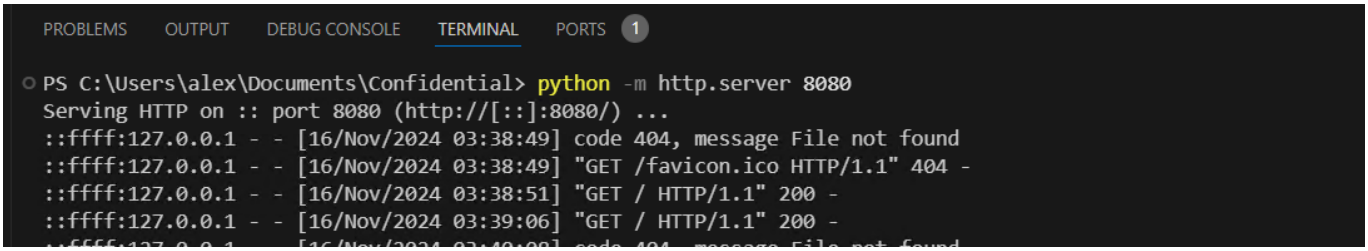
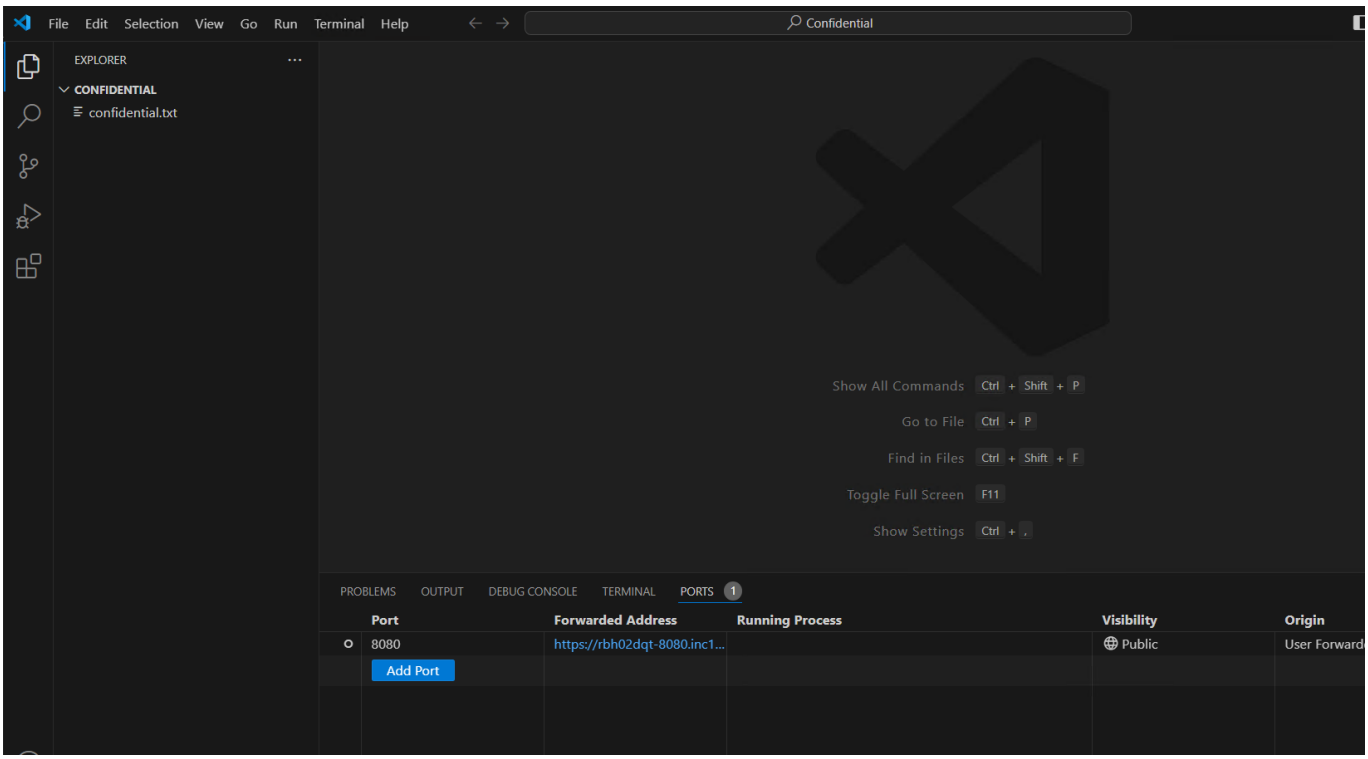
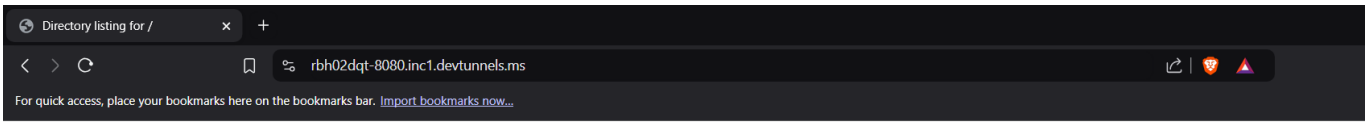
VS Code Feature Abuse For Exfiltration

