ANÁLISIS DE VULNERABILIDADES DE CREDENCIALES DÉBILES O POR DEFECTO EN APLICACIONES WEB LMS (HERRAMIENTAS DE GESTIÓN DE APRENDIZAJE)

Área de Conocimiento Seguridad Informática

Jorge Sánchez Freire[1]
Pamela Parra Zamora[2]

1. Ingeniero en Sistemas Computacionales e Informáticos. Universidad Tecnológica Indoamérica Ambato, *Webmaster* Institucional. Ambato Ecuador. Correo: jorgesanchez@uti.edu.ec
2. Estudiante Universitaria de la Carrera de Ingeniería en Sistemas. Pontificia Universidad Católica del Ecuador. Ambato – Ecuador. Correo: pamela.j.parra.z@pucesa.edu.ec

RESUMEN

En toda aplicación *web* existen riesgos y vulnerabilidades que deben ser mitigados, uno de los más grandes el usuario quien muchas veces para procurar no olvidar sus credenciales de acceso, utiliza las mismas que le fueron otorgadas por los administradores o a su vez fáciles de recordar y adivinar por cualquier persona externa. En el manejo de aplicaciones web por parte de estudiantes y docentes muchas veces se deja de lado la seguridad por parte de los usuarios provocando acceso no deseado a información sensible.

En la presente investigación se realiza un análisis, mediante el uso de la metodología OWASP en su apartado de análisis de vulnerabilidades de usuarios, en el cual se determina la presencia las mismas, ya sea por el uso de credenciales de acceso débiles o por protocolos de seguridad obsoletos. De esta manera se propone posibles soluciones hacia los administradores de la aplicación para disminuir el riesgo de un acceso no autorizado, el cual es presentado en este estudio.

PALABRAS CLAVE

Vulnerabilidades, credenciales, seguridad informática, aplicación *web*.

ABSTRACT

In every web application there are risk and vulnerabilities which have to be mitigated, one of the biggest is the final user itself who, most of the times, in order to don´t forget his access credentials, uses the same ones that the administrator had given to him or uses some easy to remember and to guess by an external person, representing a high vulnerability in a security chain. In web management done by users most of times security is left out causing unwanted access to sensitive information.

This investigation attempts to realize an analysis by using the user's vulnerabilities chapter in the OWASP methodology, which determines the presence this, either by using weak access credentials or because of obsolete security protocols. In that way

solutions can be proposed to the administrators of the application to lower the risk of an unauthorized access which it´s shown in this study.

KEYWORDS

Vulnerabilities, credentials, information security, web application.

1. INTRODUCCIÓN

El avance de la tecnología presenta nuevas formas de vulnerar las distintas seguridades presentadas por las aplicaciones *web* por lo cual existen nuevas herramientas para reducir estas vulnerabilidades.

Dentro de cada entidad existen ciertos procesos que deben ser cumplidos por los usuarios, los procedimientos en que se focaliza la presente investigación se centran en cómo es gestionado el uso de credenciales por los usuarios para el ingreso hacia las aplicaciones de la entidad perteneciente a la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato.

El autor Bilal Ayyub (2014) acota que, si bien existen procesos con los cuales se puede garantizar un mejor uso de credenciales, para evitar el ingreso de terceros, muchas veces son los mismos usuarios quienes cambian dichas credenciales seguras por otras de mayor facilidad para ellos y para un atacante.

Son los administradores quienes tienen que buscar la manera de contrarrestar estas vulnerabilidades mediante el control de las credenciales de los usuarios y cómo son cambiadas por los mismos.

Para los autores (Cano, 2016); (Barrio, 2017) concuerdan que existen diferentes etapas de los procesos desde la creación de nuevos usuarios hasta el control de cómo se realizan los ingresos a las prestaciones de la aplicación web por parte de cada persona, los cuales deben ser analizados para detectar en cuál de ellas presentan falencias por parte de los usuarios y determinar cuáles pueden ser controlados por los administradores de la aplicación.

