Ciencia Latina Revista Científica Multidisciplinar
Julio-Agosto, 2023, Volumen 7, Número 4.
https://doi.org/10.37811/cl_rcm.v7i4.6884

Seguridad en la plataforma moodle, utilizada por los Institutos Superiores Tecnológicos públicos del Ecuador

Carlos Bladimir Moreano Guerra [1]
moreanocarlos1@gmail.com
http://orcid.org/0000-0001-9554-8420
Universidad Central del Ecuador

Gisella Brigitte Huera Páez
gbhuerapaez@gmail.com
https://orcid.org/0009-0004-0291-1323
Universidad Politécnica Salesiana UPS

Celia Marisol Pesántez Huanga
cemary_01@hotmail.com
https://orcid.org/0000-0001-8953-0945
Universidad Internacional de la Rioja

Franco Rocha Yadira Guissela
yady10@hotmail.com
https://orcid.org/0009-0009-9196-4078
Universidad de los Hemisferios

RESUMEN

La investigación aborda un diagnóstico de los niveles de seguridad en el trabajo desarrollado en la plataforma Moodle como herramienta principal utilizada en los institutos superiores de educación para el desarrollo de las clases virtuales. Se orientó a identificar deficiencias y vulnerabilidades, que presenta el sistema, para proponer alertas a la comunidad educativa y, con el propósito de que los usuarios, principalmente profesores y tutores puedan tener la certeza de que su información está debidamente protegida. Se realizó experimentos con pruebas en aulas simuladas en el Instituto Superior Tecnológico Sucre determinando algunos tipos de amenazas que ponen en riesgo la accesibilidad y los contenidos de los cursos de las asignaturas dictadas por los profesores. Se encontró que el cambio de rol se puede realizar con relativa facilidad entre los diferentes niveles de usuarios, se puede pasar de estudiante a profesor, estudiante a gestor, y de profesor a gestor o administrador; con esto el estudiante puede tener acceso a los cuestionarios, bancos de preguntas y a las calificaciones almacenadas dentro del aula virtual. Se concluye que el mismo sitio web utilizado por Moodle para la recopilación de fallos puede ser atractivo para los crackers, ellos dispondrían de un período de tiempo para su explotación en perjuicio de los usuarios, mientras se soluciona el problema; cuanto más antigua sea la versión tanto más probable que tenga vulnerabilidades, requiriéndose de una continua actualización y del establecimiento de controles preventivos.

Palabras clave: *Plataforma Moodle; Seguridad en Moodle; Aulas virtuales; vulnerabilidades en EVA.*

[1] Autor Principal

Security in the moodle platform, used by public Higher Technological Institutes of Ecuador

ABSTRACT

The research addresses a diagnosis of safety levels at work developed on the Moodle platform as the main tool used in higher education institutes for the development of virtual classes. It was aimed at identifying deficiencies and vulnerabilities, which the system presents, to propose alerts to the educational community and, with the purpose that users, mainly teachers and tutors, can be sure that their information is properly protected. Experiments were carried out with tests in simulated classrooms at the Sucre Superior Technological Institute, determining some types of threats that put at risk the accessibility and content of the courses of the subjects taught by the teachers it can be found that the change of role can be carried out with relative ease between the different levels of users, it can be passed from student to teacher, student to manager, and from teacher to manager or administrator; With this, the student can have access to the questionnaires, question banks and the grades stored within the virtual classroom. It is concluded that the same website used by Moodle to collect bugs can be attractive to crackers, they would have a period of time to exploit it to the detriment of users, while the problem is solved; the older the version, the more likely it is to have vulnerabilities, requiring continuous updating and the establishment of preventive controls.

Keywords: *Moodle platform; Moodle security; virtual classrooms; vulnerabilities in EVA.*

Artículo recibido 05 junio 2023
Aceptado para publicación: 05 julio 2023

INTRODUCCIÓN

La pandemia generada por el covid-19 ocasionó cambios súbitos a todo nivel. El nivel educativo no estuvo exento. El sistema educativo del país tuvo que adaptarse a las nuevas circunstancias de la vida, en especial al confinamiento y la necesidad imprescindible del distanciamiento, direccionándose a una modalidad de educación virtual.

A nivel de la educación superior y particularmente de los institutos superiores tecnológicos públicos que brindan clases virtuales, en lugar de clases presenciales. El pasaje del ámbito presencial al virtual fue rápido, "implico una rápida adaptación de docentes y estudiantes al uso de distintas herramientas tecnológicas" (Carabelli, 2020)

El uso del entorno virtual de aprendizaje se popularizó, con el objetivo de llevar adelante los procesos de aprendizaje, para este fin se escogieron algunas plataformas, entre ellas el Moodle, como complemento de la clase virtual online, generada en reuniones académicas a través de la utilización de servicios de videoconferencia como zoom, meet, Skype, entre algunas.

