Security Assessment Report: www.google.com

Executive Summary

This automated assessment identified a total of 3 potential vulnerabilities. The findings include 0 Critical-risk, 2 High-risk, and 1 Medium-risk issues. Immediate attention is required to address all Critical and High-risk vulnerabilities to mitigate potential impact.

Detailed Findings & Remediation

Finding: FTP Service (21/tcp) Exposed

Risk Level: High
Summary: The File Transfer Protocol (FTP) is an unencrypted protocol susceptible to credential theft and unauthorized file access.
Recommended Action: If FTP is not essential for business operations, disable the service immediately. If required, restrict access to trusted IP addresses via firewall rules and enforce the use of SFTP (SSH File Transfer Protocol) with key-based authentication.

Finding: Unencrypted HTTP Service (80/tcp) Detected

Risk Level: Medium
Summary: The web server supports unencrypted HTTP, which can expose sensitive data in transit.
Recommended Action: Implement TLS/SSL to enforce HTTPS. Configure the web server to automatically redirect all HTTP requests to HTTPS.

Finding: Potential Cross-Site Scripting (XSS) Vulnerability

Risk Level: High
Summary: The application may be vulnerable to Cross-Site Scripting (XSS), allowing an attacker to execute malicious scripts in the browsers of other users.
Recommended Action: Implement context-aware output encoding for all user-supplied data before it is rendered on a page. Use a Content Security Policy (CSP) to restrict the sources from which scripts can be loaded.