Website Vulnerability Scan Report

Scanned URL: **https://www.youtube.com/**

Date: 2025-07-11 11:26:01

A01: Broken Access Control

Status: Secure
Severity: Low

All tested endpoints are protected from unauthorized access.

A02: Crypto Failures

Status: Secure
Severity: Low

Site uses HTTPS and HSTS is properly configured.

A03: Sql Injection

Status: Vulnerable
Severity: High

SQL error message detected at: https://www.youtube.com/?id=' OR '1'='1

A04: Xss Scanner

Status: Secure
Severity: Low

No XSS vulnerability detected at: https://www.youtube.com/?q=alert(1)

A05: Security Headers

Status: Vulnerable
Severity: Medium

Missing security headers:
Referrer-Policy

A06: Vulnerable Components

Status: Vulnerable
Severity: Medium

Static test only: Check jQuery/bootstrap versions manually in HTML source.

This scanner does not currently parse or validate actual library versions.

A07: Auth Failures

Status: Manual Review
Severity: Medium

Authentication endpoints found. Manual testing recommended:
https://www.youtube.com/login — should be tested for brute-force protection and 2FA
https://www.youtube.com/admin — should be tested for brute-force protection and 2FA
https://www.youtube.com/change-password — should be tested for brute-force protection and 2FA

A08: Data Integrity

Status: Manual Review
Severity: Low

This test requires monitoring of CI/CD pipelines, file integrity checks, or signed updates.
Static analysis is insufficient to detect software/data integrity issues.

A09: Logging Monitoring

Status: Manual Review
Severity: Low

No public evidence of logging or monitoring issues found.
Proper detection requires backend access to verify log generation, alerting, and retention policies.

A10: Ssrf

Status: Secure
Severity: Low

No SSRF behavior detected via: https://www.youtube.com?url=http://127.0.0.1:80