La realidad virtual introdujo nuevas formas de comprender el proceso educativo y produjo nuevos cuestionamientos como: ¿Qué tipo de aprendizaje genera la educación virtual? Y ¿Cuáles son las problemáticas sociales que surgen de este tipo de realidades virtuales? (Floralba, 2020)

"El uso de las tecnologías en la educación ha contribuido a una evolución mental e imaginativa de los estudiantes, permitiéndoles observar otros sistemas, culturas, literaturas, lugares, entre otros, diferentes al que pueden conocer en su entorno. Es así como las diferentes herramientas que ofrece la tecnología educativa permiten, a través de la conexión a internet, hacer un aprendizaje más fácil y moderno." (Millan, 2018)

El aprendizaje en las aulas virtuales ha generado cambios en el proceso de aprendizaje de los estudiantes, en los roles de los actores, en la planificación, en los contenidos, material didáctico y en la evaluación de los resultados alcanzados. Los retos que se van superando han sido grandes, uno de ellos es la amplia brecha generacional, (Innovación Tecnológica en la Educación, 2020) "el analfabeto digital (docente) debe enseñar al erudito tecnológico del siglo XXI (estudiante). Otro de

los retos lo constituye la disponibilidad de los recursos de las instituciones y de los estudiantes, y las deficiencias a ser superadas en los entornos virtuales de aprendizaje enmarcadas en la seguridad"

"Las plataformas de formación virtual son consideradas por el profesorado como herramientas tecnológicas con fuertes potencialidades didácticas." (Del Prete & Almenara, 2019)

Una de las herramientas más difundidas y utilizadas es el Moodle, siendo preferido como entorno virtual de aprendizaje por su flexibilidad, la cual está pensado sobre la pedagogía del constructivismo social. (Juca, 2016)

La palabra Moodle es el acrónimo de Modular Object Oriented Dynamic Learning Environment (Ambiente de Aprendizaje Modular Orientado a Objetos Dinámicos). Es una plataforma de software libre. Su diseño es modular lo que permite agregar o quitar módulos dependiendo de lo que se desee. Es la plataforma educativa más difundida y utilizada. (Juca, B-learning y Moodle como estrategia en la educación universitaria, 2020)

Los resultados de evaluación del aprendizaje no deben ser distorsionados como consecuencia de las debilidades de seguridad en la plataforma Moodle utilizada. El docente competente en un mundo mediado por la tecnología requiere estar consciente de la vulnerabilidad digital, del empoderamiento crítico y de desarrollar su capacidad técnica guiada por el buen juicio para mitigar el impacto negativo (Alvarez, 2021) y ser responsable de sus interacciones en Internet que podrían ser perjudiciales para su seguridad o bienestar físico, psicológico y social.

Esta investigación se direcciona a identificar a través de pruebas experimentales aplicadas en el Instituto tecnológico Sucre las posibles deficiencias en la utilización de la plataforma Moodle con el propósito de alertar a los docentes en la toma de acciones que permitan disminuir estos riesgos.

DESARROLLO

Se ha realizado una investigación exhaustiva del tema y se a continuación se cita material utilizado.

Consideraciones sobre la seguridad de la Plataforma Moodle

La plataforma Moodle se encuentra actualizándose constantemente para corregir posibles vulnerabilidades y los llamados agujeros de seguridad para lo que ha puesto a disposición el link :

http://moodle.org/security/ , en el que se presentan informes de seguridad, se alimenta de posibles errores y se proporciona alternativas y recomendaciones de seguridad. Resulta importante primero identificar el problema para buscar una solución.

Los últimos anuncios presentados por esta plataforma indican que:

La biblioteca PHP H5P incluida con Moodle se ha actualizado a la última versión menor que incluye una corrección de seguridad

Severidad / Riesgo: Grave

Versiones afectadas: 3.10 a 3.10.3, 3.9 a 3.9.6 y 3.8 a 3.8.8

Versiones arregladas: 3.11, 3.10.4, 3.9.7 y 3.8.9

Reportado por: Sara Arjona

Identificador CVE: N/A

Cambios (maestro): http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-71408

Problema del rastreador: MDL-71408 Actualizar la biblioteca PHP H5P a la última versión secundaria (upstream). (Moodle, 2021)

La plataforma Moodle cuenta con niveles de seguridad que pueden establecerse en el servidor que se instala en la aplicación. La responsabilidad de la seguridad radica en el administrador principal, las configuraciones básicas en los niveles más dedicados están dados en: Servidor, autentificación, contraseñas y roles.

