

INTISARI

Kemungkinan akan terjadinya kebocoran data atau informasi, merupakan hal yang tidak dapat diprediksi, seperti halnya pencurian data informasi yang dimiliki suatu pemerintahan ataupun Perusahaan yang memiliki website, Keamanan website sering kali diabaikan oleh para *developer* termasuk website profil pemerintahan yang memiliki sebuah data penting yang mungkin bisa dicuri oleh pihak yang tidak bertanggung jawab. Pemerintahan Desa Kebutuh merupakan instansi yang dikelola oleh desa untuk melaksanakan tugas dan wewenangnya tidak lepas dari penggunaan website. Dari wawancara yang telah dilakukan, pemerintahan Desa Kebutuh memiliki website yang digunakan sebagai sarana pelayanan masyarakat serta sumber informasi mengenai berita terbaru dari Desa Kebutuh, dan website tersebut pernah mengalami suatu kendala dimana pihak desa tidak dapat login website tersebut, dari masalah itu pihak kominfo selaku pengelola pusat website yang dimiliki oleh setiap desa melakukan perbaikan pada website Desa Kebutuh, setelah dilakukannya perbaikan, pihak desa juga ingin mengetahui kerentanan apa saja yang masih terdeteksi ketika sudah dilakukannya perbaikan. Oleh karena itu perlu dilakukannya *Vulnerability Assessment*, *Vulnerability Assessment (VA)* adalah proses pemindaian sistem untuk mengetahui kerentanan dan celah yang ada pada sebuah sistem website, celah ini memberikan *backdoor* ke penyerang untuk dapat menyerang sistem korban. Metode yang digunakan dalam penelitian ini adalah metode *Action Research*. Tujuan dari penelitian ini adalah untuk menguji & mengetahui kerentanan yang terdapat pada website Desa Kebutuh dan resiko ancaman kejahatan *cyber* yang mungkin bisa terjadi setelah dilakukannya perbaikan oleh pihak pusat yang mengelola website tersebut. Proses pengujian keamanan website ini dilakukan menggunakan tools *OWASP ZAP* untuk mempermudah melakukan proses pemindaian kerentanan. Hasil akhir dari penelitian ini berupa dokumen yang berisi jenis kerentanan yang ditemukan serta saran perbaikan dari kerentanan yang ditemukan tersebut.

Kata Kunci: *OWASP-ZAP, Vulnerability, Website, Backdoor, Action Research*..

ABSTRACT

The possibility that data or information leaks will occur is something that cannot be predicted, such as theft of information data belonging to a government or company that has a website. Website security is often ignored by developers, including government profile websites that have important data that could possibly be stolen by irresponsible parties. The Kebutuh Village Government is an agency managed by the village to carry out its duties and authority which cannot be separated from the use of the website. From the interviews that have been conducted, the Kebutuh Village government has a website which is used as a means of community service as well as a source of information regarding the latest news from Kebutuh Village, and the website has experienced problems where the village cannot log in to the website, because of this problem, the Ministry of Communication and Information as the central manager of the website owned by each village has made improvements to the Kebutuh Village website. After the repairs have been made, the village also wants to know what vulnerabilities are still being detected. Therefore, it is necessary to carry out a Vulnerability Assessment, Vulnerability Assessment (VA) is a system scanning process to find out vulnerabilities and gaps that exist in a website system, these gaps provide a backdoor for attackers to be able to attack the victim's system. The method used in this research is the Action Research method. The purpose of this research is to test & determine the vulnerabilities contained in the Kebutuh Village website and the risk of cyber crime threats that might occur after repairs are carried out by the center that manages the website. This website security testing process is carried out using the OWASP ZAP tool to make the vulnerability scanning process easier. The final result of this research is a document containing the types of vulnerabilities found as well as suggestions for improvements to the vulnerabilities found.

Keywords: OWASP-ZAP, Vulnerability, Website, Backdoor, Action Research..