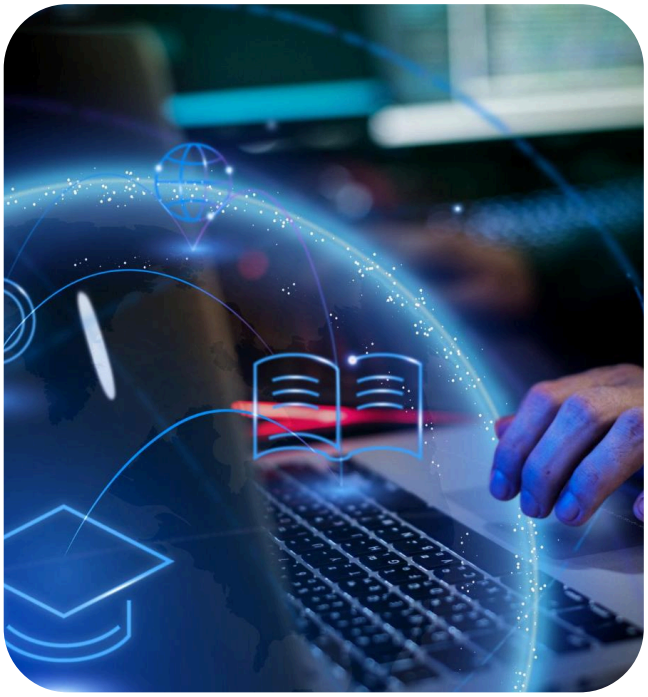
QBurst | A High AI-Q™ Company

Securing a High-Traffic EdTech Platform Against Critical Vulnerabilities

Read how our QE team eliminated critical security risks to ensure compliance, protect sensitive academic data, and deliver immediate ROI.

Overview

- Delivered a comprehensive web application security assessment, uncovering 23 vulnerabilities and preventing large-scale account compromise.
- Enabled FERPA and GDPR compliance, unlocking $2.5M in enterprise contracts.
- Eliminated potential breach risks valued between $1.5M and $5M.



Client Profile

A fast-scaling, US-based educational technology company offering a web-based learning management system. Serving over 10,000 students, instructors, and administrators, the platform supports course management and sensitive academic data while expanding its enterprise footprint globally.

Challenge: When Growth Outpaced Security

- No prior professional security assessment, leaving the platform without a defined security baseline.
- Absence of FERPA and GDPR compliance, limiting enterprise readiness.
- Critical weaknesses in authentication flows, including password reset and session management.
- Rapid feature expansion increased the attack surface without corresponding security validation.
- Exposure of sensitive data such as AWS credentials and database schema in application responses.

QBurst Solution: Comprehensive Security Assessment and Remediation Strategy

We implemented a structured, four-phase web application security assessment combining automated scanning with expert manual testing to uncover deep-seated vulnerabilities, such as business logic flaws and authentication bypass risks that automated tools miss. The four-phased engagement extended beyond detection to a remediation partnership, ensuring vulnerabilities were resolved effectively and securely.

- Full application reconnaissance covering architecture, roles, and authentication flows
- Manual testing aligned with OWASP Top 10 and SANS Top 25 standards
- Proof-of-concept exploit validation with CVSS v3.1 scoring and attack chain documentation
- Detailed remediation roadmap with developer training and fix verification

Findings & Remediation

Our assessment identified **23 vulnerabilities,** including **two critical authentication flaws (CVSS 9.8 & 9.1)** that could enable full account takeover and administrative access without credentials.

Key Risks Uncovered

- **Complete account takeover** via password reset manipulation
- **Authentication bypass** through insecure session cookies
- Stored XSS enabling malicious script execution across users
- Broken access control allowing privilege escalation
- Sensitive data exposure, including AWS credentials and internal architecture
- No brute-force protection, leaving accounts vulnerable to automated attacks

Remediation Actions Delivered

- Patched critical authentication vulnerabilities to prevent account takeover
- Eliminated XSS and injection risks through input sanitization
- Implemented rate limiting and account lockout to stop brute-force attacks
- Rotated AWS credentials and hardened infrastructure security
- Embedded security into CI/CD and development practices

"The assessment was eye-opening. They found vulnerabilities automated scanners would never catch, then worked with us to fix them - and taught us how to build security into our process. The ROI was immediate when we closed our first enterprise contract."
- Engineering Lead, EdTech Platform

Impact: Exploitable to Enterprise-Ready

- Achieved full FERPA and GDPR compliance, enabling enterprise readiness.
- Secured $2.5M in new contracts post-certification.
- Protected 10,000+ users by eliminating critical account takeover and session hijacking risks.
- Prevented potential breach losses estimated between $1.5M and $5M.
- Reduced security incidents by 90% and accelerated developer review cycles by 60%.