CyberSweep Scan Report

Generated on: 2025-07-17 22:38:37

Target URL

https://www.exploit-db.com/

Scan Timestamp

2025-07-17 22:37:36

Resolved IP

192.124.249.13

Response Headers

{'Date': 'Thu, 17 Jul 2025 17:07:38 GMT', 'Content-Type': 'text/html; charset=UTF-8', 'Content-Length': '17238', 'Connection': 'keep-alive', 'X-Sucuri-ID': '12013', 'Cache-Control': 'no-cache, private', 'Set-Cookie': 'exploit_database_session=eyJpdiI6IkxxaHMzWmhUWER4UmRYcXVsYllHcGc9PSIsInZhbHVlIjoiTUk1a090S0FOSzhhWDlFMXFrSnJnbE93ZEJOOUNGcFNYS2dmWFQ0dVJFTjJHSXpuSEpIUFNjRlFWZjQwdmlUYiIsIm1hYyI6ImRlZGNkMGZhYWNjNzVhNTIwODFhMGQ0YzlmYTdjYTAwMTFjMzliNWMzNDg3NzNiYThhY2UyMDIwZDQ1NTQzN2IifQ%3D%3D; expires=Thu, 17-Jul-2025 19:06:54 GMT; Max-Age=7200; path=/; secure; httponly', 'Vary': 'Accept-Encoding', 'Content-Encoding': 'gzip', 'X-Frame-Options': 'DENY', 'Referrer-Policy': 'same-origin', 'Server': 'Sucuri/Cloudproxy', 'X-Sucuri-Cache': 'HIT', 'Alt-Svc': 'h3=":443"; ma=2592000, h3-29=":443"; ma=2592000'}

Open Ports

Port 80/tcp is OPEN (Service: http, Product: Sucuri/Cloudproxy)

Port 443/tcp is OPEN (Service: https, Product: Sucuri/Cloudproxy)

Security Header Analysis

WARNING: Missing HSTS header. Should enforce HTTPS.

WARNING: Missing X-Content-Type-Options header. Should be 'nosniff'.

WARNING: Missing Content-Security-Policy (CSP) header. Provides defense against XSS and data injection attacks.

WARNING: Missing Permissions-Policy header. Controls browser features and APIs for the page.

XSS Scan Findings

No query parameters found for XSS injection (skipped).

Directory & File Discovery

Forbidden/Unauthorized: https://www.exploit-db.com/phpmyadmin/ (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/.env (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/wp-config.php.bak (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/config.php.bak (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/index.php.bak (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/admin/ (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/server-status (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/index.bak (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/.git/HEAD (Status: 403)

Found: https://www.exploit-db.com/sitemap.xml (Status: 200)

Forbidden/Unauthorized: https://www.exploit-db.com/.htaccess (Status: 403)

Forbidden/Unauthorized: https://www.exploit-db.com/wp-admin/ (Status: 403)

Found: https://www.exploit-db.com/robots.txt (Status: 200)

Vulnerability Scan

Browser opened to https://www.exploit-db.com/. Manual interception required in Burp Suite (configured on 127.0.0.1:8080).

Stealth Network Scan Results

No active hosts found on the specified local network range (basic ARP scan).

Database Access Attempts

No common database ports found open. Skipping deeper database access attempts.

Discovered URLs (Crawl)

https://www.exploit-db.com/

Sensitive Data Findings (Crawl)

No sensitive data patterns found in crawled pages (basic check).