



PXL SECURITY · RESEARCH

State of Our Findings 2026

What a decade of manual penetration testing and red teaming actually turns up — the severity mix, the most common root causes, and where the real risk sits.

Based on 21 anonymised engagements and 190 findings delivered by the PXL Security team. Contains no client names, systems or data.



About this report

Most “state of security” reports are written to sell a product. This one is written from our own delivery work. It aggregates the findings from recent PXL Security engagements — web, API, mobile, internal, external, red-team and phishing — across fintech, SaaS, healthcare, manufacturing, logistics and the public sector.

It is deliberately honest about its limits. The sample is modest, and we publish it because it is **real**, not because it is large. Every number below comes from a delivered report; nothing is modelled or inflated.

Method & honesty note. Counts are taken verbatim from each engagement's own findings summary. Where a report did not rate findings on a CVSS scale (some red-team reports), those findings are counted in the totals but left out of the severity split rather than guessed at. All data is anonymised to counts only — no client, system or personal data was used.

21

engagements

190

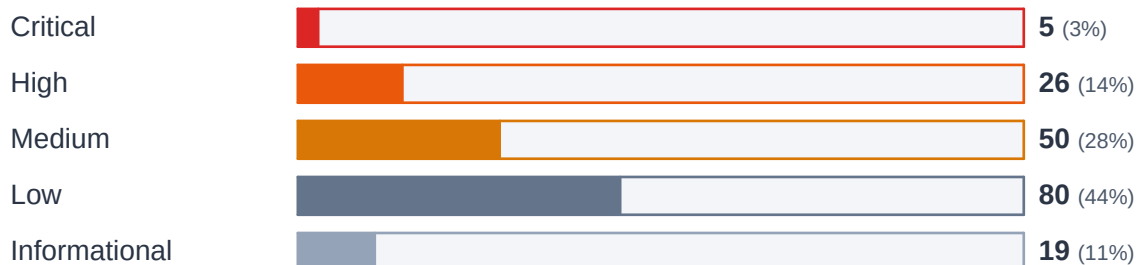
findings

6

sectors

1 · Severity distribution

Of the 180 findings rated on a CVSS scale (10 red-team findings were reported as narrative risk and are excluded from this split):



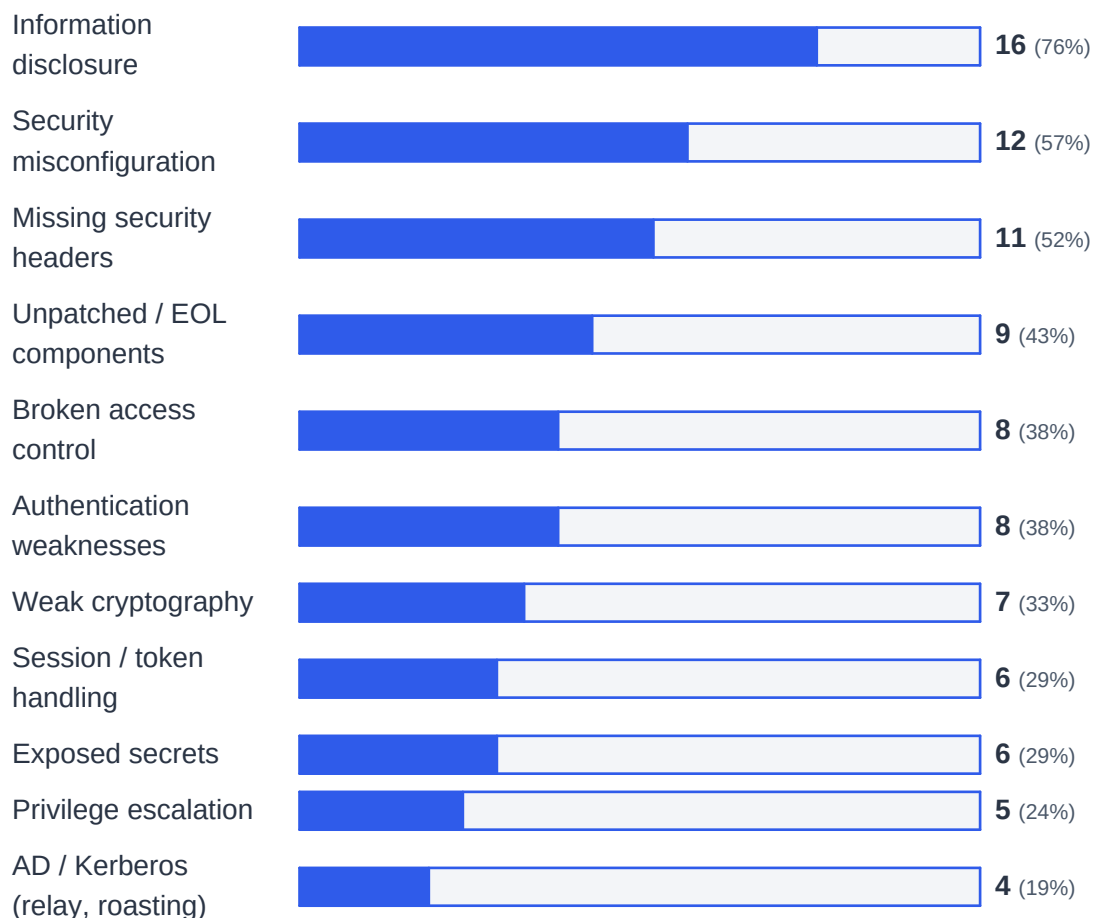
High and Critical together make up about 17% of rated findings — the minority, but the part that ends engagements. The long tail of Low and Informational issues is where most of the volume sits, and where a scanner would stop; the serious findings are almost always the ones that needed a human to chain together.

