

Forum:[Hack Forums](#)

Thread: [Commit-based Github URLs - Security recommendation](#)

Hackers - October 6, 2025, 9:33 am

My recommendation:

- > Require vendors (or ALL users) to use commit based links when sharing repos
- > Require codebase reviews or vouches to include the reviewed commit by auditors (quote it, or manually include a new link if OP has not included it)

This creates accountability, lowers the risk of future malware changes (intentional by an OP, or unintentional w/ a hacked Git account, etc).

With the popularity of attacks on devs, it's very easy for someone to share a Git repo that has malicious auto-run commands, build steps, or other sneaky malware embedded.

However, there's a way to make this a lot easier and safer for every user on HF now & in the future... Commit hash verification.

When someone shares a repo, they can share the public, dynamic URL
ex: github.com/ username-here / repo-name-here

There are also ways to share a specific branch.

However, neither the branch URL or main repo URL are "safe".
If I share a repo today with that URL, you could say "this is safe" in a thread, and I could modify it tomorrow to be malicious.

If we get into the habit of commit hash URLs, it's a lot easier to audit AND guarantee the security & safety in the future.

By using the /tree/ syntax in the URL, I can share an immutable version of the repo that is connected to this very specific hash:
Code github.com/ username /files/tree/ 47d5ff4e6f18a975ba4bb12383222ccfc4ef0f /random
Even a commit hash can link to a single file or folder! There's no downside.

If anyone audits my repo, they could say that the repo (as of the last hash '47d5ff4e6f18a975ba4bb12383222ccfc4ef0f') is safe.
In the future, other users can make sure they are on the right hash tree to stay safe.
This would prevent me from being able to modify my repo to include malware, tricking future users after HF staff or members have given a repo the thumbs up.

Simply put, without commit based URLs, or without users intentionally finding the commits and including them in their vouches, there's no great way for future downloaders to be protected.
How can a future user know if a repo is safe? With the commit hash included in vouches.

Tyr - *October 14, 2025, 8:15 pm*

Dynamic repo links age badly; pinned SHAs are auditable and immutable. I'd suggest turning your recommendation into a lightweight policy + checklist readably available online. Not only that but congested reviews and vouches to a specific commit hash, you make safety verifiable forever. Anyone can re-check that same commit later and confirm they're on the exact code that was previously reviewed — not a modified or malicious version.

You got my brain sparked up though. Very interesting.