Scansione automatica eseguita da Tessera: 11 ottobre 2026 alle ore 11:10 (ora italiana). I risultati descrivono lo stato del sito in quel momento.

RISERVATO — non distribuire

Report Quick Check di sicurezza

Target	**https://www.negozio.example/**
HTTP status	**200**
ID report	**esempio**
Data e ora del test	**11 ottobre 2026 alle ore 11:10 (ora italiana)**
Preparato da	**Tessera Quick Check — piattaforma di scansione automatica (nessuna revisione umana)**



PUNTEGGIO DI SICUREZZA

Classe D · Da migliorare

Alto	0
Medio	4
Basso	6
Informativo	4

100 meno 25 punti per ogni problema Alto, 10 per ogni Medio e 3 per ogni Basso; gli informativi non contano. Con almeno un problema Alto il punteggio non supera 49, con almeno un Medio non supera 79.

Executive Summary

Livello di rischio complessivo: MEDIO

Il sito www.negozio.example non presenta vulnerabilità di severità alta. Sono emersi 4 problemi di severità media, tutti legati alla configurazione: mancano gli header che proteggono il browser (Content-Security-Policy, Strict-Transport-Security, protezione dal clickjacking) e il server accetta ancora i protocolli TLS 1.0 e 1.1. Sono interventi di configurazione del server, risolvibili in poche ore senza modifiche all'applicazione. I 6 problemi di severità bassa riguardano soprattutto hardening e informazioni esposte.

Sintesi generata da Claude (Anthropic) sulla base dei finding rilevati in questo scan.

Scala di severità

Alto
Problema direttamente sfruttabile con impatto serio (es. bypass di autenticazione, esposizione di dati, esecuzione di codice). Richiede intervento urgente.

Medio
Sfruttabile in condizioni specifiche, o una debolezza dei controlli che aumenta il rischio in modo significativo senza essere direttamente sfruttabile da sola. Da correggere nel breve termine.

Basso
Impatto pratico limitato da solo, tipicamente una lacuna di hardening o difesa in profondità. Da affrontare nella normale manutenzione.

Informativo
Osservazione senza impatto diretto sulla sicurezza, inclusa per completezza o consapevolezza.

Scope e regole di ingaggio

Target testato: https://www.negozio.example/. Tipo di test: black-box, dall'esterno, senza credenziali (nessuna sessione utente autenticata è stata usata in questo scan). Base di autorizzazione: il controllo del dominio www.negozio.example è stato verificato da Tessera tramite record DNS TXT pubblicato dal cliente; ultima verifica: 11 ottobre 2026 alle ore 10:55 (ora italiana). L'utente ha inoltre dichiarato in interfaccia di essere autorizzato al test. Non sostituisce una lettera di autorizzazione firmata dal titolare del sito.

Compreso nel test:

- Superficie pubblica del sito raggiungibile dall'URL indicato (pagine, asset statici, endpoint scoperti dallo spider di ZAP)
- Header di sicurezza HTTP e configurazione TLS/HTTPS
- Ricerca di vulnerabilità note, misconfigurazioni e credenziali di default (Nuclei)
- Vulnerabilità applicative rilevabili passivamente e con probe attivi automatizzati (ZAP)

Escluso dal test:

- Aree autenticate o che richiedono un account utente
- Codice sorgente dell'applicazione
- Infrastruttura cloud sottostante oltre a quanto esposto pubblicamente
- Social engineering, test fisici, denial-of-service

Metodologia

Questo Quick Check combina controlli passivi e attivi eseguiti automaticamente: verifica degli header di sicurezza HTTP, analisi della configurazione TLS (testssl.sh), ricerca di vulnerabilità note e misconfigurazioni tramite Nuclei, e scansione applicativa con OWASP ZAP (spider, passive scan e active scan). A differenza di un penetration test manuale, questo Quick Check non include revisione del codice sorgente né verifica mirata della logica di autorizzazione applicativa: individua i problemi rilevabili automaticamente dall'esterno, in una finestra di tempo limitata.

Standard e framework di riferimento

CVSS v3.1 (FIRST.org)

Punteggio di severità calcolato con la formula ufficiale pubblicata da FIRST, non stimato: per i finding Nuclei preso dai metadata del template quando presente, per i finding ZAP valutato secondo la metodologia ufficiale e dichiarato in chiaro (vettore + punteggio) in ogni finding. Il livello di rischio mostrato (Alto/Medio/Basso) deriva dal punteggio CVSS (Alto >= 7.0, Medio 4.0-6.9, Basso < 4.0), non dalla severità grezza dello strumento.

CWE — Common Weakness Enumeration (MITRE)

Ogni finding con impatto di sicurezza è classificato secondo la tassonomia standard delle debolezze.

