SENTRIC · CYBERSECURITY

SENTRIC

SECURITY ASSESSMENT REPORT

38
/100
SENTRIC SCORE

ALVO	CLIENTE	DATA
acme-shop.example	ACME Shop, Lda (exemplo)	13/07/2026

ANALISTA	REFERENCIA	ESTADO
Sentric	SNTC-SAMPLE-2026	CONCLUIDO

1	2	3	8
CRITICAL	HIGH	MEDIUM	TOTAL

SUMARIO EXECUTIVO

NIVEL DE RISCO: CRITICO

Score Sentric: 38/100 | 8 vulnerabilidade(s) | Alvo: acme-shop.example

A avaliacao de seguranca ao sistema "acme-shop.example" foi realizada em 13/07/2026 pela Sentric. Foram identificadas 8 vulnerabilidade(s): 1 critica(s), 2 alta(s), 3 media(s) e 2 baixa(s). Score Sentric: 38/100 — nivel insuficiente (remediacao urgente).

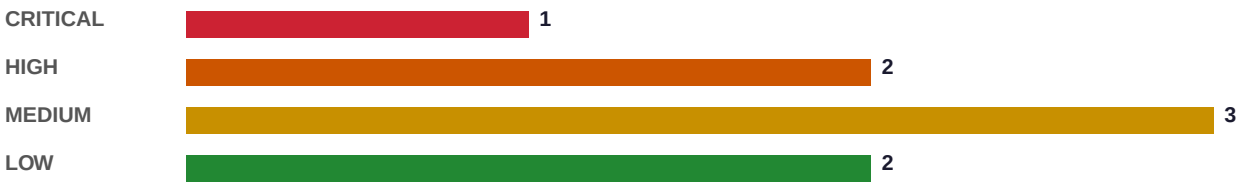
SCOPE DO TESTE

- Reconhecimento de rede: portas TCP, SSL/TLS, DNS (SPF, DMARC, MX), headers HTTP
- Paths expostos identificados: 2
- Subdominios verificados: 7
- Testes web: CORS, rate limiting, slowloris, metodos HTTP, open redirect
- Codigo-fonte analisado: 14 ficheiro(s)
- Deteção de secrets: AWS, GitHub, Stripe, JWT, DB URLs, API keys

TECNOLOGIAS IDENTIFICADAS

- Nginx (Server)
- PHP (Language)
- WordPress (CMS)

DISTRIBUICAO POR SEVERIDADE



VULNERABILIDADES ENCONTRADAS

CRITICAL SR-01 [exposicao]

Ficheiro .env exposto com credenciais

/.env acessivel publicamente (HTTP 200) revelando chaves de API e password de base de dados.

REMEDIACAO:
Remover o ficheiro do webroot e rodar todas as credenciais expostas de imediato.

HIGH SR-02 [injecao]

Injecao SQL provavel em /search

O parametro q reflete erros de base de dados, indicando falta de sanitizacao.

REMEDIACAO:
Usar consultas parametrizadas (prepared statements) e validar toda a entrada.

HIGH SR-03 [headers]

Header Content-Security-Policy em falta

Sem CSP, a pagina fica exposta a XSS e injecao de conteudo.

REMEDIACAO:
Definir Content-Security-Policy restritiva (default-src 'self').

MEDIUM SR-04 [email]

Sem registo SPF

Ausencia de SPF facilita spoofing de email a partir do dominio.

REMEDIACAO:
Publicar registo TXT: v=spf1 -all (ajustar aos emissores legitimos).

MEDIUM SR-05 [email]

Sem DMARC

Sem DMARC nao ha enforcement anti-spoofing nem relatorios.

REMEDIACAO:
Publicar _dmarc com p=reject apos periodo de monitorizacao.

VULNERABILIDADES (6/8)

MEDIUM SR-06 [headers]

Clickjacking possivel

Pagina enquadravel em iframe (sem X-Frame-Options / frame-ancestors).

REMEDIACAO:
X-Frame-Options: DENY ou CSP frame-ancestors none.

LOW SR-07 [dns]

Sem registo CAA

Qualquer autoridade certificadora pode emitir certificado para o dominio.

REMEDIACAO:
Adicionar registo CAA a restringir as CAs autorizadas.

LOW SR-08 [processo]

Sem security.txt

Sem canal documentado de reporte de vulnerabilidades (RFC 9116).

REMEDIACAO:
Publicar /.well-known/security.txt com contacto de seguranca.

TERMOS E DISCLAIMER

AUTORIZACAO

Este teste foi conduzido mediante autorizacao expressa do responsavel pelo sistema "acme-shop.example". Testes sem autorizacao escrita constituem crime informatico.

CONFIDENCIALIDADE

Este relatorio e confidencial. O seu conteudo nao deve ser partilhado com terceiros sem autorizacao previa e escrita da Sentric.

LIMITACOES

Este relatorio reflete o estado do sistema na data do teste. Recomenda-se re-avaliacao periodica apos atualizacoes ou mudancas de infraestrutura.

REMEDIACAO

Recomenda-se correcao prioritaria de todos os findings CRITICOS e ALTOS. Para suporte na implementacao, contacte a Sentric.

RESPONSABILIDADE

A Sentric nao se responsabiliza por vulnerabilidades identificadas apos a data do teste ou por danos resultantes de exploracao por terceiros.

Sentric
Sentric

ACME Shop, Lda (exemplo)
Data: 13/07/2026