COMP435 In-Class Problems 10/8/25 Name: _____

Question 1: Confused Deputy Example A company builds a desktop chat app using **Electron**. Electron bundles a browser engine (Chromium) and Node.js so the app can run JavaScript that also reads and writes local files.

The developers add this code to let web content save chat logs:

```
// preload.js (runs with Node privileges)
const { writeFile } = require("fs");
window.saveLog = (filename, text) => {
 writeFile(filename, text, () => console.log("saved!"));
};
```

Then, any web page loaded inside the app can call:

```
  saveLog("/home/user/Desktop/log.txt", chatHistory);
```

1.1. Who is the deputy and who is the attacker in this case?

1.2. How does ambient authority play a role here?

1.3. Give one example (one code snippet) of how a malicious chat message or website could exploit this.

1.4. Suggest one change to the design that would prevent this problem.