LONGARINI 13 - R10 Qualification Record

Public technical evidence release / 08 NOV 2026 / Private IP retained

OWASP ZAP 2.17.0 - actual passive campaign

7/7 traditional spider scans completed across 13 demos on 7 hosts; no active exploitation or form submission. First-party original scanner counts: 1 High, 89 Medium and 217 Informational.
High alert: apparent PII disclosure was 16 digits inside a public SHA-256 digest. Classified as false-positive candidate. 89 Medium alerts: wildcard CORS on public resources, not proof of credentialed data exfiltration. Neither finding is erased.
Source ZAP machine-report SHA-256: 406abab58b85b464279f0aa5e4119586df3da1c9a7f2dbe933776aa8bd56ff5d.

Physical access versus actual measurements

OVHcloud browser dashboard authenticated; SSH network transport reachable. FPGA Pi3 lab browser connection and web power-on status observed. This QA runner has no authenticated shell/JTAG control; new pin timing, NIC hardware offload and electrical results: NOT MEASURED.

Independent native reference, not proprietary-engine qualification

C++20 1,951,560 optimized reference checks (zero predicate disagreements); 521,560 sanitized checks. Generic isolated XDP on veth: 40/40; three-process SQLite/TCP recovery: 180 cases on ONE Linux host. No FPGA product, avionics, production wire-to-wire or globally atomic settlement certification.

User-facing functional acceptance and scope

Prior Chrome campaign 39/39 at 390/768/1440 px for all 13 demo pages. Fixed-scope buyer diagnostic uses TWO calls of 20 minutes, separate approved isolated sample, written GO/NO-GO/INCONCLUSIVE dossier. No commercial outreach or LinkedIn publishing done in this run.
Evidence is narrowly scoped. Original ZAP report checksum can be compared with the retained internal machine file. Never infer that passive scanning proves no vulnerabilities.