Public Report

CourseWave Security Assessment

Title	**CourseWave Security Assessment Public Report**
Version	1.0
Reporting Date	Thursday, January 29, 2026
Prepared by	Cyberglobal
Prepared for	American Book Company
Contact	Octavian Minea Cyber Operations Manager
Classification	Public

cyberglobal

Document Control

Version	Date	Author	Change Description
0.1	Monday, October 20, 2025	Cyber Security Team	Security Assessment Start
0.2	Monday, October 27, 2025	Quality Control Manager	Security Assessment Report Delivery
0.3	Wednesday, January 28, 2026	Cyber Security Team	Vulnerability Remediation Verification Completed
1.0	Thursday, January 29, 2026	Quality Control Manager	Public Report Delivery

cyberglobal

Legal name: CyberGlobal
Email: info@cybergl.com
Website: cybergl.com

CREST

Cyberglobal is a CREST Accredited Company in Penetration Testing.

Independent Security Assessment Report

Cyberglobal LTD (“Cyberglobal”) has performed the Web Application Security Assessment for American Book Company (“Client”) while acting as an independent security assessor. This assessment was performed with the intent of evaluating the security and resiliency of the client’s web application.

The methodology utilized during this assessment is detailed in Methodology. Cyberglobal developed this methodology based on extensive professional experience and information system security assessment best practices gathered from the NIST Risk Management Framework, Open Source Security Testing Methodology Manual ("OSSTMM"), the National Institute of Standards and Technology ("NIST") Special Publication 800-115: Technical Guide to Information Security Testing and Assessment, the Penetration Testing Execution Standard ("PTES"), NIST Guide Details Forensic Practices, various CIS Benchmarks, and the Open Web Application Security Project ("OWASP") Testing Guide.

While this type of assessment is intended to mimic a real-world attack scenario or identify the capacity of the existing controls, Cyberglobal is bound by rules of engagement, defined scope, allocated time, and additional related constraints. Cyberglobal has made every effort to perform a thorough analysis and to provide appropriate remedial advice. However, inherent limitations, errors, misrepresentations, and changes to the Client environment may have prevented Cyberglobal from identifying every security issue that was present in the Client environment at the time of testing. Therefore, the findings included in this report should be considered to be representative of what a similarly skilled attacker could achieve with comparable resources, constraints, and time frame.

Additionally, it is worth emphasizing that the findings and remediation recommendations are the result of a point-in-time assessment based on the state of the Client environment as of Wednesday, January 28, 2026. Cyberglobal therefore does not provide any assurance related to configuration or control modifications in the Client environment, changes in regulatory or compliance requirements, discoveries of new vulnerabilities and attack techniques, or any other future event that may impact the Client’s security posture.

The information contained in this report represents a fair and unbiased assessment of the Client’s environment based on the agreed-upon criteria as defined in the Statement of Work. This report is provided to the Client as notification of outstanding security risks that threaten the confidentiality, integrity, and availability of sensitive information, as well as to provide assistance and direction with remediation. The evidence and references provided for each finding serve as the basis for our qualified opinions in this report.

Octavian Minea
Cyber Operations Manager
Cyberglobal, LTD

Scope of Work

Background Information

Cyberglobal performed a security audit following the Web Application Security Assessment methodology to assess the risk that a real-life, targeted attacker poses to the security and integrity of the client's assets. Understanding the current vulnerabilities is the first step in remediating and ultimately enhancing American Book Company's overall security maturity.

The purpose of the assignment was to identify and evaluate any risks or potential issues that could impact the Confidentiality, Integrity, or Availability of the systems in scope. In this assessment, both automated and manual security testing techniques were used to identify weaknesses in the systems in scope from an attacker's perspective.

Cyberglobal performed testing from both unauthenticated (anonymous) and authenticated perspectives. Unauthenticated testing identifies vulnerabilities and weaknesses available to anyone who possesses network connectivity to the CourseWave environment. Authenticated testing identifies vulnerabilities and weaknesses in functionality that are only available to valid, authenticated users. Since most applications commonly limit anonymous access and provide the majority of their functionality to authenticated users, authenticated testing often provides the best insight into the security posture of the systems in scope.

Remediation Verification

Remediation verification was performed using an updated system version. All previously identified findings from the initial assessment were validated to confirm if successful remediation had occurred.

