Análisis de vulnerabilidades en aplicaciones Web.

Angélica González Páramo[1], Einar Jhordany. Serna Valdivia[1] y Luis Armando García de la Rosa[1]

1 Instituto Tecnológico Superior de Guanajuato. agonzalez@itesg.edu.mx

En la actualidad, se están presenciando varios acontecimientos de ciberataques, en importantes organizaciones públicas y privadas, que han sufrido ataques a sus sistemas informáticos.Es importante identificar vulnerabilidades en sitios web, ya que ahora todo se trabaja por medios electrónicos, es decir por medios dinámicos que acceden a servicios, como el consultar calificaciones, transferencias bancarias, cursos, pagos, etc., todo esto por medio de una página web.¿Y cuál es la problemática que se presenta en las páginas?, pues como la mayoría de usuarios usan estos métodos para ahorrar tiempo, hay personas dedicadas a buscar vulnerabilidades para hacer mal uso de la información que se maneja, aprovechando:**Configuración débil**, esta se presenta cuando de los dispositivos que intervienen se dejan por defecto, debido a que desean lanzar rápido el servicio web. **Comunicación insegura entre cliente y servidor**. Es importante que la comunicación entre cliente y servidor esté cifrada, como contraseñas de acceso al sitio, ya que si se filtra un monitoreo de red, puede detectarse esta información sensible. Por último, **se tiene software desactualizado,** es una de las situaciones que a menudo se presenta en pequeñas empresas, y es la forma más sencilla de poder obtener información de la empresa o las personas que acceden a sistema.

Para poder buscar vulnerabilidades, es importante enfocarse en las fases del pentesting, bajo la guia de OWASP(Proyecto abierto de seguridad de aplicaciones web), esta busca hacer del mundo un lugar en el que el software inseguro es la anomalía, no la norma, y la Guía de Pruebas es una pieza importante del rompecabezas, para disminuir las vulnerabilidades en sistios web u otras alternativas de software.

Pensando en esto, el proyecto se enfoca el analisis del manejando las fases de pentesting que recomienda la guia,esto con el fin de adquirir conocimiento previos, para lograr indagar las etapas de pentesting, las cuales son: Preparación, Recopilación de información(pasiva/activa), Análisis de vulnerabilidades, Explotación de vulnerabilidades, Post-Explotación y reporte de las vulnerabilidades encontradas, esto aplicado en primera etapa como investigación básica .

Este proceso se aplica a un sitio web oficial de una institución publica bajo un ambiente controlado, obteniendo el acceso a fotografias de alumnos, contraseñas, bajo que lenguaje y que versión fue creado este sitio, no soporta multiples solicitudes de acceso, ya que al hacer una denegación de servicio, la página colapso por segundos y no se pudo acceder al sitio, puede clonarse sin ninguna restrticción, al referirse que se puede clonar, es que se puede crear una copia identica a la oficial, ya que no cuenta con certificados de seguridad, ni actualizaciones en el lenguaje o administrador de base de datos.

El enfoque de OWASP permite establecer la siguiente formula: **Riesgo = Probabilidad * Impacto** .Esta guia tiene una plantilla con la información y formulas para obtener el nivel de riesgo, hasta el momento el desarrollo de este proyecto esta en etapa de investigación, pero algunos de los datos obtenidos que se generaron se encuentran inferiores a la nota 3, que de acuerdo a OWASP aún se consideran bajos.