Seguridad en el servidor

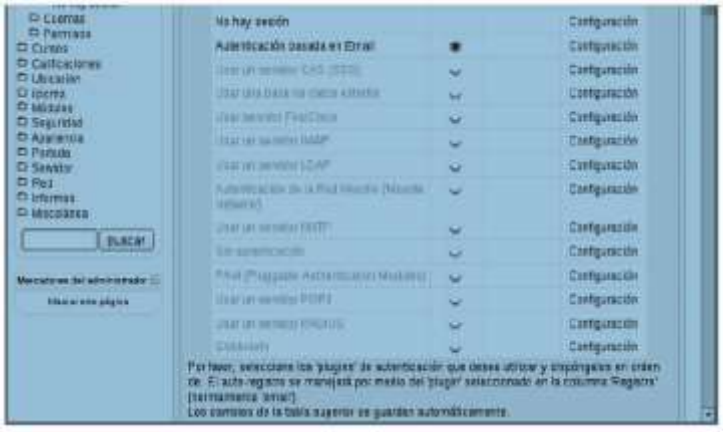
La seguridad del servidor le compete al administrador del sistema, se debe prever los controles básicos como:

Seguridad en la autentificación.

En primera instancia se debe decidir cuál será el método utilizado para la autenticación de los usuarios en la red Wi-Fi®, utilizando como protocolo de seguridad WPA2-Enterprise. Se recomienda por lo comentado anteriormente la utilización de EAP-TLS, además de si se requiere de autenticación de usuario y contraseña, EAP-TTLS, utilizando el controlador de dominio como origen de los datos. (Dominguez Vega, 2018)

La autentificación es un paso dentro del proceso de identificación – autentificación en el que se determina si un usuario o entidad puede tener acceso a un sistema o recurso. Los métodos de autentificación se clasifican en 5 tipos: los basados en un toke (algo que el usuario posee), los basados en información biométrica (algo que el usuario es), los basados en conocimiento (algo que el usuario conoce), la ubicación (direcciones IP y los sistemas híbridos. (Osviel Rodriguez, 2018)

Figura 1: *Pantalla de gestión de autenticidad.*



Fuente: pruebas realizadas en aulas de Moodle del IST.Sucre

Seguridad en contraseñas.

Las contraseñas se originan en el método de autentificación que está basado en el conocimiento que posee el usuario. Estas tienden a no ser seguras y presentar vulnerabilidades, debido a que muy pocas veces los usuarios siguen las recomendaciones para establecer alguna clave. Los usuarios casi siempre ignoran las recomendaciones para la confección de claves seguras, estas tienden a ser cortas y poco aleatorias. (Revista Cubana de Ciencias Informáticas, 2018) Existen muchas técnicas y herramientas

que aprovechan estas vulnerabilidades y de una manera relativamente fácil permiten obtener una contraseña. Lamentablemente estas pueden ser fácilmente aplicadas o atacadas.

No hay un estándar para la configuración de las contraseñas, pero se han establecido algunas recomendaciones como:

Una longitud mínima de 8 caracteres

Incluir en la contraseña números, letras y caracteres especiales, incluir mayúsculas y minúsculas.

Desde la aplicación se pueden considerar estándares para delinear las condiciones que debe tener una contraseña. Como definir número de caracteres, posiciones de mayúsculas y minúsculas, números y caracteres especiales. Se configuran desde la sección administración – seguridad.

Figura 2: Pantalla de gestión de autenticidad

Fuente: pruebas realizadas en aulas de Moodle del IST.Sucre

Seguridad en Roles.

En la plataforma Moodle los accesos se encuentran asignados a través de privelegios, que permite acceder a contenidos, recursos, tareas, calificaciones, que se maneja como permisos de los usuarios, se determina, qué es lo que puede hacer un usuario y qué es lo que no puede hacer.

Moodle tiene configurado siete roles basados en el nivel de permiso para realizar las actividades en la plataforma: Administrador, Creador de Cursos, Profesor, Profesor no Editor, Estudiante, Invitado e Usuario Autentificado.

Cada rol se puede asignar de forma global y también de forma específica para cada curso, los permisos de los roles son heredados. Por ejemplo, si tenemos permisos de Creador de Cursos de rol global podemos tener también el rol de Estudiante en un curso determinado, teniendo los permisos de Estudiante en el curso y los permisos heredados de Creador de Cursos que no sean incompatibles entre ellos.

