Security Vulnerability Report

Web Cache Poisoning Vulnerability Report

Vulnerable Domain: https://www.nwbbank.com

🔍 Description

A **Web Cache Poisoning** vulnerability was identified on the nwbbank.com domain. This vulnerability arises from improper handling of user-controlled headers by caching mechanisms, allowing an attacker to inject malicious headers and poison the cache.

Web Cache Poisoning occurs when an attacker manipulates cacheable content to serve malicious or unintended content to other users, potentially leading to phishing, redirection, or malware distribution.

📌 Technical Impact

Successful exploitation may:

- Redirect users to malicious domains (phishing or malware).
- Damage brand trust due to altered behavior.
- Allow attackers to craft deceptive URLs with harmful payloads.

🛠️ Remediation Recommendations

- Implement strict **cache-control** headers to avoid caching untrusted user inputs.
- Avoid reflecting user-supplied headers like Host, X-Forwarded-Host, etc., in cached responses.
- Validate and sanitize all incoming headers before using them in responses.
- Ensure that downstream caches (e.g., CDNs or proxies) respect header-based restrictions.

✅ Disclosure Status

- Vulnerability responsibly reported.
- Awaiting response from the vendor. *(Update this as necessary.)*