PTES — Penetration Testing Execution Standard

Struttura del report allineata alle sezioni previste dallo standard: executive summary, scope e regole di ingaggio, metodologia, finding dettagliati, raccomandazioni prioritizzate, appendici tecniche.

OWASP Testing Guide (WSTG)

Riferimento metodologico per l'ambito effettivamente coperto in questo Quick Check (header di sicurezza, configurazione TLS/HTTPS, vulnerabilità note). Non copre l'intero WSTG: business logic, autenticazione e gestione sessione restano fuori — vedi Limitazioni.

NIST SP 800-115

Struttura generale dell'engagement (pianificazione, discovery, test delle vulnerabilità, reporting) applicata in forma automatizzata su una singola scansione.

Limitazioni — cosa non è stato testato

- Nessuna revisione del codice sorgente: i finding derivano esclusivamente da comportamento osservabile dall'esterno.
- Nessuna verifica mirata della logica di autorizzazione o della business logic specifica dell'applicazione (es. escalation di privilegi tra ruoli, bypass di flussi multi-step).
- Nessun test su aree autenticate: lo scan non utilizza credenziali né sessioni utente.
- Nessuna verifica manuale/proof-of-concept dei singoli finding: i risultati provengono interamente da strumenti automatici (ZAP, Nuclei, testssl.sh) e non sono stati confermati manualmente da un operatore.
- Nuclei limitato a un sottoinsieme curato di template, non l'intero corpus di template disponibile.

Finding dettagliati

Medio

1. Header Strict-Transport-Security assente

CWE-319

CVSS 3.1: 4.8 (Medium) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N (vettore valutato per questo tipo di alert, non fornito nativamente da ZAP)

Il sito non obbliga il browser a usare solo HTTPS: la prima visita può essere intercettata su una rete non fidata.

Evidenza: https://www.negozio.example/ · https://www.negozio.example/prodotti (+25 altre occorrenze)

Raccomandazione: Configura il server in modo che invii l'header Strict-Transport-Security con una durata di almeno un anno (max-age=31536000).

Rilevato da: OWASP ZAP · nome originale: Strict-Transport-Security Header Not Set

Medio

2. Protocolli deprecati abilitati: TLS 1.0, TLS 1.1

CWE-326

CVSS 3.1: 4.8 (Medium) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N (vettore valutato da Tessera)

Il server accetta connessioni TLS 1.0 e TLS 1.1, protocolli deprecati (RFC 8996) e non più accettati dai browser moderni e dagli standard di conformità (es. PCI DSS).

Evidenza: TLS 1 offered (deprecated)

Raccomandazione: Disabilitare TLS 1.0 e 1.1 e lasciare solo TLS 1.2 e 1.3.

Rilevato da: testssl.sh

Medio

3. Header anti-clickjacking assente

CWE-1021

CVSS 3.1: 4.3 (Medium) — CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N (vettore valutato per questo tipo di alert, non fornito nativamente da ZAP)

La risposta non protegge dagli attacchi di clickjacking: la pagina può essere caricata in un iframe di un altro sito, che può indurre l'utente a cliccare su elementi nascosti.

Evidenza: https://www.negozio.example/ · https://www.negozio.example/account/login · https://www.negozio.example/carrello (+16 altre occorrenze)

Raccomandazione: Imposta l'header X-Frame-Options a DENY o SAMEORIGIN, oppure la direttiva frame-ancestors della Content-Security-Policy.

Rilevato da: OWASP ZAP · nome originale: Missing Anti-clickjacking Header

Medio

4. Header Content-Security-Policy (CSP) assente

CWE-693

CVSS 3.1: 4.2 (Medium) — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N (vettore valutato per questo tipo di alert, non fornito nativamente da ZAP)

Content Security Policy (CSP) è un livello di sicurezza aggiuntivo che aiuta a rilevare e mitigare alcuni tipi di attacco, tra cui Cross Site Scripting (XSS) e iniezione di dati. Senza CSP il browser esegue qualunque script presente nella pagina.

Evidenza: https://www.negozio.example/ · https://www.negozio.example/prodotti · https://www.negozio.example/carrello · https://www.negozio.example/contatti (+19 altre occorrenze)

Raccomandazione: Configura il server web in modo che invii l'header Content-Security-Policy, partendo da una policy restrittiva (default-src 'self') e aggiungendo solo le origini necessarie.

Rilevato da: OWASP ZAP · nome originale: Content Security Policy (CSP) Header Not Set

Basso

5. Il server rivela informazioni nell'header X-Powered-By

CWE-497

CVSS 3.1: 3.7 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N (vettore valutato per questo tipo di alert, non fornito nativamente da ZAP)

Il server rivela la tecnologia usata (PHP/8.1.2) nell'header X-Powered-By: un attaccante può usare l'informazione per cercare vulnerabilità note di quella versione.