Calendario de liberaciones.

Estas son las fechas esperadas para liberación.

Después de los lanzamientos importantes, habrá lanzamientos menores.

xx1 ocurrirá aproximadamente dos meses después de cada versión principal (por ejemplo, 2.x).

Luego, habrá otro lanzamiento de puntos cada dos meses.

Todas las liberaciones son precedidas por una advertencia previa de una semana.

Estas fechas pueden variar ligeramente debido a circunstancias no previstas.

Planteamiento del problema

La pandemia generada por el covid-19 ocasionó cambios súbitos a todo nivel. El nivel educativo no estuvo exento. El sistema educativo del país tuvo que adaptarse a las nuevas circunstancias de la vida, en especial al confinamiento y la necesidad imprescindible del distanciamiento, direccionándose a una modalidad de educación virtual.

Las IES se vieron abligadas a buscar opciones de mantener un contacto con los estudiantes a fin de continuar garantizando una educación de calidad; por lo cual, la mayor parte de los institutos del Ecuador se acogieron a la pataforma virtual Moodle como medio de interacción entre estudiante-docente, pero en no al no contar con los recursos y conocimientos adeuados algunos de ellos no han podido actualizar las versiones de esta paltaforma, por lo cual algunos estudiantes acceden a la información privada, vulnerando las seguridades de accesos de usurios que la plataforma mantiene en sus versiones.

METODOLOGÍA

La investigación se basó en una metodología cualitativa descriptiva y exploratoria en la que se modeló la propuesta partiendo de los resultados obtenidos en las pruebas de las aulas simuladas, que se llevó adelante en el Instituto Superior tecnológico Sucre.

El estudio se enfocó en dos aspectos:

La seguridad tanto en contenidos como en accesibilidad de la información procesada a través de la plataforma Moodle. Para su determinación se levantó información a través de una encuesta dirigida a todos los docentes de Institutos Superiores tecnológicos del sector público, quienes utilizan esta herramienta. Se buscó la formalización de la investigación logrando el apoyo de la Subsecretaria de la Secretaría de Educación Superior, Ciencia y Tecnología (Senescyt), organismo a través del cuál se enviaron las encuestas.

Para la determinación de las deficiencias del entorno Moodle se realizó experimentos con pruebas en aulas simuladas en el Instituto Superior Tecnológico Sucre determinando algunos tipos de amenazas que ponen en riesgo la accesibilidad y los contenidos de los cursos de las asignaturas dictadas por los docentes. En la ejecución de las pruebas se consideró dos puntos resumidos en la intencionalidad, por un lado, las amenazas provocadas por los ataques cibernéticos y por otro los errores y descuidos que cometen los propios usuarios de la plataforma Moodle.

Recolección de datos

Se realizó una encuesta a los institutos del Ecuador, a fin de conocer sobre las versiones y vulnerabilidades detectadas en las plataformas utilizadas.

Tabla 1: *Tabulación de datos recolectados*

PREGUNTA	Opciones	Datos obtenidos	Representación en porcentaje
Estudiantes matriculados en el periodo actual en el instituto	0-300	11	17%
	301-600	4	6%
	601-1000	44	69%
	Mas 100	5	8%
¿Qué plataforma de entorno virtual utilizan actualmente en la institución?	Classroom	4	6%
	Moodle	55	86%
	Schoology	1	2%
	Otros	4	6%
¿Qué plataforma de entorno virtual utilizan actualmente en la institución?	Moodle 2.0	1	1,6%
	Moodle 3.1	2	3,1%
	Moodle 3.10	1	1,6%
	Moodle 3.10.4	3	4,7%
	Moodle 3.3	1	1,6%
	Moodle 3.6.5	39	60,9%
	Moodle 3.5.0	1	1,6%
	Cloudlinux 7.8	1	1,6%
	Google Workspace 2021	1	1,6%
	Moodle 3.10+	1	1,6%
	(Build:20201204)	1	1,6%
	Moodle 3.7	2	3,1%
	Riolearning	1	1,6%
	Version 3.8	2	3,1%
	Moodle 3.6	2	3,1%
	Moodle 3.9	2	3,1%
	Versiones anteriores	3	4,7%
	Sin respuesta		
¿Ha evidenciado problemas de inseguridad en la plataforma que utiliza?	No	47	73%
	Si	17	27%
¿Qué tipos de problemas de inseguridad ha evidenciado en la plataforma?	Acceso no autorizado al servidor	1	1,6%
	Alguna vez apareció un icono raro en el aula virtual yo di aviso a coordinación y ya cuando ingresaron a revisar desapareció el icono.	1	1,6%
	En una ocasión vi un ícono diferente en el aula di aviso y	1	1,6%