De esta manera mitigar los accesos no autorizados mediante la implementación o mejoramiento de políticas de seguridad.

Dentro de las pruebas a realizar se encuentran:

- Creación de nuevos usuarios: Es común que la creación de usuarios sea llevada a cabo por un administrador de la aplicación. Para el Instituto Vasco de Estadística (2018) dentro de cada entidad las políticas que se utilizan para ello varían en ciertos procesos, más los principales se basan en la automatización o semi-automatización de la creación de nuevos usuarios.

El análisis del proceso de definición de roles como lo indica para Oscar Gómez (2017) representa una de las primeras secciones del análisis ya que es necesario conocer las funciones que tienen los distintos tipos de usuarios dentro de la aplicación.

Así mismo, como lo señala Ana Abril, Jarol Pulido y John Bohada (2013) al crear un nuevo usuario se debe verificar qué información es usada para su nombre de usuario y contraseña, y de qué manera se hace llegar esta información al usuario final a través de la administración.

- Métodos de acceso a la aplicación por parte de los usuarios: Uno de los principales problemas de toda entidad son sus usuarios finales, y el uso que le dan a la aplicación, muchas veces sin tener en cuenta las políticas de seguridad existentes, para facilitar el manejo de la misma, provocando una vulnerabilidad muy grave dentro de una entidad.

En el caso de las credenciales por defecto Luis Leal (2013) menciona se debe a distintas causas que pueden ser controladas tales como la creación de usuarios con credenciales débiles o simplemente que al ingresar por primera vez a la aplicación no se pida un cambio de contraseña.

A pesar de las medidas tomadas el momento de ingresar por primera vez existen formas de lograr que las credenciales sean de mayor facilidad para el usuario, pero esencialmente inseguras.

- Función de reseteo de contraseñas: El reseteo de una contraseña para Maritta Heisel, Wouter Joosen, Javier López, Fabio Martinelli (2014) ocurre cuando un usuario no puede recordar las credenciales necesarias para iniciar sesión dentro de una aplicación *web*, por lo cual una aplicación correctamente diseñada tiene que verificar la información requerida por la aplicación para el reseteo de contraseña, cómo son generadas las nuevas contraseñas y de qué forma se comunica el reseteo de las mismas al usuario.

Para Julian Barreto (2018) afirma que existe el proceso de cambio de contraseñas, el cual permite al usuario modificar sus credenciales de acceso, por lo cual un análisis similar al expuesto en el anterior punto es necesario; a más de ello es necesaria la confirmación de la presencia de la contraseña anterior para completar el cambio, de otra manera se considera a la aplicación como insegura y expuesta a ataques utilizando esta vulnerabilidad.

- Uso de mecanismos de bloqueo: Los mecanismos de cierre que tienen ciertas aplicaciones son utilizados principalmente para reducir las posibilidades de un ataque de fuerza bruta.

Los autores (Montenegro, 2018); (Modarres, Kaminskiy, & Krivtsov, 2016); (Rojas, 2018) concuerdan con que al realizar un número determinado de peticiones a la aplicación ésta se bloquea durante un tiempo determinado, evitando que se pueda realizar la misma petición una y otra vez hasta conseguir mediante prueba y error las credenciales de un usuario. Además, existen varias maneras de realizar un mecanismo de cierre, bloquean la página por una cantidad determinada de tiempo, mediante la utilización de *captchas*, los cuales aparecen después de un intento determinado de veces o el bloqueo definitivo de la cuenta en cuestión con el cual se debe solicitar una activación al administrador de la aplicación *web*.

