



Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

Auditoría para identificar vulnerabilidades en las páginas web del Instituto Geográfico Militar (IGM).

AUTORES:

Marco F. Rodríguez L.
Cesar A. Triviño C.
Nelson R. Acurio R.
Richard M. Ramos T.

TUTOR:

Alejandro Cortés L.

Resumen

Este proyecto está enfocado en analizar la seguridad de las dos páginas web del Instituto Geográfico Militar (IGM) frente a posibles ciberataques. Para este análisis se utilizó el modelo de auditoría web, ya que esto nos permite descubrir vulnerabilidades en sitios web, mediante el uso de escaneo de herramientas especializadas, logrando con esto prevenir y mitigar accesos no autorizados en nuestra organización que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información y servicios que esta ofrece o los clientes nacionales como internacionales. El objetivo de este proyecto es identificar las vulnerabilidades del IGM, mediante el uso de las herramientas de escaneo de páginas web Burp Suite e Invisi. La metodología usada para realizar este análisis consta de planificación, búsqueda investigativa, escaneo y análisis de resultados. En el análisis de resultados obtenidos, las vulnerabilidades con un mayor rango de criticidad en la página principal del IGM se evidenciaron los siguientes: inyección SQL, MQSL obsoleta, versión Apache obsoleta, entre otros, por otro lado, en la página del geoportal las vulnerabilidades más relevantes que se evidenciaron son: versión Apache obsoleta, OPENSSL obsoleta, entre otras. Esto nos ha permitido emitir criterios técnicos de ciberseguridad utilizando las herramientas de análisis de las páginas web, con el fin de brindar a los directivos de la organización argumentos técnicos, para la aceptada toma de decisiones en lo que concierne a la seguridad de la información de la institución.

Abstract

This project is focused on analyzing the security of the two websites of the Military Geographic Institute (IGM) against possible cyberattacks. For this analysis, the web audit model was downloaded, since this allows us to discover vulnerabilities in websites, through the use of specialized scanning tools, thereby preventing and reducing unauthorized access in our organization that can put confidentiality at risk., equipment and availability of the information and services that it offers to national and international clients. The objective of this project is to identify IGM vulnerabilities, by using the Burp Suite and Invisimart web page scanning tools. The methodology used to carry out this analysis consists of planning, investigative search, scanning and analysis of results. In the analysis of the results obtained, the vulnerabilities with a higher range of criticality on the main page of the IGM showed the following: SQL injection, obsolete MQSL, obsolete Apache version, among others, on the other hand, on the page of the geoportal the vulnerabilities The most relevant ones that were evidenced are: obsolete Apache version, obsolete OPENSLL, among others. This has allowed us to issue technical cybersecurity criteria using the analysis tools of web pages, in order to provide the directors of the organization with technical arguments, for the accepted decision-making regarding the security of the information of the institution.