**Vulnerability Assessment Report**

**Introduction:** The security of an organization's website is paramount in today's digital landscape. Vulnerabilities within web servers can expose sensitive data and compromise user trust. Recently, The Accountability Partners (TAP) underwent a comprehensive Nessus scan to identify potential vulnerabilities within its website infrastructure. The following report outlines the findings of this scan and provides recommendations for remediation.

**Vulnerabilities:**

1. **HSTS Missing From HTTPS Server (ID: 84502):**
   * This vulnerability indicates that the website's HTTP Strict Transport Security (HSTS) policy is not enabled.
   * Solution: Configure the remote web server to use HSTS to ensure a more secure connection.
2. **HTTP Methods Allowed (per directory) (ID: 43111):**
   * This finding suggests that certain directories on the website allow multiple HTTP methods, which could potentially lead to security issues.
   * Solution: Review and restrict the allowed HTTP methods in the affected directories to minimize security risks.
3. **HyperText Transfer Protocol (HTTP) Information (ID: 24260):**
   * This informational vulnerability provides details about the website's HTTP configuration.
   * Further analysis and action may be needed based on the specific HTTP information revealed.
4. **Nessus SYN scanner (ID: 11219):**
   * The Nessus SYN scanner detected during the scan suggests the presence of an IP filter to protect the target.
   * Solution: Ensure that the target is adequately protected with an IP filter to mitigate potential risks.
5. **Nessus Scan Information (ID: 19506):**
   * This finding provides general information about the Nessus scan conducted on the website.
   * Further review and consideration of the scan information may be necessary for comprehensive security assessment.
6. **Web Server No 404 Error Code Check (ID: 10386):**
   * This informational finding indicates that the website does not check for the presence of a 404 error code.
   * Additional measures may be required to enhance error handling and response mechanisms on the website.

**Conclusion:** While no critical, high, medium, or low-severity vulnerabilities were identified during the assessment, it is essential to address the informational findings to enhance the overall security posture of TAP's website. By implementing the recommended solutions and conducting further analysis as needed, TAP can strengthen its defenses and mitigate potential risks effectively. Regular vulnerability assessments and proactive security measures are crucial for maintaining a secure online environment.