FICTIONAL PREVIEW - NO LIVE WEBSITE WAS ASSESSED

STAGE 1 / A FIRST LOOK AT YOUR WEBSITE

example.com

03 Nov 2026, 12:00 UTC

1 configuration item(s) deserve a closer look. These are review prompts, not confirmed exploitable vulnerabilities.

4	5	1	0
Passed	Observed	Review	Not assessed

What this tells you

Passed means a specific limited configuration condition was met. Observed means a policy was present; effectiveness was not assessed. Review is a configuration improvement prompt. None of these outcomes proves the application is secure.

The exact scope

A configuration baseline of one unauthenticated HTTPS HEAD response at /. No redirects followed. A HEAD response may differ from GET. This is not a penetration test or proof that a website is secure.

Your next useful step

- Content Security Policy presence: Review a restrictive CSP against the application's real scripts and resources; header presence does not establish XSS protection.

Talk to TGG before committing

Discuss website security or AI protection with our team. You can speak first or verify domain control first. We agree the scope and fee, you approve it, and only then do we issue a crypto invoice. Work starts after confirmed payment and current DNS verification.

tobias@tgg.group | https://tgg.group/contact

Reference: FICTIONAL-PREVIEW

Configuration observations

01 HTTPS certificate validation

Passed / info

A trusted certificate matching this hostname was validated using TLSv1.3.

Next step: Keep certificate renewal monitored; this does not test every TLS protocol or cipher.

02 Certificate renewal window

Passed / info

Certificate expires on 2027-01-25.

Next step: Ensure automated renewal succeeds before this date.

03 HTTPS enforcement policy

Passed / info

One HSTS header with a positive max-age was observed.

Next step: Keep HSTS enabled with a suitable max-age; include subdomains only after confirming HTTPS compatibility.

04 Content Security Policy presence

Review / low

A single enforcing CSP header was not observed.

Next step: Review a restrictive CSP against the application's real scripts and resources; header presence does not establish XSS protection.

05 Framing policy signal

Observed / info

One recognized X-Frame-Options value was observed.

Next step: Review CSP frame-ancestors and, where appropriate, X-Frame-Options for the intended embedding policy.

06 MIME sniffing policy

Passed / info

One nosniff directive was observed.

Next step: Keep nosniff enabled and serve correct Content-Type values.

07 Referrer policy presence

Observed / info

One Referrer-Policy header was observed; validity was not assessed.

Next step: Choose a referrer policy suitable for your privacy and navigation requirements.

08 Browser permissions policy

Observed / info

One Permissions-Policy header was observed; the allowed features were not evaluated.

Next step: Review which pages need camera, microphone, location and other browser features; restrict only features the application does not require.

09 Cross-origin resource policy

Observed / info

A recognized Cross-Origin-Resource-Policy value was observed: same-origin.

Next step: Review cross-origin resource sharing and isolation against real integrations. Header presence alone does not establish protection.

10 Cookie attribute snapshot

Observed / info

This HEAD response included 1 Set-Cookie header(s): 1 carried Secure, 1 HttpOnly and 1 a recognized SameSite value. Cookie names and values were not retained.

Next step: Review actual authentication cookies separately. Some application cookies intentionally need JavaScript access; this snapshot does not classify cookies or establish session security.

Outside this check

SQL injection, XSS, SSRF, authentication, authorization, business logic, other pages and subdomains, old TLS protocol support

This is a configuration baseline, not a penetration test, certification or guarantee of security. Email verification confirms mailbox access; it is not independent proof of domain ownership.