	cuando se ingresó de nuevo desapareció.	33	51,6%
		1	1,6%
	Estudiantes que ingresa con otro numero de cedula.	21	32,8%
		1	1,6%
	Ingreso en el aula virtual.	3	4,7%
	La clave de ingreso se guarda.	1	1,6%
	Ninguno		
	No se cuenta con una plataforma oficial.		
	Problemas de Phishing.		
	Vulneración de base de datos.		
¿Ha sido víctima de hacker en sus aulas virtuales?	No	63	98%
	Si	1	2%
¿Conoce de alguien que ha sido víctima de ataques malicioso en las aulas virtuales?	No	55	86%
	Si	9	14%
¿Se ha tomado medidas preventivas en los problemas de inseguridad detectados en las aulas virtuales?	No	29	45%
	Si	35	55%

Fuente: encuesta aplicada a los institutos. Elaboración propia

El 69% de los institutos que accedieron a la encuesta tienen un número de estudiante matriculados en el periodo actual entre 601 a 1000; 8% tienen una cantidad de matriculados mayor a 1000, lo que se puede deducir que mientras más estudiantes tengan acceso a la plataforma mayor riesgo.

La plataforma de entorno virtual de aprendizaje más utilizadas por los institutos superiores tecnológicos es Moodle, representando un 86% de los institutos a nivel nacional, resultado que nos lleva a sustentar la presente investigación.

El 79,69% de los institutos encuestados están utilizando versiones de la categoría 3.0 a 3.10 dato que permite orientar el trabajo de investigación hacia ese segmento.

El 17% de los encuestados han evidenciado problemas de inseguridad en la utilización de las plataformas LMS. Lo que conlleva a verificar las percepciones.

El 67% ha experimentado algún tipo de problemas; de los cuales el 52% reporta haber identificado accesos no autorizados en el aula.

El 14% sí conoce de alguien que ha sido víctima de ataques maliciosos en las aulas virtuales.

El 45% de los encuestados no han tomado medidas preventivas para disminuir el riesgo de las inseguridades en los entornos virtuales utilizados.

RESULTADOS

Moodle desde su lanzamiento presenta 338 versiones hasta la presente fecha, lo que significa que mantiene un promedio de 19 versiones por año. Existe una constante evolución de la plataforma, ocasionada por mejoras en el programa, fundamentalmente en el aspecto de la seguridad necesario debido a los continuos reportes e informes de novedades de vulnerabilidades que envían sus usuarios. Al generarse el inconveniente se procede a los ajustes correspondientes y se libera una nueva versión que soporta a las anteriores.

El tiempo de respuestas o demora en correcciones de problemas generales se lo hace en 12 meses y la solución de los problemas a través de parches de seguridad se lo realiza en 18 meses y en algunos casos en 36 meses, como es el caso de las versiones 2.7, 3.1 y 3.5, a partir de los reportes de las vulnerabilidades, el procedimiento que se establece es el siguiente: se ha creado un link https://tracker.moodle.org/browse/CONTRIB-8637?filter=-4 al que pueden acceder los usuarios para informar de las dificultades o errores hallados, con esta información se procede a su verificación y rectificación si procede, liberando una nueva versión.

El número de errores considerados como: bajo 235, graves en el tiempo de operatividad de la plataforma Moodle ha sido 140, con el número de vulnerabilidades este período ha sido de las 375 reflejan la necesidad de estar pendientes de las correspondientes actualizaciones con la finalidad de disminuir el riesgo de inseguridad que presentan las anteriores. Una vez publicado el error se presenta la advertencia en el sitio web, que se constituye una pronta a la que todos quienes la utilizamos debemos estar listos para tomar acciones de prevención.

Cambio o acceso no autorizado a los diferentes niveles o roles:

La versión de Moodle empleada por el Instituto Superior Tecnológico Sucre 3.6.5 en las pruebas realizadas presenta deficiencias en cuanto a cambio de roles de los usuarios con las implicaciones que

representa un cambio de un nivel inferior a un cambio de nivel superior, obteniendo mayores privilegios de usuario.

El procedimiento aplicado en la prueba es un ataque denominado escalamiento de privilegios, versión 3,7 de Moodle.

Software: Windows 10

Servidor XAAM

Burp Suite: testing detección hasta 100 vulnerabilidades

Este valor de riesgo es SEVERO.