Evidenza: https://www.negozio.example/ · https://www.negozio.example/prodotti (+22 altre occorrenze)

Raccomandazione: Disattiva l'header X-Powered-By nella configurazione di PHP (expose_php = Off) o del server web.

Rilevato da: OWASP ZAP · nome originale: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Basso

6. Contenuto HTTPS disponibile anche via HTTP

CWE-311

CVSS 3.1: 3.7 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N (vettore valutato per questo tipo di alert, non fornito nativamente da ZAP)

Il contenuto disponibile in HTTPS è raggiungibile anche in HTTP senza redirect: chi usa il collegamento in chiaro espone i dati a intercettazione.

Evidenza: http://www.negozio.example/

Raccomandazione: Reindirizza tutte le richieste HTTP verso HTTPS con un redirect permanente (301) e attiva HSTS.

Rilevato da: OWASP ZAP · nome originale: HTTPS Content Available via HTTP

Basso

7. Cifrari CBC abilitati (potenziale esposizione a LUCKY13)

CWE-327

CVSS 3.1: 3.7 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N (vettore valutato da Tessera)

Il server offre suite cifrate in modalità CBC. testssl.sh segnala una potenziale esposizione a LUCKY13 (CVE-2013-0169), un attacco temporale di difficile sfruttamento sulle implementazioni moderne, ma la presenza di CBC è considerata una lacuna di hardening.

Evidenza: LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches

Raccomandazione: Preferire suite AEAD (AES-GCM, ChaCha20-Poly1305) con forward secrecy e rimuovere le suite CBC se i client da supportare lo consentono; verificare che la libreria TLS sia aggiornata.

Rilevato da: testssl.sh

Basso

8. Cookie senza attributo SameSite

CWE-1275

CVSS 3.1: 3.1 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N (vettore valutato per questo tipo di alert, non fornito nativamente da ZAP)

Un cookie è stato impostato senza l'attributo SameSite: il browser lo invia anche nelle richieste partite da altri siti, il che facilita attacchi di tipo cross-site request forgery.

Evidenza: https://www.negozio.example/ · https://www.negozio.example/account/login

Raccomandazione: Imposta l'attributo SameSite a Lax o Strict su tutti i cookie.

Rilevato da: OWASP ZAP · nome originale: Cookie without SameSite Attribute

---

Basso

9. Header X-Content-Type-Options assente

CWE-693

CVSS 3.1: 3.1 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N (vettore valutato per questo tipo di alert, non fornito nativamente da ZAP)

L'header anti-MIME-sniffing X-Content-Type-Options non è impostato a 'nosniff': alcuni browser possono interpretare un file con un tipo diverso da quello dichiarato.

Evidenza: https://www.negozio.example/ · https://www.negozio.example/static/app.js · https://www.negozio.example/static/style.css (+28 altre occorrenze)

Raccomandazione: Imposta l'header X-Content-Type-Options: nosniff su tutte le risposte.

Rilevato da: OWASP ZAP · nome originale: X-Content-Type-Options Header Missing

---

Basso

10. Cookie senza flag HttpOnly

CWE-1004

CVSS 3.1: 3.1 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N (vettore valutato per questo tipo di alert, non fornito nativamente da ZAP)

Un cookie è stato impostato senza il flag HttpOnly: uno script eseguito nella pagina, ad esempio tramite una vulnerabilità XSS, può leggerlo.

Evidenza: https://www.negozio.example/account/login

Raccomandazione: Imposta il flag HttpOnly su tutti i cookie che non devono essere letti da JavaScript, a partire da quello di sessione.

Rilevato da: OWASP ZAP · nome originale: Cookie No HttpOnly Flag

---

Informativo

11. Divulgazione di informazioni: commenti sospetti

CWE-615

La risposta contiene commenti nel codice che possono rivelare informazioni utili a un attaccante (ad esempio note di sviluppo o riferimenti a funzioni interne).

Evidenza: https://www.negozio.example/static/app.js (+1 altre occorrenze)

Raccomandazione: Rimuovi dal codice inviato al browser i commenti che fanno riferimento a dettagli interni.

Rilevato da: OWASP ZAP · nome originale: Information Disclosure - Suspicious Comments

---

Informativo

12. Contenuto memorizzabile nelle cache condivise

CWE-524

Le risposte possono essere conservate nella cache di proxy condivisi: se contengono dati personali, un altro utente dello stesso proxy potrebbe ricevere una copia.

