Browser Extension Security Audit Report

Date: November 2, 2025
Task: Browser Extension Security Review
Prepared By: Gautham

Executive Summary

I conducted a thorough review of all installed browser extensions in Google Chrome. The purpose of this audit was to ensure that no malicious, unused, or suspicious extensions were present that could compromise browser security or user privacy.

Audit Process

1. Reviewed all installed extensions via chrome://extensions
2. Checked each extension’s developer, permissions, and reviews in the Chrome Web Store
3. Verified that all extensions were essential for daily use
4. Ensured that no extensions requested unnecessary permissions
5. Cross-checked with online security sources for known malicious extensions

Findings

No unused, suspicious, or malicious extensions were found. All installed extensions are from trusted developers and have appropriate permissions for their intended functions. Examples of installed extensions include reputable tools for productivity and security verification.

Conclusion

The audit confirms that the browser environment is secure, with no harmful extensions detected. This result indicates adherence to good cybersecurity hygiene practices. Regular periodic audits are recommended to maintain continued browser security.

Sample Report Statement (For Documentation)

"I reviewed all installed extensions in Google Chrome. I checked each extension’s permissions, developer, and reviews on the web store. No unused, suspicious, or malicious extensions were found. All installed extensions are from trusted developers and have permissions that are appropriate for their function."

Learning Outcome

This exercise helped in understanding the importance of proactive extension audits in cybersecurity. It reinforces the habit of maintaining a minimal, trusted extension list and reviewing browser security regularly.