Security Audit Framework

Security Audit Report

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

Scan Mode: full

Generated: 2026-02-23T18:06:23.525363Z

Executive Summary

Grade F

Score	33.3%
Passed	8 / 24
High Risk	5

Attack Surface Heatmap

Layer	Pass Rate	Status	Risk
Web App	66.7% (4/6)	■	MEDIUM
Web Server	66.7% (4/6)	■	MEDIUM
Container	0.0% (0/6)	■	HIGH
Host	0.0% (0/6)	■	HIGH

Configuration Drift vs Hardened Flask LMS

Grade Delta	Grade.F vs A
Pass Delta	-14 checks vs baseline
Improved Checks	None
Regressed Checks	APP-ADMIN-001, APP-RATE-001, WS-TLS-001, WS-LIMIT-001, CONT-USER-001, CONT-PORT

APP Layer Findings

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

WEBSERVER Layer Findings

ID	Check	Status	Severity	Details
WS-HSTS-001	HSTS header enabled	PASS	Severity.HIGH	HSTS present with strong max-age=63072000.
WS-SEC-001	Security headers present	PASS	Severity.HIGH	3/4 security headers present: ['Access-Control-Allow-Origin', 'Cache-Control', 'Content-Encoding', ' Content-Security-Policy', ' Content-Type', 'Date', ' Expires', 'Last-Modified', ' P3P', 'Pragma', ' Set-Cookie', 'Strict-Transport-Security', 'Vary', ' X-Blackboard-appserver', ' X-Blackboard-product', ' X-Blackboard-Ultra-Version', 'X-Content-Type-Options', ' X-Frame-Options', ' transfer-encoding', ' Connection']
WS-TLS-001	TLS 1.2+ with strong ciphers	WARN	Severity.HIGH	TLS details unavailable or legacy cipher detected
WS-SRV-001	No server version disclosure	PASS	Severity.MEDIUM	Server: . No common server fingerprint detected.
WS-DIR-001	Directory listing disabled	PASS	Severity.MEDIUM	Directory listing disabled
WS-LIMIT-001	Request size limits	WARN	Severity.LOW	No direct request limit test available. Content-Length: 0

CONTAINER Layer Findings

ID	Check	Status	Severity	Details
CONT-USER-001	Non-root container user	WARN	Severity.HIGH	Pending Docker API - requires 'docker inspect' to check USER directive
CONT-PORT-001	Minimal ports exposed	WARN	Severity.MEDIUM	Pending Docker API - requires 'docker ps' to check port bindings
CONT-RES-001	Resource limits configured	WARN	Severity.MEDIUM	Pending Docker API - requires docker-compose.yml CPU/memory limits check
CONT-HEALTH-001	Health checks configured	WARN	Severity.LOW	Pending Docker API - requires Dockerfile HEALTHCHECK directive
CONT-REG-001	Trusted image registry	WARN	Severity.MEDIUM	Pending Docker API - requires image source validation
CONT-SEC-001	No hardcoded secrets	WARN	Severity.CRITICAL	Pending file parsing - requires docker-compose.yml secret scanning

HOST Layer Findings

ID	Check	Status	Severity	Details
HOST-SSH-001	SSH hardened configuration	WARN	Severity.HIGH	Pending SSH connection - requires 'cat /etc/ssh/sshd_config | grep PermitRootLogin' (should be 'no')
HOST-SVC-001	No unnecessary services	WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl list-units --type=service --state=running' to check for risky services
HOST-UPDATE-001	Automatic security updates	WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl is-enabled unattended-upgrades' (should be 'enabled')
HOST-PERM-001	Correct file permissions	WARN	Severity.HIGH	Pending SSH - requires 'find /etc -perm -o+w -ls 2>/dev/null' (no world-writable files)
HOST-FW-001	Firewall configured	WARN	Severity.HIGH	Pending SSH - requires 'ufw status' or 'iptables -L' (firewall should be active)
HOST-LOG-001	Logging and monitoring	WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl is-active rsyslog' and '/var/log/auth.log' writable

Critical Attack Paths

#	Attack Path	Risk	Score
1	Web → Container Escape	HIGH	8.5
2	Server → Internal Services	MEDIUM	6.5

2 attack path(s) identified. Remediate highest-score paths first.

Server Fingerprint

Detected Stack	Docker
Inference Method	HTTP headers, framework behaviours, container/host findings