- Manejo de datos por canales encriptados: Para Kathleen Mastrian y Dee McGonigle (2016) las credenciales transportadas por canales encriptados a pesar de tener todas las seguridades posibles para proteger credenciales, las mismas quedan inutilizadas si las mismas son transportadas por medio de canales inseguros, los cuales pueden ser interceptados y al no contar con una encriptación adecuada, las credenciales quedan totalmente expuestas. De estos canales encriptados el principal es conocido como protocolo *HTTPS* (protocolo de transferencia segura de hipertexto), de igual forma concuerda con Luis Guallpa (2017) indica en donde la aplicación posee un cifrado basado en *SSL* el cual garantiza que los datos enviados, a pesar de ser interceptados, no pueden ser leídos.

La encriptación de las credenciales para ACISSI (2015) indica que la encriptación de las credenciales al viajar por un canal seguro es necesaria para cualquier entidad que maneje este tipo de datos, cualquier página que contenga información que deba viajar a través de la red debe disponer de un certificado el cual le permita cifrar su contenido de extremo a extremo para evitar ataques de *Man in the Middle* los cuales buscan el robo de datos personales.

Dentro del sitio *web* correspondiente al aula virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial que es manejada Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato, la cual será el caso de estudio de la presente investigación, se evidencia un uso incorrecto de credenciales de acceso por parte de los usuarios de la misma. El objetivo de la investigación será el de proponer soluciones a los administradores de la aplicación para mitigar en la mayor medida las amenazas a la seguridad de los usuarios tanto en canales de comunicación como en la aplicación. y evitar que ellos, por desconocimiento o falta de experiencia, utilicen credenciales de acceso inseguras o mantengan las que son otorgadas por defecto.

2. METODOLOGÍA

Para los autores (Salgado, 2014); (Hernández & Mejía , 2015) ;(Rodríguez, 2015); (Muñoz & Garcia, 2017) concuerdan que la delimitación de las acciones que se van a ejecutar para el análisis de la existencia de vulnerabilidades dentro de aplicaciones *web*; para lo cual se toma como base ciertos aspectos de la metodología OWASP para el análisis de aplicaciones web y en la presente investigación se focalizan los procesos referentes al uso de credenciales débiles o por defecto, especificados en la misma.

Los autores *Open Web Application Security Project Foundation* (2015); (Machaca, 2018) concuerdan que dentro del apartado de análisis de vulnerabilidades de usuario de la metodología OWASP, manifiesta que se requiere acceso directo a interfaces de administrador para la verificación de creación y manejo de usuarios, mientras que para los demás puntos es necesario la realización de *tests* externos a la entidad, muchos de ellos son contemplados en varios análisis llamados *pentesting* el cual también posee una serie de pasos a seguir para verificar las

vulnerabilidades existentes y de qué manera explotarlos para posteriormente corregirlos.

Para la realización del presente trabajo fueron necesarios los siguientes materiales:

- Máquina con Procesador *Intel Core* i3, 4 Gb de memoria *Ram* Sistema Operativo Windows 8 *Service Pack* 3
- Software de virtualización *Oracle VM Virtualbox* 5.1.
- Sistema Operativo *Kali Linux* 2.0.
- Navegador web *Chrome* 56.0.2924.87
- Servidor *proxy*

3. RESULTADOS

Gracias a la colaboración existente por parte de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato, se pudieron realizar las pruebas planteadas en la introducción de la investigación, tales como verificar de qué manera se crean usuarios, como ellos ingresan a la aplicación, de qué manera se controla el cambio de contraseñas y por qué canal es transportada esa información. Al realizar los análisis correspondientes siguiendo la metodología propuesta se obtuvieron distintos resultados, los cuales, de existir vulnerabilidades se sugiere métodos correctivos para evitar las mismas.

3.1 Creación de nuevos usuarios

La primera vez que el usuario ingresa a la aplicación se le solicita que realice un cambio de contraseña, la cual debe contener al menos una letra mayúscula, al menos un número y al menos un dígito no alfanumérico y que tenga una longitud mínima de 8 caracteres, lo cual se considera correcto para una contraseña segura.
La única posible vulnerabilidad encontrada en este proceso es el uso de una credencial demasiado pública para la contraseña, la cual, muchas veces, no es cambiado por el usuario final.