Las pruebas realizadas permitieron demostrar que se puede modificar los roles de los usuarios de la plataforma Moodle, a través de los siguientes pasos:

Ingreso a Moodle.

Acceso a los cursos y creación de un nuevo usuario con rol o privilegio de profesor, el objetivo es escalar este usuario a gestor:

Abrir el software Burp Suite.

Dar clic en “interception”:

Después crear el usuario y Burp comenzará a rastrear las tramas de datos de Moodle.

Una vez que Burp obtiene conexión con la plataforma Moodle se procede a interceptar el dato del usuario en la sección: Actions-> Send to Repeater

Verificar cuál es el rol del usuario actual, reinyectar el código que se utiliza en el repetidor. El Id. es el número 3 (nivel del rol docente).

Regresar a Burp Suite y buscar la etiqueta “user list” y modificar este valor elevando el privilegio a “1” (nivel de rol gestor) y enviar.

Verificar el usuario creado con privilegio 3 “profesor”.

En Burp suite, nos confirma la modificación “success”.

Por último, se verifica los cambios actualizando la página de Moodle

Confirmar el privilegio modificado a administrador basado en una vulnerabilidad del código del Moodle.

Acceso a evaluaciones o cuestionarios y sus respuestas por código fuente:

A través del código fuente de la página Web en algunas variables se puede verificar el formulario de evaluación, como también, verificar las respuestas de las preguntas.

Esta vulnerabilidad afecta a la versión 3.6.5 que actualmente es utilizada por el Instituto Sucre y puesta en estudio para este caso.

Inyección de código SQL:

Identificar las sentencias SQL que se utilizan para consultar las bases de datos. La base de datos tiene funciones básicas como crear, leer, actualizar y borrar (CRUD), que se constituyen en la base para empezar la inyección.

La alteración del lenguaje de programación SQL es una falla de seguridad informática, lo cual tiene penalidad a nivel legal, siendo un delito informático.

Habiendo explicado esto; queda bajo responsabilidad de las personas realizar esta técnica, siguiendo los siguientes pasos:

Entrar a la página de Moodle.

Instalar Moodle.

Analizar la estructura de la base de datos, buscando identificar el nombre de la tabla y de la base de datos, también un parche que permita saltar al ingreso de seguridad que tiene MYSQL para poder realizar el SCRIPT que permita: leer, actualizar, escribir o eliminar.

Prácticamente se coloca de manera directa en el navegador, una técnica que se basa en inyectar un código en este caso se hará la misma inspección sin embargo se realizará una modificación, dónde se agregará una nueva línea de sentencia de código para que desde el navegador se pueda consultar y hacer una actualización a las claves y al examen.

Habiendo completado esta acción, se puede observar cómo se configura y cómo se maneja una sentencia de lenguaje, la primera sentencia es para consultar un dato que está en la base de datos y la

segunda es para realizar una actualización a ese dato, que se le aplicará en la página web donde está el examen; al aplicarlo se generará un enunciado diciendo que no se puede realizar la consulta porque falta algo muy importante; y es el parche para vulnerar MYSQL y PHP.

A continuación, se explica cómo parchar en la base de datos:

Cuando ya se tiene el acceso directo a la base de datos, se añade la actualización a través de las líneas de código para modificar un examen.

Visualizar respuestas.

Hackeo con software Intercepter

Intercepter: es un software para interceptar paquetes de datos dentro de la red.

Para el efecto se ha seguido los siguientes pasos:

Configurar el intercepter en el dispositivo Android.

Buscar una conexión.

En ese momento el interceptor comienza a rastrear los paquetes que fluyen a través de la red.

A continuación, ingresar los datos de un usuario de Moodle y el software comienza a rastrear el usuario y la contraseña.

Inmediatamente que el usuario ponga la clave el software se rastreará los datos que puso como usuario y contraseña.

Utilizar el usuario y la contraseña obtenida para ingresar de forma no autorizada al Moodle.

Ataque Hacking para aumento de privilegios de Usuario “Estudiante” a “Gestor” en Moodle 3.6.5

Entorno: Prueba en entorno real con hosting y dominio activo.

Ingreso de usuario administrador de la plataforma.

Crear un usuario en Moodle para posteriormente cambiarle los privilegios.

Se sube el BURP SUITE PROFESIONAL, que es la plataforma integrada para la realización de las pruebas de seguridad de las aplicaciones web.

Dar clic en “Proxy” y en “Intercept”

Se activó el browser de BURP SUITE donde se obtiene el tráfico desde el dominio.

Se visualiza el browser de Burp: y se a asigna un curso al usuario a través del browser interceptado.

