

■■ Security Audit Framework Report

Target: <https://bblearn.londonmet.ac.uk/ultra/stream>

Scan Mode: quick

Generated: 2026-02-22T20:25:37.443017Z

■ EXECUTIVE SUMMARY

OVERALL GRADE	Grade.D (66.7%)
Total Checks	12
Passed	8
High Risk Issues	1

Risk Level: ■ HIGH RISK

■ APP LAYER FINDINGS

ID	Check	Status	Severity	Details
APP-DEBUG-001	Debug mode disabled	■ Status.PASS	Severity.HIGH	No obvious debug/traceback content in root response.
APP-COOKIE-001	Secure session cookies	■ Status.PASS	Severity.HIGH	At least one cookie appears to use both Secure and HttpOnly flags.
APP-CSRF-001	CSRF protection enabled	■ Status.PASS	Severity.MEDIUM	CSRF patterns detected.
APP-ADMIN-001	No exposed admin endpoints	■ Status.FAIL	Severity.MEDIUM	Admin paths exposed: /admin, /debug, /test, /wp-admin.
APP-RATE-001	Rate limiting configured	■■ Status.WARN	Severity.MEDIUM	Rate limiting not evident.
APP-PASS-001	Strong password policy	■ Status.PASS	Severity.LOW	Password hints: 3/5 complexity requirements met.

■ WEB SERVER LAYER FINDINGS

ID	Check	Status	Severity	Details
WS-HSTS-001	HSTS header enabled	■ Status.PASS	Severity.HIGH	HSTS present with strong max-age=63072000.
WS-SEC-001	Security headers present	■ Status.PASS	Severity.HIGH	3/4 security headers present: ['Access-Control-Allow-Origin', 'Content-Security-Policy', 'X-Content-Type-Options', 'X-XSS-Protection']
WS-TLS-001	TLS 1.2+ with strong ciphers	■■ Status.WARN	Severity.HIGH	TLS details unavailable or legacy cipher detected.
WS-SRV-001	No server version disclosure	■ Status.PASS	Severity.MEDIUM	No server version disclosure detected.
WS-DIR-001	Directory listing disabled	■ Status.PASS	Severity.MEDIUM	Directory listing disabled.
WS-LIMIT-001	Request size limits	■■ Status.WARN	Severity.LOW	No direct request limit test available. Content-Length header present.

■■ PRIORITY REMEDIATION

Priority	Issue	Recommended Fix
#1	WS-TLS-001: TLS 1.2+ with strong ciphers	TLS details unavailable or legacy cipher detected.