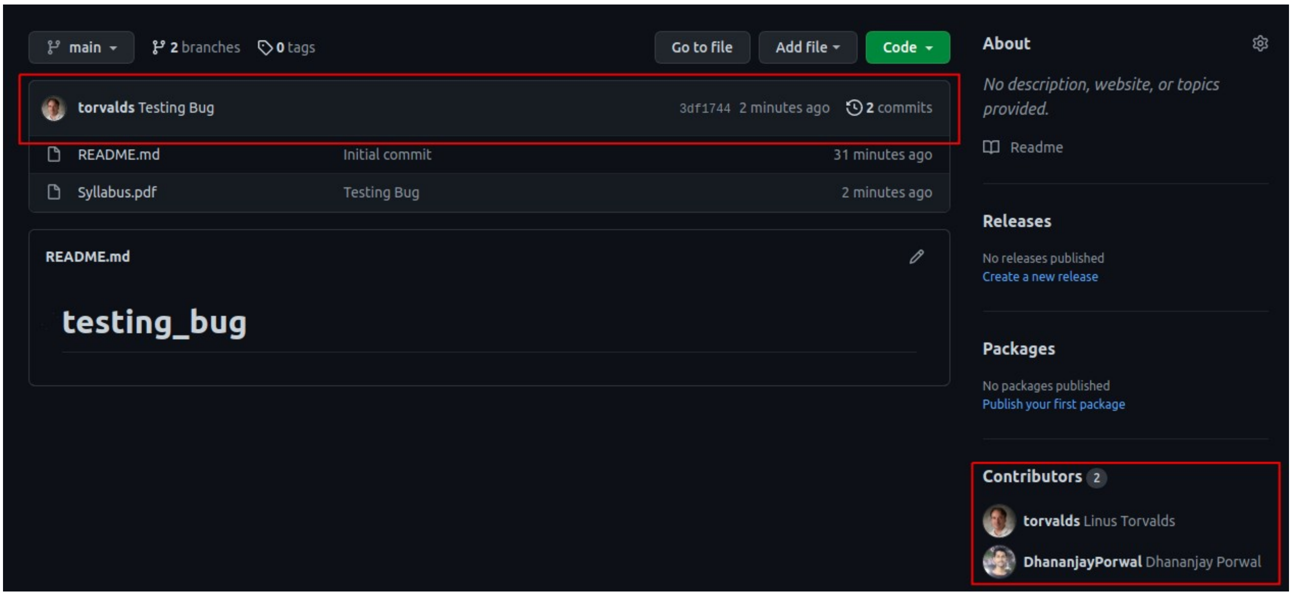
```
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report$ git clone
https://github.com/DhananjayPorwal/testing_bug.git
Cloning into &apos;testing_bug&apos;...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 6 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (6/6), 1.38 KiB | 706.00 KiB/s, done.
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report$ cd testing_bug/
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report/testing_bug$ ls
README.md
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report/testing_bug$ git
init
Reinitialized existing Git repository in
/home/dhananjay/Downloads/Vulnerability_Report/testing_bug/.git/
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report/testing_bug$ git
status
On branch main
Your branch is up to date with &apos;origin/main&apos;.

Untracked files:
  (use "git add <file>..." to include in what will be committed)
        Syllabus.pdf

nothing added to commit but untracked files present (use "git add" to track)
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report/testing_bug$ git
add .
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report/testing_bug$ git -c
user.name=&apos;Linus Torvalds&apos; -c user.email=&apos;torvalds@linux-
foundation.org&apos; commit -m "Testing Bug"
[main 3df1744] Testing Bug
 1 file changed, 0 insertions(+), 0 deletions(-)
 create mode 100644 Syllabus.pdf
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report/testing_bug$ git
pull
Already up to date.
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report/testing_bug$ git
push
Username for &apos;https://github.com&apos;: DhananjayPorwal
Password for &apos;https://DhananjayPorwal@github.com&apos;:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (3/3), done.
```

```
Writing objects: 100% (3/3), 284.88 KiB | 14.99 MiB/s, done.
Total 3 (delta 0), reused 0 (delta 0)
To https://github.com/DhananjayPorwal/testing_bug.git
   2f34553..3df1744  main -> main
dhananjay@dhananjay-desktop:~/Downloads/Vulnerability_Report/testing_bug$
```

Result:
I created fake commit by Linux Torvalds' name without their knowledge.



torvalds Testing Bug 3df1744 2 minutes ago 2 commits

README.md Initial commit 31 minutes ago

Syllabus.pdf Testing Bug 2 minutes ago

README.md

testing_bug

No description, website, or topics provided.

Readme

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Contributors 2

torvalds Linus Torvalds

DhananjayPorwal Dhananjay Porwal

Impact:
Anyone can commit with the username of any user without their knowledge, leads to fraud commits in projects which decreases the quality of open-source projects.

Recommendation:
For commiting any commit in Git user must required username, user-email, PAT everytime.

Reference :
https://github.com/DhananjayPorwal/testing_bug