Configuration Alerts

Open Directory (opendir)

What is it

A web server misconfiguration that allows visitors to browse directory contents (e.g., `/files/`) instead of being restricted to specific web pages.

How is it detected

Nimbusec searches for file directory listing when visiting webpage.

Alert levels

YELLOW – Can expose sensitive files and aid in targeted attacks.

Recommended action

- Disable directory listing.
- Store sensitive files outside web-accessible directories.
- Conduct regular audits of file paths exposed to the internet.

PHP Error Display

What is it

When PHP error messages are displayed directly in the browser instead of being hidden and logged securely.

How is it detected

Nimbusec searches for php error message when visiting webpage.

Alert levels

YELLOW – Reveals internal system details (file paths, queries, API keys) that attackers can exploit.

Recommended action

- Disable `display_errors` in production environments.
- Log errors to a secure server or file instead of displaying them publicly.
- Implement custom error pages for users.
- Regularly review logs for abnormal or repeated errors.

Public Config

What is it

Apache status pages are checked for public access without authentication.

How is it detected

Nimbusec checks /server-info /server-status for public accessibility

Alert levels

YELLOW – Reveals internal system details, which can lead to different attack vectors.

Recommended action

- Apply “private by default” permissions to all storage resources.
- Use encryption and authentication for all sensitive files.
- Enable monitoring for unauthorized public access changes.

Security Header Config

What is it

Missing or misconfigured HTTP response headers that strengthen browser-level protections against attacks.

Occures when SHR grade is lower than "**D**".

How is it detected

Nimbusec calculates a grade from A to F for the Security Headers of scanned domains based on Mozilla Observatory.

Common headers include `CSP`, `HSTS`, `X-Frame-Options`, and `X-Content-Type-Options`.

Alert levels

- YELLOW – Increases exposure to XSS, clickjacking, and MITM attacks.

Recommended action

- Add and properly configure key security headers.
- Follow OWASP Secure Headers Project guidelines.
- Review headers after web server or app updates.

Revision #7
Created 2025-09-26 09:19:21 UTC by Lukas Tasch
Updated 2025-10-01 12:52:07 UTC by Lukas Tasch