We use vscode portforwarding feature to exfiltrate data from the compromised machine.

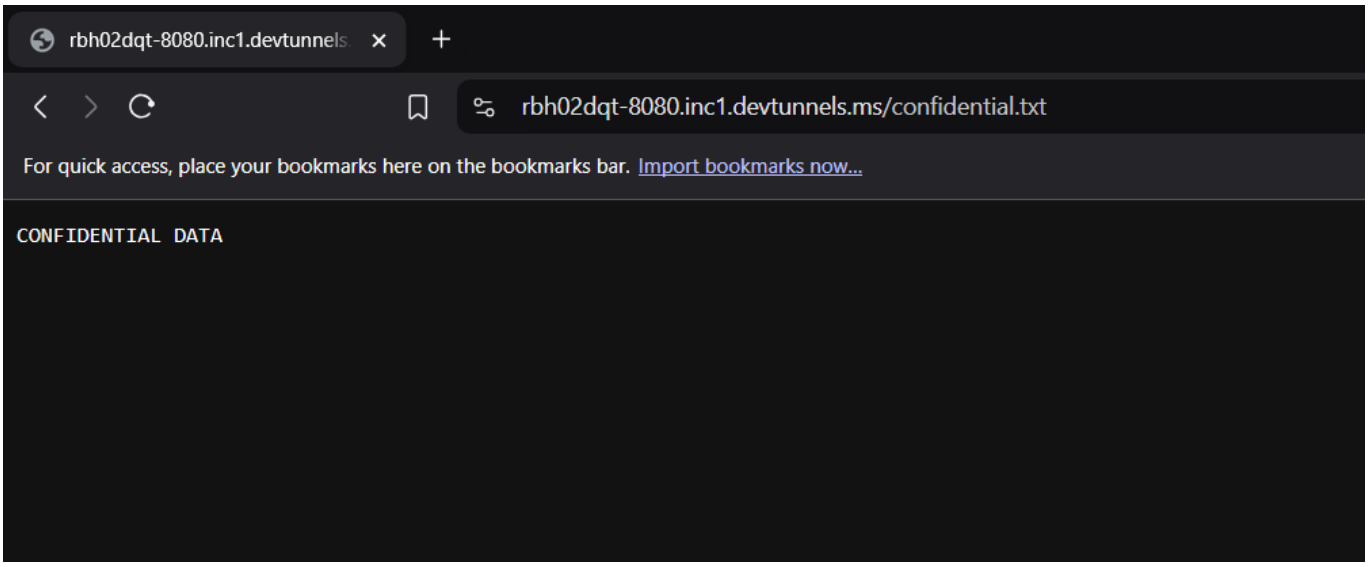






Directory listing for /

- confidential.txt


rbh02dqt-8080.inc1.devtunnels
rbh02dqt-8080.inc1.devtunnels.ms/confidential.txt
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
CONFIDENTIAL DATA