3.2 Ingreso de usuarios a la aplicación mediante el uso de credenciales por defecto

La vulnerabilidad del uso de credenciales débiles es la más preocupante a nivel administrativo debido a que pueden existir accesos no autorizados externamente, debido a que muchos de los usuarios utilizan como credenciales de acceso su propio número de cédula; ésta vulnerabilidad fue explotada con total éxito logrando entrar a la cuenta de un docente de la institución *Figura 1,* y teniendo acceso a toda la interfaz del mismo incluyendo manejo de trabajos, alumnos, exámenes, calificaciones y su perfil.
De la misma manera, al utilizar *Kali Linux* y una red que estuvo conectada a un servidor proxy los accesos no pudieron ser rastreados hasta la máquina atacante.

Figura 1. Ingreso a banco de preguntas de examen (Fuente, investigación realizada al Aula Virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial)

3.3 Funcionalidad de reseteo de contraseñas

Si existe en algún momento una pérdida de la contraseña de acceso hacia la aplicación *web*, la misma tiene la funcionalidad de recuperar la contraseña mediante el nombre de usuario o el correo electrónico vinculado a la cuenta, la aplicación envía un *link* al cual se ingresa para otorgar una nueva contraseña al usuario, no existen preguntas de seguridad para el restablecimiento de la contraseña en cuestión.

Figura 2. Página de restablecimiento de contraseña (Fuente, investigación realizada al Aula Virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial)

3.4 Funcionalidad de cambio de contraseña

Al analizar la presente funcionalidad se encontró con una irregularidad, si bien al realizar el primer cambio de contraseña cuando se lo solicita por primera vez, se pide que la misma tenga una seguridad bastante alta, al realizar por segunda vez un cambio de contraseña estas políticas ya no estaban activas por lo que fácilmente se puede realizar un cambio de contraseña a una no segura o por defecto como es el utilizar cédula y cédula como credenciales de ingreso *Figura 3.*

