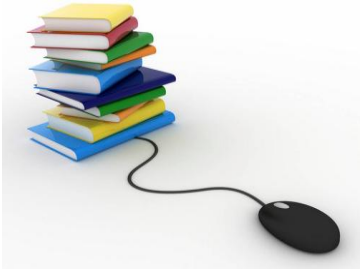
Publishing, Secure Coding For A Start Up
Case Study – Putting Security at the Centre of Software Development Life Cycle

The Client

A Start-Up publishing company with a disruptive technology and approach for the academic publishing industry.



Client Profile

A very well financed start up headquartered in London. The company was set up as an interdisciplinary publisher of scholarly peer-reviewed research. Backed by editorial standards, the mission is to make academic publishing efficient, transparent accessible and fair. The academic publishing industry is worth in the region of $25.5 Billion globally.

The skilled front end and back end development teams were working in a technology environment reflective of industry trends. By using Node.js, AWS (Amazon Web Services) and Ubuntu and Nginx which are at a peak of popularity. Nginx is a hugely popular open source HTTP server.

CYBERRISK.COM
SECURITY - ASSURANCE - FORENSICS - ENABLING

The Challenge

The creation of a secure and resilient web-based platform and interface, for a new disruptive paradigm for academic publishing and research. The web-based platform's resilience had to include, but was not limited to, robust and predicable responses to web-based attacks such as DDOS, Injection Vulnerabilities. We needed to provide assurance that secure interfaces both internally and externally were robust in restricting access, to authorised personnel; whilst protecting databases and storage media from intrusion and loss of data and privacy.

Response

Cyberrisk.com was engaged to lead the initiative to embed cyber security front, back and centre of the software development life cycle with regards industry best practices; in addition to establishing the board room approach to managing cyber risks as a business imperative for success.

Cyberrisk.com highlighted the attack surfaces and critical trust boundaries of the application, through detailed threat modelling. Thereby creating an understanding of current web application threats relative to the application's security posture. This was followed by vulnerability and risk assessments, code reviews and penetration testing of the web application. At the corporate level, a scalable cyber security strategy was developed that will mature as the organisation grows; which will be the basis for managing cyber risks and information as a strategic asset. Mentoring of the development team in cyber security best practice principles was a key element of success, along with cyber risk awareness education at all levels.

Result

- The development and implementation of a scalable cyber security strategy.
- Mitigation of identified web-application vulnerabilities providing resilience to common and novel attack scenarios and privacy breaches.
- Adoption of industry best practice based on the Trusted Software Initiative (TSI) as a central approach of the software development life cycle.
- Continuous cyber security mentoring for the development team.
- Cyber Risks adopted as a core tenant of overall business process by the founders.

e-mail: hi@cyberrisk.com