INFORME DE CIBERSEGURIDAD

Análisis de Seguridad

Campus Virtual PUCMM

`campusvirtual.pucmm.edu.do/moodle/`

Analista	Steven Capellán
Fecha	07 de mayo de 2026 — 4.a revisión
Asignatura	Análisis Forense Digital · 5.o Periodo
Universidad	Pontificia Universidad Católica Madre y Maestra
Clasificación	CONFIDENCIAL — Uso académico exclusivo

Herramienta	Resultado	Severidad
Mozilla Observatory	F · 20 / 100	CRÍTICO
WAVE Accessibility	AIM 3.1 / 10	CRÍTICO
SSL Labs	Nota B	MEDIO
W3C HTML Validator	Múltiples errores	ALTO
Headers HTTP (curl)	5 ausentes	ALTO

01

Resumen Ejecutivo

El presente informe documenta el análisis de seguridad pasivo realizado sobre el Campus Virtual de la Pontificia Universidad Católica Madre y Maestra (PUCMM), específicamente sobre el portal Moodle disponible en campusvirtual.pucmm.edu.do/moodle/. El análisis fue llevado a cabo mediante herramientas de inspección no intrusiva, sin interacción activa ni explotación de vulnerabilidades.

Se identificaron vulnerabilidades de severidad crítica, alta y media distribuidas en cinco áreas: configuración de cabeceras HTTP, protocolo TLS/SSL, accesibilidad web, calidad del código HTML y exposición de información del servidor.

La plataforma obtuvo una calificación de F (20/100) en Mozilla Observatory y B en SSL Labs, indicando deficiencias significativas que deben ser atendidas con prioridad. La buena noticia es que la mayoría de los hallazgos son corregibles mediante cambios de configuración sin modificar el código fuente de Moodle.

2	Vulnerabilidades de severidad CRÍTICA
3	Vulnerabilidades de severidad ALTA
3	Vulnerabilidades de severidad MEDIA
8	Total de hallazgos documentados

02

Stack Tecnológico Identificado

La inspección de cabeceras HTTP mediante el comando curl -I reveló la siguiente infraestructura de servidor:

Componente	Versión / Valor	Observación
Servidor Web	Apache/2.4.62	Versión exacta expuesta — información sensible
Sistema Operativo	Rocky Linux	Derivado de RHEL — entorno empresarial estable
SSL/TLS	OpenSSL 3.2.2	Versión moderna, no representa riesgo
Backend	PHP/8.2.30	Versión exacta expuesta via X-Powered-By
LMS	Moodle	Identificado por cookie MoodleSession
Load Balancer	F5 BIG-IP	Detectado via cookie BIGipServerSDTO-WEB
Idioma	es-mx	Content-Language: español México

03

Vulnerabilidades Identificadas

VUL-001 Content-Security-Policy (CSP) Ausente — CRÍTICO

La ausencia de una política CSP permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso desde dominios externos. Un atacante podría ejecutar scripts arbitrarios en el navegador de usuarios autenticados y robar credenciales o sesiones.

Evidencia: `curl -I: Content-Security-Policy no presente en la respuesta HTTP`

Penalización: –25 pts · Mozilla Observatory

VUL-002 Cookie MoodleSession sin Flag HttpOnly — CRÍTICO

La cookie de sesión principal posee el flag Secure (solo viaja por HTTPS) pero carece del flag HttpOnly, lo que la expone al acceso desde JavaScript. En combinación con un XSS exitoso, permite secuestro de sesión de cualquier usuario autenticado, incluidos administradores.

Evidencia: `Set-Cookie: MoodleSession=...; path=/moodle/; secure (falta HttpOnly)`

Penalización: –30 pts · Mozilla Observatory

VUL-003 TLS 1.0 y TLS 1.1 Habilitados — TLS 1.3 Ausente — ALTO

TLS 1.0 y 1.1 fueron declarados obsoletos por el IETF en RFC 8996 (marzo 2021). Son vulnerables a ataques BEAST y POODLE. Adicionalmente, la ausencia de TLS 1.3 impide aprovechar las mejoras de rendimiento y seguridad del protocolo más moderno.

Evidencia: `SSL Labs Report: TLS 1.0 activo · TLS 1.1 activo · TLS 1.3 no soportado`

Penalización: SSL Labs: Nota B en lugar de A

VUL-004 Strict-Transport-Security (HSTS) Ausente — ALTO

Sin HSTS, el navegador no fuerza HTTPS en visitas subsecuentes. Esto posibilita ataques SSL Stripping donde un adversario en posición de red intermedia puede degradar la conexión a HTTP plano, exponiéndola a interceptación y manipulación de tráfico.

Evidencia: `curl -I: Header Strict-Transport-Security no presente`

Penalización: –20 pts · Mozilla Observatory

VUL-005 Exposición de Versiones de Servidor — MEDIO

Los headers Server y X-Powered-By revelan las versiones exactas de Apache y PHP. Esta información permite a un atacante identificar CVEs específicos para esas versiones y preparar ataques dirigidos sin necesidad de técnicas activas de reconocimiento.