2 · Where the serious findings were

A High or Critical finding appeared in **7 of 21 engagements** by CVSS rating. On top of that, **two to three red-team engagements reached full domain compromise** — reported as narrative risk rather than a CVSS number — so a genuinely serious outcome was present in closer to half of all engagements. The headline issues clustered around credential handling, access control and Active Directory hygiene, not novel exploits.

3 · The most common root causes

By share of engagements in which each class appeared at least once:



The pattern is consistent year on year: the issues that recur most are **configuration and hygiene**, not clever bugs. Information disclosure, misconfiguration and missing hardening show up almost everywhere; the damaging ones — access control, exposed secrets, AD relay and Kerberoasting — are fewer but far more impactful.

4 · What we tested

By engagement type	By sector
Web 9 · Red team 3 · External 3 · Mobile 2 · Internal 2 · API 1 · Phishing 1	SaaS 8 · Bank / fintech 7 · Manufacturing 3 · Healthcare 1 · Logistics 1 · Public sector 1

5 · The good news we also report

Not every engagement is a horror story, and we report clean results as carefully as serious ones. In this dataset: one external web application returned **zero findings** (CDN/WAF, CAPTCHA and rate-limiting all effective); a large logistics perimeter of roughly 80 hosts had **no exploitable High or Critical** issues, with seven headline CVEs proven non-exploitable; and a bank's red team saw **0% phishing click-through**, one whole campaign blocked at the gateway, and network segmentation that stopped lateral movement. A verified clean result is evidence worth having.

6 · Where this says to spend

- 1. Secrets and privilege.** Where our worst findings come from — hardcoded and exposed secrets, over-privileged database and service accounts.
- 2. Server-side authorization.** On every object and every action; broken access control is the most common serious application bug we see.
- 3. AD hygiene.** Signing and channel binding, Kerberoast and AS-REP exposure, privileged-group cleanup — the cheapest high-impact internal wins.
- 4. Patching and EOL.** Unsupported components sit behind a large share of our critical findings.
- 5. Token lifecycle.** Short-lived, server-revocable, never in URLs or page scripts.

Want this picture for your own environment?

Everything in this report comes from manual testing by senior engineers — the same work we'd bring to your systems, with evidence for every finding and a retest to prove the fix. Penetration testing, red teaming and secure development, independent since 2014.

Request a proposal: pxlsec.com/contact · hello@pxlsec.com

PXL Security LTD · 12 Vasil Levski Blvd., 1142 Sofia, Bulgaria · VAT BG203239331