Vulnerability Report for https://www.facebook.com/

Target Host: www.facebook.com

Security Headers Check:

- **Content-Security-Policy**: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net 'unsafe-eval';script-src *.facebook.com *.fbcdn.net *.facebook.net *.google-analytics.com *.google.com 127.0.0.1:* 'unsafe-inline' blob: data: 'self' connect.facebook.net 'unsafe-eval';style-src fonts.googleapis.com *.fbcdn.net data: *.facebook.com 'unsafe-inline';connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com;font-src data: *.gstatic.com *.facebook.com *.fbcdn.net *.fbsbx.com;img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: googleads.g.doubleclick.net www.googleadservices.com *.whatsapp.net *.fb.com *.oculuscdn.com *.tenor.co *.tenor.com *.giphy.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com https://*.giphy.com;frame-src *.doubleclick.net *.google.com *.facebook.com www.googleadservices.com *.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net https://paywithmybank.com/ https://sandbox.paywithmybank.com/;worker-src blob: *.facebook.com data:;block-all-mixed-content;upgrade-insecure-requests;

- **Strict-Transport-Security**: max-age=15552000; preload

- **X-Frame-Options**: DENY

- **X-XSS-Protection**: 0

- **X-Content-Type-Options**: nosniff

- **Cross-Origin-Resource-Policy**: cross-origin

- **Cross-Origin-Opener-Policy**: unsafe-none;report-to="coop_report"

- **Cross-Origin-Embedder-Policy**: MISSING

- **Public-Key-Pins**: MISSING

- **Expect-CT**: MISSING

- **Feature-Policy**: MISSING

- **Referrer-Policy**: MISSING

- **X-Permitted-Cross-Domain-Policies**: MISSING

Security Header Issues:

- **Cross-Origin-Embedder-Policy** is missing.

Missing Cross-Origin-Embedder-Policy header can make the application vulnerable to Cross-Origin Embedder Policy (COEP) attacks, where an attacker can load the application as an embedder or a nested document in a malicious website.

- **Public-Key-Pins** is missing.

Missing Public-Key-Pins header can expose the application to Man-in-the-Middle (MitM) attacks by allowing attackers to impersonate the server using fraudulent certificates.

- **Expect-CT** is missing.

Missing Expect-CT header can expose the application to Certificate Transparency (CT) policy violations, allowing attackers to use fraudulent certificates without detection.

- **Feature-Policy** is missing.

Missing Feature-Policy header can expose the application to various risks associated with allowing or restricting specific browser features. It helps prevent unauthorized access to features like geolocation, microphone, and camera.

- **Referrer-Policy** is missing.

Missing Referrer-Policy header can leak sensitive information by sending referrer headers to external domains. It helps control how much information is included in the referrer header when navigating to external links.

- **X-Permitted-Cross-Domain-Policies** is missing.

Missing X-Permitted-Cross-Domain-Policies header can expose the application to Cross-Domain Policy (XDP) misconfigurations, allowing unauthorized access to resources from different domains.

Open Ports Check:

- **Port 80**: OPEN

HTTP (Hypertext Transfer Protocol) port is vulnerable to various attacks including cross-site scripting (XSS), SQL injection, cross-site request forgery (CSRF), and DDoS attacks.

- **Port 443**: OPEN

HTTPS (Hypertext Transfer Protocol Secure) port is vulnerable to various attacks including cross-site scripting (XSS), SQL injection, cross-site request forgery (CSRF), and DDoS attacks.