Activación de lectura del tráfico del dominio con Burp.

Dar clic en “matricular usuario”

Se matriculó en el curso con el Rol “estudiante”

Se puede visualizar la lectura del tráfico. Esta es la sección donde está el código con los datos interceptados del usuario, el cual se asignó al curso.

Enviar el código nuevamente hacia el dominio accediendo a través de una vulnerabilidad del código de Moodle 3.6.5. La sección del código que interesa es donde se puede modificar el privilegio del usuario.

La variable userlist es el ID del usuario, mismo que esta identificado en el Moodle.

La variable roletoassign es el perfil del usuario, en este caso el nivel 5 que corresponde a “estudiante”, esta se va a modificar a “1” que es el privilegio de “gestor”.

Ir al BURP e intentar reenviar el código modificado, a través de la herramienta “Repeater”.

En “Repeater” modificar la variable enrolid con el valor “1” que es gestor.

A continuación, se inyecta el código al Moodle.

Se ha obtenido éxito en la modificación del rol del usuario.

Ingresar con el usuario puesto en estudio y se podrá visualizar que se activaron las opciones de administrador.

Ingresar a la evaluación deseada.

Editar cuestionario.

DISCUSIÓN

El uso de la plataforma Moodle es constante, los requerimientos son continuos, las instituciones educativas y en forma particular los Institutos Superiores Tecnológicos del sector público en el país, conforme se ha evidenciado, utilizan en su mayoría (86%) esta plataforma en sus clases virtuales para el desarrollo de sus actividades educativas de tipo asincrónico y sincrónico, siendo notoriamente las primeras en donde se centra la atención y su utilidad.

En esta época de pandemia, la utilización de la plataforma Moodle se ha difundido en esta área por la propia necesidad de buscar espacios de educación que no involucren el contacto directo entre estudiante y docente, para así reducir los efectos de la pandemia frente al colapso del sistema de salud existente en el país.

La estructura de Moodle ésta dispuesta para que los usuarios puedan acceder y utilizar de acuerdo a sus ámbitos, se establecen de esta forma niveles o roles: los cuales limitan su campo de acción o las facultades que pueden tener cada uno.

Las principales vulnerabilidades encontradas en la plataforma Moodle se centran:

Cambio o acceso no autorizado a los diferentes niveles o roles.

Acceso a evaluaciones o cuestionarios y sus respuestas.

Posible revisión de respuestas por código fuente.

Inyecciones de Código SQL.

Hackeo con software Intercepter.

CONSLUSIONES

De las pruebas realizadas como piloto en las diferentes aulas del Instituto Tecnológico Superior Sucre se pudo determinar que la versión utilizada no ha sido actualizada, por tal motivo está sujeta a varias vulnerabilidades: acceso no autorizado, cambio de roles, acceso no autorizado a cuestionarios y banco de preguntas, ataques de hackers, modificaciones de la configuración de las aulas a través de códigos fuentes; dejando vulnerable a que los roles se puede cambiar con relativa facilidad entre los diferentes niveles de usuarios dentro de la plataforma Moodle, se puede pasar de estudiante a profesor, estudiante a gestor, y de profesor a gestor o administrador; con esto el estudiante puede tener acceso a los cuestionarios, bancos de preguntas y a las calificaciones almacenados dentro del aula virtual para ser modificadas a sus propios intereses. Se concluye que se debe actualizar la plataforma a su última versión o utilizar sistemas de automatización automática.

El estudiante a través de la manipulación del lenguaje de programación SQL y de los códigos fuentes puede tener acceso a los cuestionarios y sus respuestas, incurriendo en un claro delito informático y

vulnerando la seguridad de la plataforma y las aulas virtuales; por lo cual, se hace necesario utilizar Moodle en un servidor propio, evitando un ambiente de alojamiento compartido.

El lanzamiento de las versiones principales se realiza cada seis meses y el lanzamiento de las versiones menores se lo realiza cada dos meses a partir del lanzamiento de la versión principal. Hasta la actualidad existen 338 versiones. Moodle también cuenta con un sitio web para la recolección de fallos que reportan los usuarios, con esta información crea una nueva versión, la cual subsana todos los casos reportados; el mismo sitio web utilizado por Moodle para la recopilación de fallos puede ser atractivo para los crackers, ellos dispondrían de un período de tiempo para su explotación en perjuicio de los usuarios, mientras se soluciona el problema; cuanto más antigua sea la versión tanto más probable que tenga vulnerabilidades.

