SECURITY & VULNERABILITY AUDIT
HEALTH HORIZON AI

1. **OWASP ZAP Active Scan**
    a. This data indicates that the active scan attempted to discover files and directories that may not be part of the public structure or were non-existent, leading to 404 errors. There's no direct indication of vulnerabilities found in these initial requests, but the scan was likely part of a broader attempt to map out the application's structure and discover unlinked resources.
2. **OWASP ZAP Spider Scan**
    a. The spider scan successfully accessed the root of the application, along with common files like robots.txt, sitemap.xml, favicon.ico, and logo192.png. These files are public and provide metadata about the website structure and branding. The fact that these were the primary findings suggests that the spider was able to crawl the site without encountering significant hidden or unlinked content.
3. **Pentest Tools Vulnerability Scan**
    a. The website vulnerability scanner report for our global webpage indicates an overall low risk level with no high or medium risks identified. Key findings include:
        i. Missing Security Headers: The site lacks several important HTTP security headers.
        ii. Referrer-Policy: Absence of this header could lead to inadvertent information leakage and user tracking.
        iii. X-Content-Type-Options: Without this, the site might be vulnerable to MIME type sniffing attacks, particularly in Internet Explorer.
        iv. Content-Security-Policy: Lack of this header increases the risk of successful XSS attacks.
        v. These missing headers suggest potential areas for improvement in the site's security configuration.
        vi. Robots.txt File: While not a direct security risk, the presence of a robots.txt file was noted. It's important to ensure this file does not inadvertently disclose sensitive information about the site's structure.
        vii. Server Software and Technology: Information about the server software and technology used (like Google Analytics, Firebase, React, etc.) was detected, which could help an attacker in crafting targeted attacks.
        viii. General Observations: The report confirmed the website's accessibility and found no issues with server-side software vulnerabilities, client access policies, security.txt file presence, certificate trust, HTTP debug methods, secure communication, directory listing, cookie flags, or Content Security Policy.
4. **Protections Moving Forward**
    a. Based on the spider scan, active scan, and vulnerability scan reports, to enhance the safety and security of our application, we should focus on the following:
        i. Address Missing Security Headers: Implement the missing Referrer-Policy, X-Content-Type-Options, and Content-Security-Policy headers. These

headers help prevent user tracking, MIME type sniffing attacks, and Cross-Site Scripting (XSS) attacks respectively.

ii. Minimize Information Disclosure: Reduce the disclosure of server software and technology details in HTTP headers and error messages to prevent attackers from exploiting known vulnerabilities specific to those technologies.

iii. Regularly Scan for Vulnerabilities: Continuously monitor and scan our application for new vulnerabilities, ensuring that both the frontend and backend components are secure against common web threats.

iv. Fix Broken Links and Incorrect Configurations: The active scan showed several 404 errors; while these are not direct security issues, they indicate that there might be broken links or misconfigurations in our application which should be rectified.