VULNERABILITY REPORT

Project Name: MSB | **Dated:** Aug 07, 2025

Security Headers & Misconfigurations Report

1. Missing Security Header: `Strict-Transport-Security`

- **Where Missing:** Not present in API response headers.
- **Issue Summary:** Without this header, attackers may force users to use an insecure HTTP connection, risking exposure of sensitive info like cookies.
- **QA Recommendation:** Add the header:

```
“Strict-Transport-Security: max-age=31536000;
includeSubDomains”
```

---

2. Missing Security Header: `Referrer-Policy`

- **Where Missing:** Not in API response headers or `<meta name="referrer">` tag.
- **Issue Summary:** Browser sends full URL of visited pages (even if sensitive) to third parties via `Referer` header.
- **QA Recommendation:** Add the header:

```
Referrer-Policy: no-referrer
```

Prevents referer information leakage.

---

3. Missing Security Header: `Content-Security-Policy`

- **Where Missing:** Not present in API response headers or meta tag.
- **Issue Summary:** Without CSP, XSS attacks become easier if any JS injection vulnerability exists.
- **QA Recommendation:** Define and add a CSP header like:

```
Content-Security-Policy: default-src 'self'
```

Adjust sources based on application needs.

---

4. Missing Security Header: `X-Content-Type-Options`

- **Where Missing:** Absent from response headers.
- **Issue Summary:** Some browsers (esp. IE) may guess content type and allow execution of malicious files.
- **QA Recommendation:** Add this header:

```
X-Content-Type-Options: nosniff
```

---

5. Robots.txt File Found

- **Where Found:** Accessible at `/robots.txt`
- **Issue Summary:** While not a vulnerability, listing sensitive paths here can expose them to attackers.
- **QA Recommendation:** Review and remove any admin or sensitive paths from this file.

---

6. Server Technology Information Exposed

- **Where Found:** In response headers and meta tags.
- **Issue Summary:** Tech stack includes: IIS 10.0, ASP.NET, React, ModSecurity, etc. This fingerprinting helps attackers craft targeted attacks.
- **QA Recommendation:** Minimize info in HTTP headers (e.g., remove or obscure `Server, X-Powered-By)`.

---

7. HTTP OPTIONS Method Enabled

- **Where Found:** Server responded to OPTIONS with allowed methods: `OPTIONS, TRACE, GET, HEAD, POST`
- **Issue Summary:** Could expose debug or unsafe methods (e.g., TRACE), leading to potential info leaks.
- **QA Recommendation:** Disable unused HTTP methods via web server config.

---

8. Misconfiguration: Missing SRI Attributes

- **Where Found:** In external scripts and stylesheets in the HTML.

- **Issue Summary:** Without Subresource Integrity (SRI), a malicious third-party script could be injected and executed.
- **QA Recommendation:** For all external resources, add integrity and crossorigin attributes:

```
<script src="..." integrity="..."
crossorigin="anonymous"></script>
```