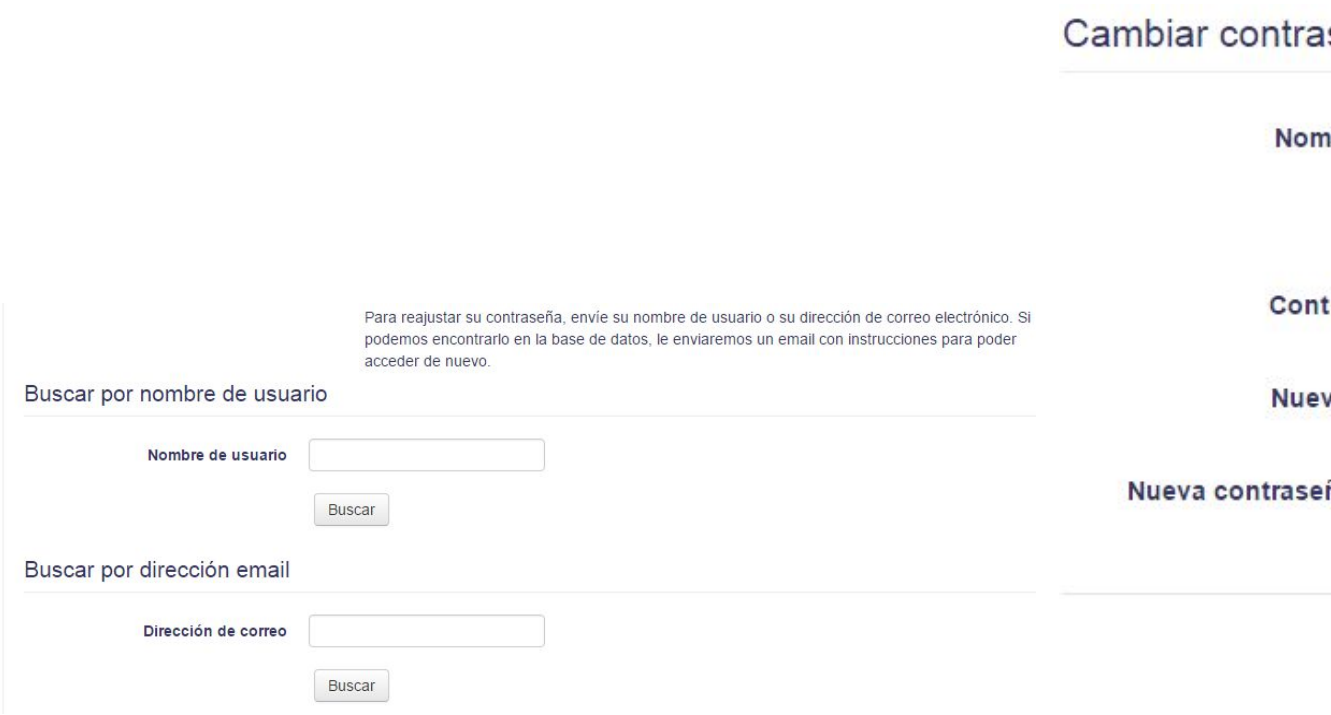

Figura 3. Cambio de contraseña por una no segura (Fuente, investigación realizada al Aula Virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial)

3.5 Mecanismos de cierre automático

La comprobación de la existencia de un mecanismo de cierre se lleva a cabo intentando ingresar con credenciales incorrectas un determinado número de veces, esperando algún resultado que indique que la cuenta ha sido bloqueada de alguna manera, al realizar el análisis a la aplicación *web* de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato se demuestra que puede existir un ataque de fuerza bruta para obtener las credenciales de un usuario debido a que no existe ningún tipo de mecanismo de cierre de la aplicación, se realizó una prueba ingreso con usuario correcto y contraseña incorrecta un total de 20 veces, inmediatamente se ingresó con la contraseña correcta sin dificultad alguna, por lo cual es una vulnerabilidad grave para aplicaciones *web*.

3.6 Credenciales transportadas por canales encriptados

Para la comprobación de la existencia de un cifrado de datos de una página web se puede revisar directamente su *URL*, en el caso enfocado en la presente investigación, la dirección de la aplicación *web* carece de esta seguridad, la cual puede ser vulnerada por un atacante para robar información y credenciales de usuarios *Figura 4.*

```
POST http://sistemaseducaciononline.uta.edu.ec/login/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Referer: http://sistemaseducaciononline.uta.edu.ec/login/index.php
Host: sistemaseducaciononline.uta.edu.ec
```

Figura 4. Petición post realizada al aula virtual (Fuente, investigación realizada al Aula Virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial)

4. CONCLUSIONES

El uso de credenciales por defecto presenta riesgos tan graves como los encontrados en la presente investigación, siendo posible editar calificaciones estudiantiles mediante el acceso a una cuenta docente.

El proceso de cambio de contraseña es realizado de manera insegura al permitir credenciales de acceso demasiado débiles o fáciles de adivinar por algún atacante.

Los mecanismos de cierre automático, tales como el bloqueo del sitio *web* al realizar una cantidad definida de intentos fallidos o la solicitud de realizar una revisión por parte del administrador, son vulnerables a ataques de fuerza bruta al permitir que se pueda fallar la contraseña una cantidad de veces indeterminada.

El protocolo *HTTPS* para el transporte de datos de manera segura y cifrada no fue encontrado por parte de la página donde se aloja la aplicación *web*.

En la presente investigación se demuestra que, existiendo la vulnerabilidad de manejo incorrecto de credenciales, se accede al 100% de in-formación sensible de

los usuarios; por lo cual se busca corregir los errores encontrados trabajando en conjunto con la Dirección de Educación a Distancia y Virtual, capacitar a los usuarios de la misma y de igual aplicar los conocimientos adquiridos, tomando en cuenta el factor humano, para ser aplicados en todo ámbito de seguridad informática de la institución utilizando para ello estándares de seguridad informática.