Scope Overview

The scope of the assessment included the following assets as authorized by American Book Company:

```
https://audit.coursewave.com
https://audit-direct.coursewave.com
https://coursewave-audit.us-east-1.elasticbeanstalk.com
```

Timeframe

The Web Application Security Assessment was performed on the dates between **Monday, October 20, 2025,** and **Monday, October 27, 2025.**

Remediation Verification was performed on **Wednesday, January 28, 2026.**

Limitations

Denial-of-service (DoS) testing was not performed during this engagement.

This was a time-boxed security assessment. During a time-boxed engagement, the Cyber Security Team prioritizes assessment of the most sensitive portions and functions of the systems in scope.

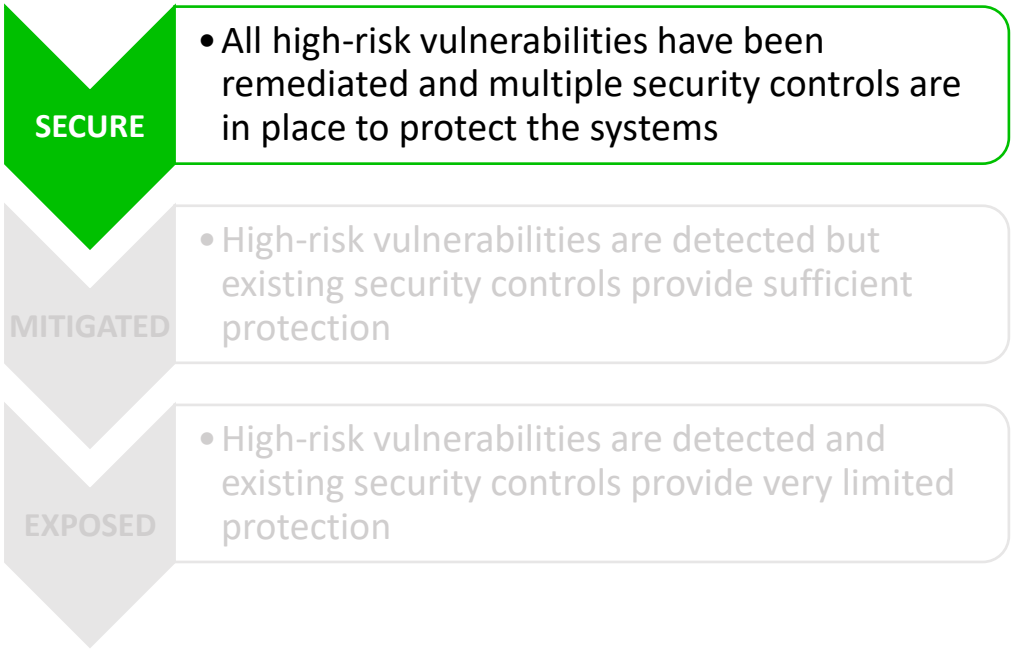
No other specific limitations were defined in the scoping phase by the client.

Summary of Findings

This section documents the results of the Web Application Security Assessment and remediation verification conducted for American Book Company. The security assessment was conducted by Cyberglobal's certified security engineers.

The Security team identified several security vulnerabilities and provided remediation advice to American Book Company.

After being notified by American Book Company that all vulnerabilities had been remediated, Cyberglobal performed a remediation test on Wednesday, January 28, 2026, and confirmed that all findings identified were either corrected or had been adequately addressed through other controls.



Identified Security Controls

Security Control in place	State
Strong Password Policy and Secure Authentication Enforced	**Good Practice**
User Enumeration Prevention Fully Implemented	**Good Practice**
Broken Access Control Strictly Enforced	**Good Practice**
Injection Prevention with Input Validation	**Good Practice**
Security Misconfiguration Hardening in Place	**Good Practice**
Secure Transport and Sensitive Data Protection Enforced	**Good Practice**

Final Statement

As a result of conducting this engagement and remediation verification, Cyberglobal has determined that cumulatively, the vulnerabilities identified pose a **Low** risk to CourseWave. While no application or system can be 100% secure, all the security findings were corrected or addressed, and it is confirmed that the systems in scope are reasonably well written from a security perspective, and the supporting systems are deployed, configured, and implemented securely.