



CASE STUDY

A 24-hour token in all the wrong places

Healthcare SaaS (patient data) · Authenticated web + API pentest

Token-lifecycle redesign delivered

Anonymised under NDA. Client and identifying details are withheld. PXL Security LTD · Sofia, Bulgaria · pxlsec.com

CASE STUDY

A 24-hour token in all the wrong places

Sector	Healthcare SaaS (patient data)
Engagement	Authenticated web + API pentest
Outcome	Token-lifecycle redesign delivered

1 token class, exposed 3 ways	24h access window per token	0 tokens revoked on logout
---	---------------------------------------	--------------------------------------

THE CHALLENGE

A multi-tenant healthcare platform handling patient data needed an authenticated, multi-role test of its web and API product and its OAuth identity layer.

HOW IT UNFOLDED

1. Tested the web + API product across multiple roles and the OAuth identity layer.
2. Found a long-lived (24-hour) patient-data API token returned in a URL fragment during SSO handoff.
3. Found the same token class embedded in a page-level JavaScript global.
4. Found it obtainable via an enabled resource-owner-password grant with long-lived refresh tokens on a public client.
5. Confirmed tokens were not revoked on logout — widening the window for theft and reuse.
6. Found a disabled-but-leaky GraphQL endpoint disclosing schema, and an order workflow accepting client-supplied status and dates.

KEY FINDINGS

High	Long-lived PHI token exposed via URL fragment and JS global
High	Resource-owner-password grant enabled on a public client
Medium	Tokens not revoked on logout
Medium	Clinical order workflow trusts client-supplied status/date

IMPACT

A single client-side foothold translated into a full day of access to patient records.

OUTCOME

A token-lifecycle redesign (authorization-code + PKCE, short lifetimes, server-side revocation, no tokens in URLs or globals) and server-side workflow validation — closing the chain at its root.

TECHNIQUES

OAuth/OIDC · Token leakage · GraphQL disclosure · Business-logic bypass · BOLA/IDOR

SERVICES

Penetration Testing · Secure Development



Work with PXL Security

Independent offensive-security testing since 2014 — penetration testing, red teaming and secure development, delivered by senior engineers with evidence for every finding and a retest to prove the fix.

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

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