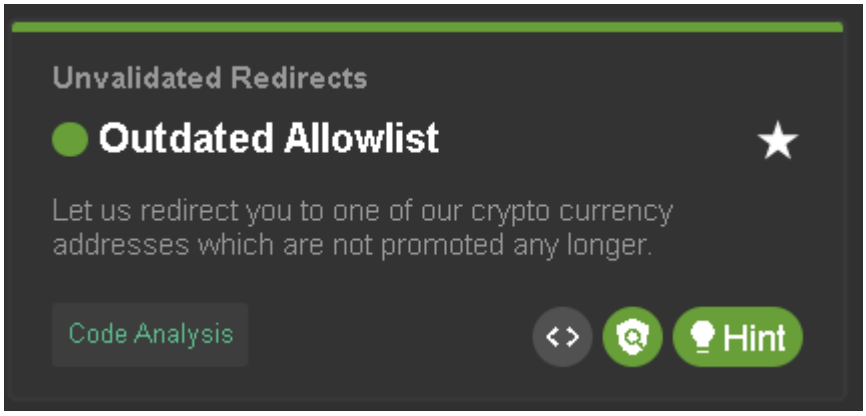
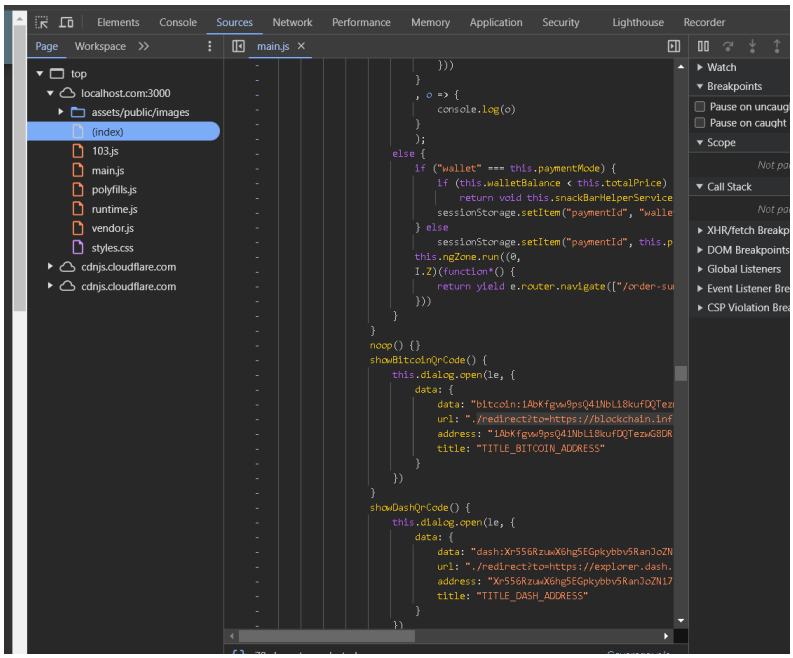
Unvalidated Redirects in OWASP Juice Shop



The objective is to exploit an outdated allowlist in the application's redirection mechanism to access deprecated cryptocurrency donation addresses.

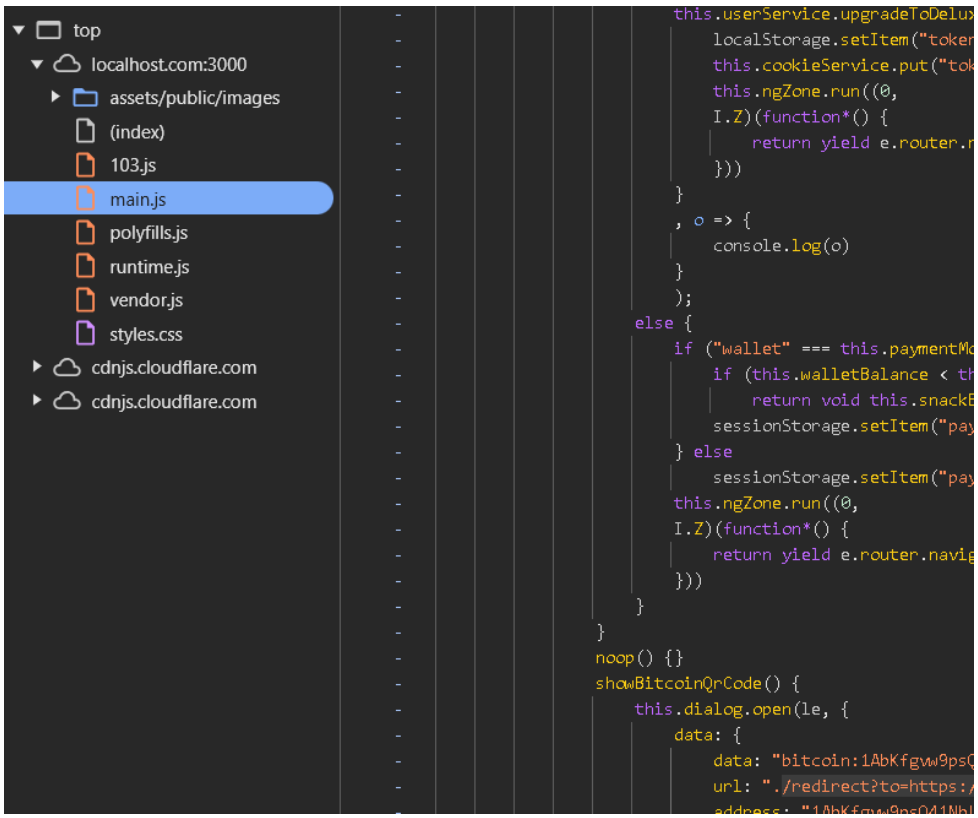
In the owasp juice shop page,
Go to developer tools by clicking inspect

Navigate to the "Sources" tab to view the site's source files.



