BUG REPORT: MIXED CONTENT WARNING AFTER WEBSITE MIGRATION AND SSL UPDATE

Reported By: Piyush Vaishnav
Environment:

- **CMS:** WordPress 6.8.1
- **Theme:** Astra Pro
- **Plugins:** WP Rocket, Elementor, Spectra, Ultimate Addons, AIOS, and 10 others
- **Server Environment:** NGINX + PHP 8.1
- **Browser Tested:** Chrome (v.141), Edge, Firefox
- **Hosting:** SiteGround (Production)

1. Issue Summary

After migrating the client's WordPress website from GoDaddy to SiteGround and installing a new SSL certificate, the site began showing **mixed content warnings** in the browser console, and a few images were broken. Despite SSL being configured correctly at the server and CDN level, several resources (mainly images, scripts, and stylesheets) continued loading over HTTP instead of HTTPS.
This issue affects both the **front-end user experience** and **site security**, as modern browsers mark the connection as "Not Fully Secure."

2. Steps to Reproduce

1. Navigate to the migrated domain: https://clientdomain.com
2. Open the **browser console** (Ctrl + Shift + I → Console tab).
3. Observe multiple warning messages.
4. Mixed Content: The page at 'https://clientdomain.com/' was loaded over HTTPS,
5. but requested an insecure image 'http://clientdomain.com/wp-content/uploads/2025/10/banner.jpg'.
6. This content should also be served over HTTPS.
7. Inspect affected elements (usually images, scripts, or iframes).
8. Confirm the source URLs still use http:// references in database or theme files.

3. Expected Behavior

All assets, including media files, scripts, and stylesheets should load over HTTPS once SSL is active and WordPress and site URLs are updated accordingly.
The browser should show a **secure padlock** without mixed content warnings.

4. Actual Behavior

Even after setting Site Address (URL) and WordPress Address (URL) to HTTPS in **Settings → General**, and updating the database URLs, certain resources continue to load via HTTP due to hard-coded links in:

- Page builder widgets (Elementor image and button links)
- Theme or plugin inline CSS references
- Cached resources served by WP Rocket before re-generation

5. Technical Findings

- Ran a search using the **Better Search Replace** plugin revealed several HTTP URLs embedded in Elementor post meta.
- The **browser console** identified insecure assets primarily from /wp-content/uploads/ and inline <style> elements.
- Some inline CSS references were generated dynamically by plugins that store asset URLs before migration.

6. Steps Taken to Fix

1. Performed full database search and replace:
   http://clientdomain.com → https://clientdomain.com
2. Cleared all the cache (WP Rocket, browser, CDN, and hosting cache).
3. Regenerated CSS files from Elementor → Tools → Regenerate CSS & Data.
4. Replaced old media links in the Media Library using **Update URLs**.
5. Verified that .htaccess included proper HTTP → HTTPS redirection rules.
6. Re-checked console: no mixed content warnings remained.

7. Resolution Status

✅ **Resolved.**
After performing a complete database URL replacement and cache purge, all resources now load securely via HTTPS. SSL padlock is active, and Google Chrome's DevTools show no mixed content warnings.

8. Recommendations

- Always perform URL replacement after any migration or SSL change.
- Clear all the caches post-migration.
- Use relative URLs in Elementor or custom fields when possible.
- Add post-deployment checks for SSL and mixed content using tools like **WhyNoPadlock**, **SSL Labs**, or browser console audits.