Salesforce Commerce Cloud Security Audit

Identify vulnerabilities. Strengthen your storefront. Prepare for AI Enablement

The **ETG SFCC Security Scanner** is a free, fully automated black-box security tool available at **scanner.etg.digital**. Powered by Playwright and Google Gemini AI, it runs **75 automated checks** across OCAPI Shop API, SCAPI Shopper API, and General HTTP layers — instantly identifying vulnerabilities in your SFCC storefront and connecting you with ETG's security engineers for full remediation guidance.

75 Automated Checks

Across OCAPI, SCAPI, and HTTP layers

AI-Powered

Playwright + Google Gemini AI

Free to Use

No install, no agent, no code access

Under 15 Minutes

Full scan completes rapidly

What the Audit Covers

AI-Powered Security Scan

- Playwright headless browser crawls your storefront maps endpoints, forms, user flows, and API calls
- Google Gemini AI selects the most relevant tests based on detected architecture (SFRA / OCAPI /
- SCAPI / Headless / Hybrid)
- Detects XSS, CORS, IDOR, injection, session fixation, auth bypass, JWT flaws, PII exposure,
- clickjacking, and 65+ more
- reCAPTCHA v2 bot protection + SSRF URL validation ensures only authorized, legitimate scans run

OCAPI Shop API — 23 Checks

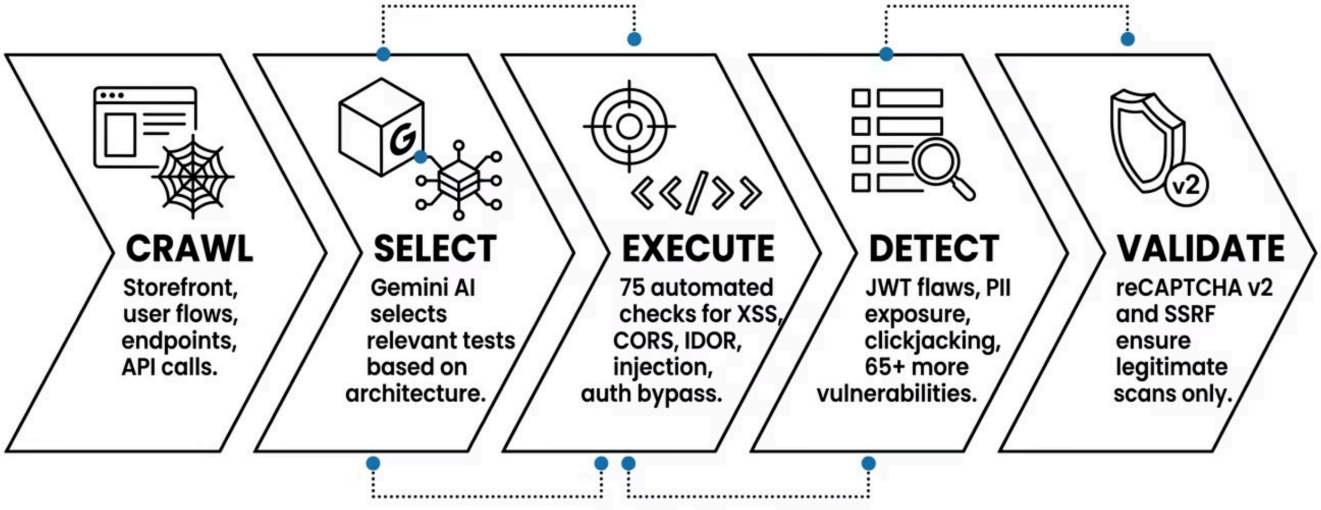
Basket IDOR, OrderPII, JWT security, Payment data exposure, WebDAV/BM exposure, Coupon brute force, and more

SCAPI Shopper API — 28 Checks

SLAS token security, Redirect manipulation, Mass assignment, Price book switching, Geolocation spoofing, and more

General HTTP — 18 Checks

XSS, CORS, CSRF, Clickjacking, Cookie security, SSL/TLS, Open redirect, JS secrets scanner, and more



Deliverables

Every scan produces a layered set of outputs — from a plain-English executive summary for stakeholders to a full technical report with CVSS scores and reproduction steps for your engineering team.

Free Summary PDF

Instantly available after scan completion. Includes:

- Severity breakdown: Critical / High / Medium / Low / Info
- Finding names and categories
- AI Executive Summary written by Gemini — plain-English risk narrative for stakeholders

No technical evidence included — safe to share broadly

Full Technical PDF *(ETG Internal)*

Delivered by ETG's engineers following lead capture. Includes:

- All findings with CVSS scores
- HTTP request/response evidence
- Reproduction steps for each vulnerability
- Remediation consultation with ETG security engineers

Lead capture gates the download — ETG team follows up with the full report

75

Automated Checks

Across all API and HTTP layers

<15

Minutes to Complete

Full scan, no install required

5

Severity Levels

Critical, High, Medium, Low, Info

0

Code Access Needed

Fully black-box, external scan

Why ETG & How to Get Started

Why Choose ETG

Salesforce Summit Partner

Deep SFCC expertise across SFRA, Headless PWA, Hybrid, and composable storefronts

Proven Accelerators

Purpose-built tools for scanning, mapping, and remediation — not generic security frameworks

Security-First Modernization

A clear path from Audit → Fix → Modernize → Salesforce Next

⚠ Authorised use only — scan domains you own or have written permission to test. CFAA / Computer Misuse Act 1990 compliant.

How to Get Started

01

Visit the Scanner

Go to **scanner.etg.digital** — enter your storefront URL

02

Run Your Free Scan

No install, no code access, no agents — completes in under 15 minutes

03

Receive Your PDF

Get your free Summary PDF instantly with severity breakdown and AI narrative

04

ETG Engineers Follow Up

Full technical report, CVSS scores, reproduction steps, and remediation consultation

ⓘ **Ready to secure your Commerce Cloud?** Contact ETG Digital at **sales@etg.digital** or visit **www.etg.digital** to start your Salesforce Commerce Cloud Security Audit today.

25 YEARS etg digital