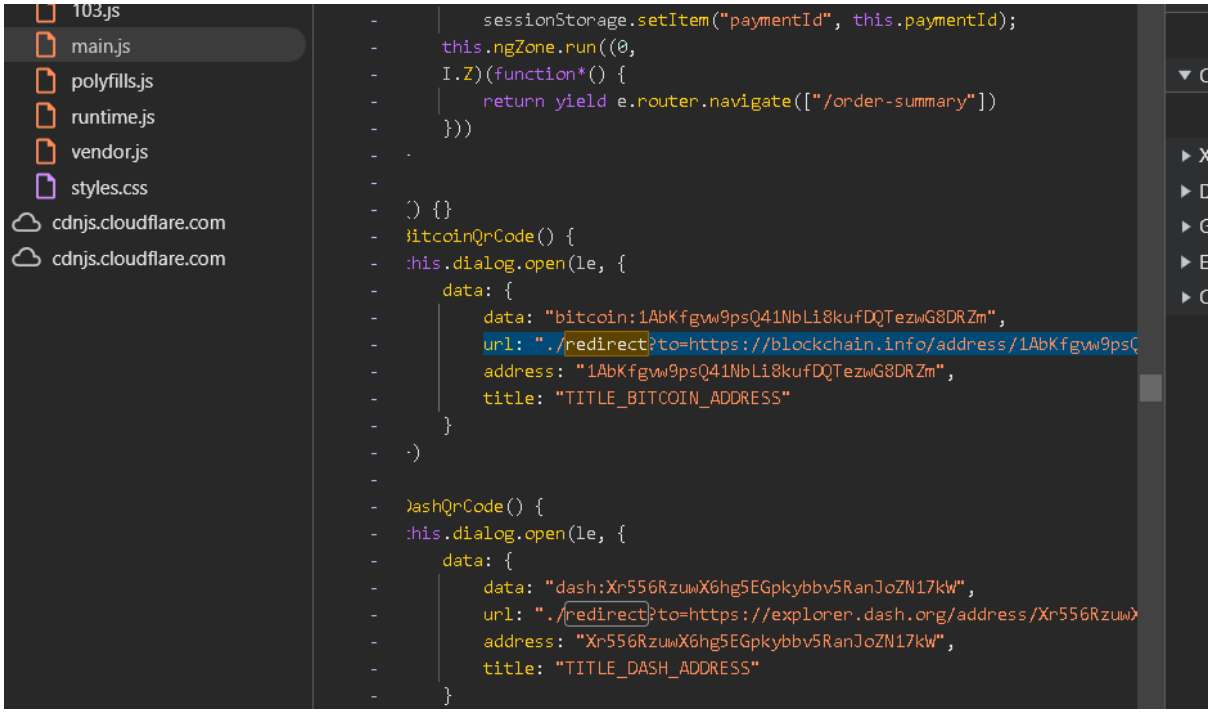
Locate the main.js File:

- In the "Sources" panel, expand the file structure to locate main.js.



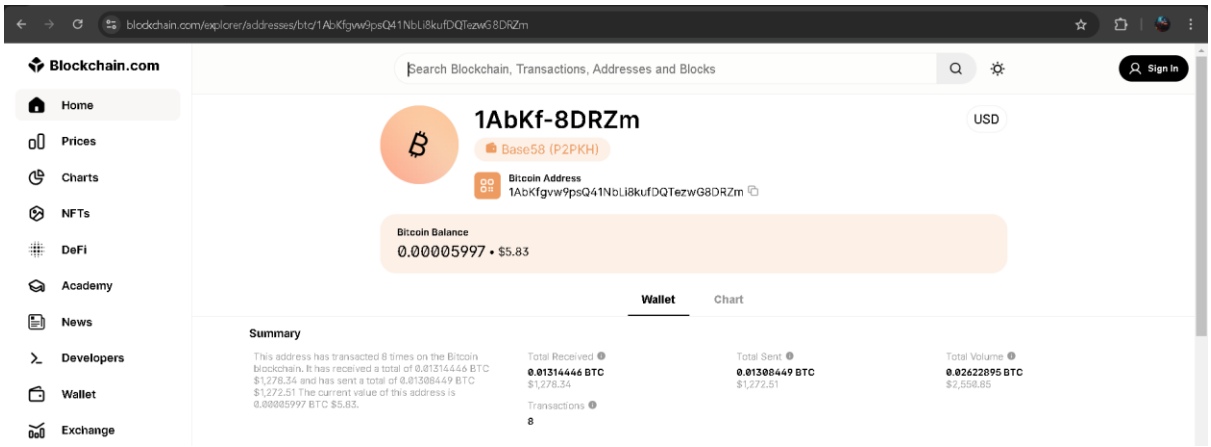
Search for Redirection Functions:

With main.js open, press Ctrl+F
Enter the keyword redirect to find functions related to redirection.
Scroll through the search results to locate lines that reference cryptocurrency addresses.



Paste the link with the url of owasp juice shop page like

“https://localhost.com:3000/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm”



Here we found the outdated link which redirects to the bitcoin page

Preventive Measures:

To prevent such vulnerabilities:

- **Regularly Update and Validate Allowlists:** Ensure that allowlists are current and free from obsolete entries.
- **Avoid Hard-Coding URLs:** Use dynamic retrieval methods for URLs to prevent outdated references.
- **Conduct Thorough Code Reviews:** Regularly review and test code to identify and remove unused or obsolete segments.