UNIVERSIDAD PUBLICA DE EL ALTO

DIRECCION DE POSTGRADO

CENTRO DE ESTUDIOS DE FORMACION Y POSTGRADO E INVESTIGACION CEFORPI

TESIS DE GRADO

"MODELO DE INTELIGENCIA ARTIFICIAL PARA LA DETECCIÓN DE AMENAZAS EN PLUGINS DE WORDPRESS"

Postulante: Jhonatan Carvajal Corani

Tutor Metodológico: M. Sc. Lic. Ing. Fanny Helen Pérez Mamani

Tutor Especialista: M. Sc. Lic. Ing. Neil Ramiro Gonzales Burgoa

Tutor Revisor: M. Sc. Lic. Ramiro Jhonatan Pardo Foronda

EL ALTO-BOLIVIA

2024

RESUMEN

En esta tesis se analizan diferentes métodos para la detección de amenazas en plugins de WordPress, es decir, aquellos plugins que se encuentran en nuestro conjunto de datos pero que no tienen un comportamiento normal. Encontrar patrones en el uso de plugins de WordPress sigue siendo un reto interesante en la seguridad informática. Las anomalias en los plugins aparecerán por varias razones, como actividades maliciosas o vulnerabilidades no detectadas. En este sentido, el análisis de los plugins y una combinación de técnicas de Inteligencia Artificial (Machine Learning) puede convertirse en un buen aliado para ir más allá de las firmas y ser capaz asi de encontrar patrones previamente desconocidos. En cada predicción realizada por un modelo diferente, la precisión varía, esto dependerá de cómo el algoritmo se comporte con nuestro Data Set y si logra cumplir con la predicción necesaria, lo Cual es la detección de amenazas en los plugins de WordPress.

En cada análisis y evaluación de cada método de predicción, los resultados obtenidos indicaron que aquellos métodos menos precisos en la predicción de detección de amenazas fueron los modelos de regresión logística y de clasificación. Por otro lado, el método que ofreció mejores resultados fue el de árboles de decisión, cumpliendo con nuestro objetivo de
detectar amenazas en los plugins de WordPress de manera efectiva.

Palabras Claves: Inteligencia Artificial, WordPress, Protección Sitios Web.