=== SECURESCAN Report ===
Target: http://testphp.vulnweb.com
Generated: 2025-11-14T17:57:34.248237

=== Quick Risk Meter ===
Score: 100 Classification: Critical

=== WHY (short) ===
 - SITE USES HTTP (not HTTPS) — traffic is unencrypted.
 - Missing security headers (CSP/HSTS/X-Frame/X-Content-Type/etc).
 - Reflected parameters / error messages detected — possible injection/XSS or error-based issues.
 - TLS handshake failed or site not using HTTPS.

=== Server Headers ===
Server: nginx/1.19.0
Date: Fri, 14 Nov 2025 12:26:57 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip

=== Security Headers Check ===
X-Frame-Options: Missing - Helps prevent clickjacking
X-XSS-Protection: Missing - Protects against XSS
Content-Security-Policy: Missing - Prevents script injection
Strict-Transport-Security: Missing - Forces HTTPS
X-Content-Type-Options: Missing - Prevents MIME-sniffing
Referrer-Policy: Missing - Controls referrer header information

=== Discovered Paths ===

=== Crawled URLs ===
http://testphp.vulnweb.com

=== Parameter Map ===
http://testphp.vulnweb.com | query_params: - | form_inputs: goButton,searchFor

=== Auto Scan (safe checks) ===
PAGE: http://testphp.vulnweb.com
  - SQLi Indicator: http://testphp.vulnweb.com?goButton='%20OR%20'1'='1'%20--%20 | payload: ' OR '1'='1'
  - SQLi Indicator: http://testphp.vulnweb.com?goButton=%22%20OR%20%221%22=%221%22%20--%20 |
  - Reflected Payload Found: http://testphp.vulnweb.com?searchFor=%3Cscr1pt%3Ealert(1)%3C/scr1pt%3E
  - Reflected Payload Found: http://testphp.vulnweb.com?searchFor=%22%3E%3Csvg/onload=alert(1)%3E
  - SQLi Indicator: http://testphp.vulnweb.com?searchFor='%20OR%20'1'='1'%20--%20 | payload: ' OR '1'='1
  - SQLi Indicator: http://testphp.vulnweb.com?searchFor=%22%20OR%20%221%22=%221%22%20--%20

=== Subdomains ===

=== TLS Info ===
TLS handshake failed or non-HTTPS.

=== Banners ===
Port 21: none
Port 22: none
Port 25: none
Port 80: none
Port 110: none
Port 143: none
Port 443: none

Port 465: none
Port 587: none
Port 8080: none
Port 8000: none

=== Suggestions ===
 - Add CSP, HSTS, X-Frame-Options, X-Content-Type-Options.
 - TLS missing or handshake failed.

=== Knowledge & Fixes (why + how to fix) ===
Missing CSP:
  Why: No Content-Security-Policy header allows browsers to execute inline scripts and mixed sources, incr
  Fix: Add a restrictive Content-Security-Policy header limiting script sources, e.g. `Content-Security-Policy:

Missing HSTS:
  Why: No Strict-Transport-Security header means browsers won't automatically enforce HTTPS, exposing u
  Fix: Enable HSTS: `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`.

Missing X-Frame-Options:
  Why: Without X-Frame-Options or CSP frame-ancestors, the site can be framed by other pages leading to
  Fix: Add `X-Frame-Options: DENY` or `SAMEORIGIN`, or use CSP `frame-ancestors`.

HTTP (not HTTPS):
  Why: Site is served over plain HTTP. Traffic is unencrypted and can be intercepted or modified (Man-in-the
  Fix: Obtain TLS certificate and serve over HTTPS. Redirect HTTP to HTTPS and enable HSTS.

Open Ports:
  Why: Exposed services on common ports can increase attack surface and run vulnerable services.
  Fix: Close unused ports, firewall restrict access, and ensure services are patched and configured securely

Reflected Payload Found:
  Why: A payload you sent was reflected back in the response. If that reflection is not safely encoded, it may
  Fix: Validate and encode user-supplied data before rendering; use proper output encoding and CSP.

Tech With CVEs:
  Why: Server technology/version fingerprint matched known CVEs in local DB; unpatched software may be
  Fix: Patch/update the software to a fixed version and follow vendor advisories.

=== End of Report ===