Evidencia: `Server: Apache/2.4.62 (Rocky Linux) OpenSSL/3.2.2 X-Powered-By: PHP/8.2.30`

Penalización: Fingerprinting facilitado

VUL-006 **X-Content-Type-Options Ausente** MEDIO

Sin este header, los navegadores pueden interpretar archivos con MIME type incorrecto (MIME sniffing). Esto facilita ataques en los que un archivo subido por un usuario malicioso es ejecutado como script en lugar de descargarse como dato.

Evidencia: `curl -I: Header X-Content-Type-Options no presente`

Penalización: –5 pts · Mozilla Observatory

VUL-007 **Referrer-Policy y Permissions-Policy Ausentes** MEDIO

La ausencia de Referrer-Policy puede filtrar URLs internas sensibles a sitios de terceros mediante la cabecera Referer. La ausencia de Permissions-Policy permite a scripts embebidos solicitar acceso a APIs del navegador (geolocalización, micrófono, cámara) sin restricción explícita.

Evidencia: `curl -I: Ninguno de estos headers presente en la respuesta`

Penalización: Postura de seguridad degradada

VUL-008 **Accesibilidad Web Deficiente — WCAG 2.1** CRÍTICO

El análisis con WAVE reveló 21 errores de accesibilidad, 38 errores de contraste de color, 34 alertas y 208 problemas ARIA. Esto viola estándares WCAG 2.1 y puede representar incumplimiento de regulaciones de accesibilidad, además de excluir a usuarios con discapacidad visual o motora.

Evidencia: `WAVE Tool: wave.webaim.org/report#/campusvirtual.pucmm.edu.do/moodle/`

Penalización: WAVE AIM Score: 3.1 / 10

04

Recomendaciones

Las siguientes recomendaciones están ordenadas por prioridad. Las marcadas como INMEDIATA pueden implementarse en menos de una hora sin afectar la funcionalidad de la plataforma.

R-01	**Implementar Content-Security-Policy**	**INMEDIATA**

Configurar una política CSP en Apache via mod_headers. Comenzar con default-src 'self' y expandir progresivamente. Esto resuelve VUL-001 y mejora +25 pts en Observatory.

R-02	**Agregar HttpOnly a MoodleSession**	**INMEDIATA**

En config.php de Moodle: $CFG->cookiehttponly = true; Alternativamente en Apache: Header edit Set-Cookie ^(.*)$ "$1; HttpOnly". Resuelve VUL-002 y mejora +30 pts en Observatory.

R-03	**Habilitar HSTS**	**INMEDIATA**

Agregar: Strict-Transport-Security: max-age=31536000; includeSubDomains. Resuelve VUL-004 y mejora +20 pts en Observatory.

R-04	**Deshabilitar TLS 1.0/1.1 y habilitar TLS 1.3**	**CORTO PLAZO**

En Apache/OpenSSL: SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.3. Elevaría la nota de SSL Labs de B a A. Resuelve VUL-003.

R-05	**Ocultar versiones de servidor**	**CORTO PLAZO**

Apache: ServerTokens Prod + ServerSignature Off. PHP: expose_php = Off en php.ini. Elimina Server detallado y X-Powered-By. Resuelve VUL-005.

R-06	**Agregar headers de seguridad faltantes**	**CORTO PLAZO**

X-Content-Type-Options: nosniff · Referrer-Policy: strict-origin-when-cross-origin · Permissions-Policy: geolocation=(), microphone=(), camera=(). Resuelve VUL-006 y VUL-007.

R-07	**Auditoría de accesibilidad WCAG 2.1**	**MEDIANO PLAZO**

Corregir los 21 errores WAVE priorizando: imágenes sin atributo alt, contraste de color insuficiente y etiquetas ARIA malformadas. Meta: alcanzar conformidad WCAG 2.1 nivel AA. Resuelve VUL-008.

05

Herramientas Utilizadas

Herramienta	Acceso	Propósito
curl -I	`Terminal (CLI)`	Inspección directa de cabeceras HTTP de respuesta
Mozilla Observatory	`observatory.mozilla.org`	Auditoría automatizada de headers de seguridad
SSL Labs	`ssllabs.com/ssltest`	Análisis de configuración TLS/SSL del servidor
WAVE	`wave.webaim.org`	Evaluación de accesibilidad web (WCAG 2.1)
W3C Nu HTML Checker	`validator.w3.org`	Validación de markup HTML5

06

Conclusión

El Campus Virtual de la PUCMM presenta una infraestructura de servidor sólida (Apache sobre Rocky Linux, F5 BIG-IP como balanceador, OpenSSL 3.2.2) pero con deficiencias importantes en su configuración de seguridad HTTP y accesibilidad web.

Los hallazgos de mayor criticidad (VUL-001, VUL-002, VUL-004) son corregibles mediante cambios de configuración de Apache en cuestión de minutos, sin requerir modificaciones al código fuente de Moodle ni intervención del proveedor. La implementación de las recomendaciones R-01 a R-03 elevaría la puntuación de Mozilla Observatory de F (20/100) a aproximadamente A (90+/100).

Se recomienda establecer un ciclo de revisión periódica de headers HTTP y configuración TLS, considerando que el panorama de amenazas evoluciona continuamente y plataformas educativas son objetivos frecuentes dado el volumen de datos de estudiantes que manejan.