Case Study: Web Application VAPT for EdTech Platform (Anonymized)

Category: Web & API Security
Duration: 2 Weeks | **Engagement Type:** Black-box & Authenticated Penetration Testing
Tools: Burp Suite Pro, OWASP ZAP, Postman, Nmap, CyberCLI, Amass, Python

---

Context

An EdTech company providing online learning tools and payment-enabled student dashboards required a **web application penetration test** before onboarding new universities.

The scope included multiple web subdomains (`portal.edtech.com`, `teacher.edtech.com`, `api.edtech.com`) with both public and authenticated interfaces.

The objective was to uncover security weaknesses that could expose student data, session tokens, or academic records — while ensuring compliance with internal AppSec standards and privacy regulations (GDPR ready posture).

Approach

Testing was conducted using a hybrid **black-box and gray-box** methodology aligned with **OWASP Web Security Testing Guide (v4.2)**.

1. **Discovery & Reconnaissance** – Mapped application surface using CyberCLI and Amass to identify 60+ live endpoints.

2. **Authentication & Session Management** – Analyzed token reuse, password reset flows, and cookie flags.

3. **Access Control** – Tested role-based access boundaries between student, faculty, and admin accounts.

4. **Input & Injection Testing** – Used custom payloads for SQLi, stored XSS, and command injection vectors.

5. **Business Logic Review** – Evaluated payment APIs and grading modules for race conditions and replay flaws.

Key Findings

Severity	Count	Highlight
Critical	1	Account takeover via insecure password reset token (predictable UUIDv4)
High	3	Broken Access Control in student grading endpoint exposed assessment data across roles
Medium	4	Reflected XSS in teacher dashboard's announcement form
Low	5	Misconfigured CORS policy exposing internal endpoints to wildcard origins

---

Remediation Summary

- Implemented **token entropy enforcement** and **single-use password reset links**.
- Deployed **object-level authorization (OLA)** middleware to prevent data leakage.
- Sanitized user inputs via server-side HTML escaping; introduced a **global XSS filter**.
- Restricted CORS headers to trusted domains and added pre-flight request validation.
- Integrated automated nightly scans in CI using **CyberCLI + ZAP CLI** with Slack reporting.

Outcome

- Eliminated 90% of high-impact vulnerabilities before launch
- Reduced response time for security issues from 5 days → under 24 hours
- Enabled continuous scanning for new builds — aligned with **Shift-Left** security principles
- Strengthened student data privacy posture and passed internal compliance validation

---

Executive Summary

The engagement revealed critical gaps in access control and token management, typical of high-scale web applications.

Through rapid remediation and validation, the EdTech team achieved a measurable improvement in application security posture without disrupting operations.

The project concluded with a collaborative **knowledge-transfer session**, ensuring developers could independently manage future assessments and integrate security into ongoing CI/CD releases.