Evidenza: https://www.negozio.example/prodotti · https://www.negozio.example/contatti (+7 altre occorrenze)

Raccomandazione: Per le pagine con dati personali o di sessione imposta Cache-Control: no-store, private.

Rilevato da: OWASP ZAP · nome originale: Storable and Cacheable Content

Informativo 13. Direttive Cache-Control da rivedere

CWE-525

L'header Cache-Control non è impostato in modo adeguato o manca: il browser o un proxy potrebbero conservare in cache contenuti personali.

Evidenza: https://www.negozio.example/account · https://www.negozio.example/carrello (+2 altre occorrenze)

Raccomandazione: Per le pagine con dati personali imposta Cache-Control: no-store; per le risorse statiche usa una durata di cache esplicita.

Rilevato da: OWASP ZAP · nome originale: Re-examine Cache-control Directives

Informativo 14. Cookie valido per un dominio troppo ampio

CWE-565

Un cookie è valido per un dominio più ampio di quello che lo imposta: anche gli altri sottodomini possono riceverlo e modificarlo.

Evidenza: https://www.negozio.example/account/login

Raccomandazione: Imposta il cookie senza attributo Domain, oppure con il solo dominio che lo usa.

Rilevato da: OWASP ZAP · nome originale: Loosely Scoped Cookie

Aspetti positivi

- Voto TLS: B (testssl, sperimentale). Il voto non considera HSTS né i cifrari CBC: vedi i finding TLS e l'header Strict-Transport-Security.
- TLS 1.3 supportato.
- Forward secrecy con cifrari AEAD disponibile.
- Catena di fiducia del certificato valida.
- Nessuna esposizione a Heartbleed, ROBOT, POODLE, SWEET32, FREAK, DROWN e altre vulnerabilità TLS note verificate da testssl.sh.
- Nessuna vulnerabilità nota rilevata da Nuclei.

Raccomandazioni prioritizzate

P1 — Proteggere il collegamento HTTPS

- Attivare Strict-Transport-Security e il redirect permanente da HTTP a HTTPS.
- Disabilitare TLS 1.0 e 1.1, lasciando solo TLS 1.2 e 1.3.

P2 — Aggiungere gli header di sicurezza

- Introdurre una Content-Security-Policy, partendo in modalità report-only per non bloccare funzioni esistenti.
- Impostare X-Frame-Options (o frame-ancestors) e X-Content-Type-Options: nosniff.

P3 — Ridurre le informazioni esposte e rafforzare i cookie

- Disattivare l'header X-Powered-By (expose_php = Off).
- Impostare SameSite sui cookie di sessione e rivedere le direttive di cache delle pagine personali.

Appendice tecnica — Header di sicurezza

Content-Security-Policy	**Assente**
Strict-Transport-Security	**Assente**
X-Frame-Options	**Assente**
X-Content-Type-Options	**Assente**

Nota: X-Powered-By: PHP/8.1.2

Appendice tecnica — TLS (testssl.sh, output completo)

```
 Start 2026-10-11 09:02:14        -->> 203.0.113.10:443 (www.negozio.example) <<--

 rDNS (203.0.113.10):           --
 Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered (deprecated)
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       not offered
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)

 Testing server defaults (Server Hello)

 Certificate Validity (UTC)   78 >= 60 days (2026-09-12 00:00 --> 2026-12-28 23:59)
 Chain of trust               Ok
 OCSP stapling                not offered

 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)               not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                      not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                    not vulnerable (OK)
 Secure Renegotiation (RFC 5746)          supported (OK)
 CRIME, TLS (CVE-2012-4929)               not vulnerable (OK)
 POODLE, SSL (CVE-2014-3566)              not vulnerable (OK), no SSLv3 support
 SWEET32 (CVE-2016-2183, CVE-2016-6329)   not vulnerable (OK)
 FREAK (CVE-2015-0204)                    not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)     not vulnerable on this host and port (OK)
 LOGJAM (CVE-2015-4000), experimental     not vulnerable (OK): no DH key detected with <= TLS 1.2
 BEAST (CVE-2011-3389)                    TLS1: ECDHE-RSA-AES128-SHA
                                          VULNERABLE -- but also supports higher protocols  TLSv1.1
TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental    potentially VULNERABLE, uses cipher block chaining (CBC)
ciphers with TLS. Check patches
 RC4 (CVE-2013-2566, CVE-2015-2808)       no RC4 ciphers detected (OK)

 Rating (experimental)

 Overall Grade                B
 Grade cap reasons            Grade capped to B. TLS 1.1 offered
                              Grade capped to B. TLS 1.0 offered

 Done 2026-10-11 09:03:31 [  79s] -->> 203.0.113.10:443 (www.negozio.example) <<--
```