La plataforma de entorno virtual de aprendizaje más utilizada por los institutos superiores tecnológicos es Moodle, representando un 86% de los institutos a nivel nacional, resultado que nos lleva a sustentar la presente investigación. El 79,69% de los institutos encuestados están utilizando versiones de la categoría 3.0 a 3.10; lo cual significa que están utilizando versiones desactualizadas y que están sujetas a vulnerabilidades de seguridad.

Los institutos no aplican mecanismos de control sobre la seguridad que brinda la plataforma Moodle; reportan que han evidenciado problemas de ingresos no autorizados al aula con números de cédula no vinculados. Por tal motivo, los administradores deben proporcionar cuentas de profesor únicamente a usuarios que se encuentren dentro del proceso de las aulas virtuales; las cuentas de profesor tienen permisos mucho más libres y es más fácil crear situaciones donde sea posible abusar de los datos o robarlos. Se recomienda mantener desactiva la opción del Moodle de acceso a invitados a las diferentes aulas virtuales, así como en el proceso de matriculación de todas las aulas incluir clave de matriculación, asegurándose de que esté deshabilitada la pista para la clave de matriculación (inscripción), lo que debería conservase así por defecto.

Los usuarios estudiados no reportan haber sido víctimas de hackers, situación lejos de considerar que exista seguridad en la plataforma puede generar un mayor riesgo dado que los profesores y

administradores no están prevenidos del caso, evidenciándose en el l 45% de los encuestados que no toman medidas preventivas para disminuir el riesgo de las inseguridades en los entornos virtuales utilizados. A fin de prevenir los ataques de cracker se debe realizar frecuentemente una copia de seguridad de respaldo, verificando los procedimientos de restauración; los profesores y administradores deben utilizar contraseñas fuertes y complejas para proteger contra el cracking; activar o seleccionar la casilla para ser obligatoria la complejidad de la contraseña en los niveles profesor y administrador; activar la opción de intentos fallidos y socializar a los usuarios que se puede intentar el acceso hasta 10 veces, y que pasado los intentos se bloqueará el acceso por el lapso de 15 minutos; activar el programa ReCaptcha para evitar el cracking a través de programas automatizados no autorizados y mantener desactivado la opción de auto registro para evitar que se creen cuentas de acceso falsas.

LISTA DE REFERECIAS

Alvarez, F. E. (febrero de 2021). Uso crítico y seguro de tecnologías digitales de profesores universitarios. La Serena, Universidad Estatal de Sonora, México. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-50062021000100033&lang=es#B26

Carabelli, P. (2020). Respuesta al brote de COVID-19: tiempo de enseñanza virtual. Scielo.

Aguilar, F. (2020). El aprendizaje en escenarios presenciales al aprendizaje virtual en tiempos de pandemia. Scielo.

Floralba, A. (2020). Del aprendizaje en escenarios presenciales al aprendizaje virtual en tiempos de pandemia. Scielo.

Aguiliar, F. (julio de 2020). Innovación Tecnológica en la Educación. Quito: Editorial universitario Abya-Yala. Obtenido de dspace.ups: https://dspace.ups.edu.ec/bitstream/123456789/19314/1/INNOVACIO%CC%81N%20TECNOLO%CC%81GICA%20EN%20LA%20EDUCACIO%CC%81N.pdf

Juca, F. (2016). La educación a distancia, una necesidad para la formación de los profesionales. Scielo, s/p.

Juca, F. (2020). B-learning y Moodle como estrategia en la educación universitaria. Scielo.

Moodle. (2021). Anuncios de Seguridad. Obtenido de moodle.org/security: https://moodle.org/security/,

Millan, J. C. (2018). repositorio.une.edu.pe. Obtenido de une.edu.ec.: https://repositorio.une.edu.pe/bitstream/handle/UNE/4358/Plataformas%20educativas.pdf?sequence=1&isAllowed=y

Del Prete & Almenara. (2019). apertura. Obtenido de Scielo: http://www.scielo.org.mx/pdf/apertura/v11n2/2007-1094-apertura-11-02-138.pdf

Dominguez Vega, L. F. (2018). Montaje y control de una red Wi-Fi® asegurada a nivel empresarial con WPA2-Enterprise. Scielo, s/n.

Revista Cubana de Ciencias Informáticas. (2018). Seguridad y usabilidad de los esquemas y t´ecnicas de autenticaci´on gr´afica. Scielo, s/n.

Osviel Rodriguez, C. L. (2018). Seguridad y usabilidad de los esquemas y t´ecnicas de autenticaci´on gr´afica. Revista Cubana de Ciencias Informáticas, s/n.