Xerago SecureScan Report

Target URL: https://www.facebook.com/

Risk Level: HIGH

Summary:

Risk Level: HIGH

SQL Injection scan inconclusive

Missing Referrer-Policy header

Cookie fr missing HttpOnly flag

Cookie fr missing SameSite flag

Cookie sb missing HttpOnly flag

Cookie sb missing SameSite flag

CSP missing frame-ancestors directive (clickjacking risk)

Sensitive file exposed: /.env

Sensitive file exposed: /config.php

Sensitive file exposed: /.git

Sensitive file exposed: /backup.zip

Sensitive file exposed: /.htpasswd

Sensitive file exposed: /web.config

Sensitive file exposed: /wp-config.php

Sensitive file exposed: /.DS_Store

Sensitive file exposed: /.bash_history

Sensitive file exposed: /id_rsa

Potential admin panel exposed: /admin

Potential admin panel exposed: /login

Potential admin panel exposed: /administrator

Potentially exposed API endpoint: /api

Potentially exposed API endpoint: /graphql

CSP policy is weak (unsafe-inline or unsafe-eval present)

Backup file exposed: /index.php.bak

Backup file exposed: /backup.tar.gz

Backup file exposed: /db.sql

Backup file exposed: /site.old

Backup file exposed: /website.zip

Version control folder exposed: /.git/

Version control folder exposed: /.svn/

Findings & Recommendations:

- SQL Injection scan inconclusive

  Recommendation: Sanitize and parameterize all database queries.

- Missing Referrer-Policy header

  Recommendation: Add Referrer-Policy header.

- Cookie fr missing HttpOnly flag

  Recommendation: Set HttpOnly flag on all cookies.

- Cookie fr missing SameSite flag

  Recommendation: Set SameSite flag on all cookies.

- Cookie sb missing HttpOnly flag

  Recommendation: Set HttpOnly flag on all cookies.

- Cookie sb missing SameSite flag

  Recommendation: Set SameSite flag on all cookies.

- CSP missing frame-ancestors directive (clickjacking risk)

  Recommendation: Review this issue and apply best security practices.

- Sensitive file exposed: /.env

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /config.php

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /.git

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /backup.zip

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /.htpasswd

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /web.config

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /wp-config.php

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /.DS_Store

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /.bash_history

  Recommendation: Remove sensitive files from the web root.

- Sensitive file exposed: /id_rsa

  Recommendation: Remove sensitive files from the web root.

- Potential admin panel exposed: /admin

  Recommendation: Restrict access to admin panels and use strong authentication.

- Potential admin panel exposed: /login

  Recommendation: Restrict access to admin panels and use strong authentication.

- Potential admin panel exposed: /administrator

  Recommendation: Restrict access to admin panels and use strong authentication.

- Potentially exposed API endpoint: /api

  Recommendation: Review this issue and apply best security practices.

- Potentially exposed API endpoint: /graphql

  Recommendation: Review this issue and apply best security practices.

- CSP policy is weak (unsafe-inline or unsafe-eval present)

  Recommendation: Review this issue and apply best security practices.

- Backup file exposed: /index.php.bak

  Recommendation: Review this issue and apply best security practices.

- Backup file exposed: /backup.tar.gz

  Recommendation: Review this issue and apply best security practices.

- Backup file exposed: /db.sql

  Recommendation: Review this issue and apply best security practices.

- Backup file exposed: /site.old

  Recommendation: Review this issue and apply best security practices.

- Backup file exposed: /website.zip

  Recommendation: Review this issue and apply best security practices.

- Version control folder exposed: /.git/

  Recommendation: Review this issue and apply best security practices.

- Version control folder exposed: /.svn/

Recommendation: Review this issue and apply best security practices.