AGRADECIMIENTO ESPECIAL

El presente trabajo fue apoyado por la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato, quienes facilitaron el acceso a sus equipos y procesos para lograr determinar la existencia de vulnerabilidades en alguno de ellos

BIBLIOGRAFIA

Abril, A., Pulido, J., & Bohada, J. (23 de Diciembre de 2013). *Análisis de Riesgos en Seguridad de la Información*. Tunja, Colombia.

ACISSI. (2015). Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa (3ª edición). Barcelona: ENI.

Ayyub, B. (2014). En *Risk Analysis in Engineering and Economics, Second Edition* (pág. 640). New York: CRC Press.

Barreto, J. (01 de Noviembre de 2018). *Universidad Nacional Abierta y a Distancia.* Obtenido de Escuela de Ciencias Basicas, Tecnologias e Ingenieria: https://repository.unad.edu.co/handle/10596/15026

Barrio, M. (2017). Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015 . Madrid: Reus.

Cano, J. (2016). *ISACA.* Obtenido de Journal: https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberattacks-the-instability-of-security-and-control-knowledge.aspx

Gómez, O. (21 de Marzo de 2017). *CISCO.* Obtenido de Blog Cisco Latinoamérica: https://gblogs.cisco.com/la/sg-oscargomez-la-seguridad-informatica-es-responsabilidad-de-toda-la-empresa/

Guallpa, L. G. (Octubre de 2017). *Dspace.* Obtenido de Uniandes: http://dspace.uniandes.edu.ec/handle/123456789/6762

Heisel, M., Joosen, W., López, J., & Martinelli, F. (2014). Engineering Secure Future Internet Services and Systems: Current Research. España: Springer.

Hernández, A., & Mejía , J. (2015). Guía de ataques, vulnerabilidades, técnicas y. *Red de Revistas Científicas de América Latina y el Caribe, España y Portugal*, 18.

Insitituto Vasco de Estadistica . (27 de Septiembre de 2018). *Eustat.* Obtenido de http://www.eustat.eus/document/datos/ct_02_c.pdf

Leal Garcia, L. (2013). *Repositorio Institucional Universidad Piloto de Colombia.* Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2665/00003531.pdf?sequence=1

Machaca, A. (22 de Enero de 2018). *OWASP ORG.*

Mastrian, K., & McGonigle, D. (2016). Informatics for Health Professionals. Estados Unidos: Jones & Barlett Learning .

Modarres, M., Kaminskiy, M., & Krivtsov, V. (2016). Reliability Engineering and Risk Analysis. *Taylor & Francis Group*, CRC Press.

Montenegro, K. S. (Marzo de 2018). *Repositorio Universidad de Guayaquil.* Obtenido de Repositorio Nacional en Ciencia y Tecnologia: http://repositorio.ug.edu.ec/bitstream/redug/27047/1/B-CINT-PTG-N.262%20Montenegro%20Avata%20Karina%20Stefany.pdf

Muñoz, M., & Garcia, L. F. (2017). Análisis de Riesgos y Prototipos de una página web mediante autenticacion CAPTCHA. Bogotá, Colombia.

Open Web Application Security Project Foundation. (2015). *Guía de Pruebas OWASP.*

Rodríguez, M. (2 de Enero de 2015). *PFC – Auditoría de aplicaciones web: metodología y práctica profesional.* Catalunya, España.

Rojas, A. (Junio de 2018). *Universidad Tecnica de Ambato.* Obtenido de Ingenieria en Sistemas,Electronica e Industrial: http://repositorio.uta.edu.ec/jspui/handle/123456789/28102

Salgado, A. L. (Abril de 2014). Análisis de las aplicaciones web de la Superintendencia de bancos y seguros, Utilizando las recomendaciones Top 10 de OWASP para terminar los riesgos más criticos de seguridad e implementar buenas practicas de seguridad para el desarrollo de sus aplicati. Sangolquí, Quito, Ecuador.