INTISARI

Website merupakan salah satu media dalam lingkup teknologi informasi yang cukup populer. Seiring dengan kepopuleran website, kepedulian terhadap keamanan suatu website perlu menjadi perhatian serius. Hal tersebut dilakukan mengingat banyaknya ancaman keamanan yang sering terjadi pada sebuah website. Serangan Cross Site Scripting (XSS) menjadi salah satu serangan siber yang sangat umum dan sering terjadi disebuah website. XSS terjadi karena terdapat celah pada suatu website yang dapat dieksploitasi oleh penyerang dengan menyisipkan kode skrip tertentu. Dampak serangan XSS dapat berupa perubahan konten suatu website hingga pencurian data rahasia pengguna. Menyikapi hal tersebut, dalam penelitian ini dilakukan proses identifikasi kerentanan website dengan menerapkan framework Open Web Application Security Project (OWASP). Framework OWASP digunakan sebagai acuan penelitian agar langkah-langkah yang dilakukan lebih terstruktur dan sistematis. Selain itu guna mendukung proses identifikasi, penelitian ini memanfaatkan software Zed Attack Proxy (ZAP) sebagai tool untuk melakukan proses pemindaian suatu website secara otomatis. Dalam proses pemindaian, informasi mengenai kerentanan suatu website akan ditampilkan sehingga dapat diketahui suatu website memiliki potensi kerentanan XSS atau tidak. Hasil yang diperoleh dalam penelitian ini berupa ditemukannya 22 jenis kerentanan pada website Art Gallery Management System (AGMS), salah satunya kerentanan XSS. Selain itu dengan melakukan proses ekploitasi terhadap kerentanan XSS, diperoleh username dan password pengguna yang digunakan sebagai akses login pada website AGMS.

Kata kunci: XSS, Identifikasi, OWASP, ZAP, Website.

ABSTRACT

A website is one of the media in the scope of information technology that is quite popular. Along with the popularity of the website, concern for the security of a website needs to be a serious concern. This is done considering the many security threats that often occur on a website. Cross-site scripting (XSS) attacks are one of the most common cyberattacks that often occur on websites. XSS occurs due to a vulnerability in a website that can be exploited by an attacker through the injection of specific script code. The impact of XSS attacks can be in the form of changes to the content of a website or the theft of confidential user data. In response to this, in this research, a website vulnerability identification process is carried out by applying the Open Web Application Security Project (OWASP) framework. The OWASP framework is used as a research reference so that the steps taken are more structured and systematic. In addition, to support the identification process, this research utilizes Zed Attack Proxy (ZAP) software as a tool to automatically scan a website. In the scanning process, information about the vulnerability of a website will be displayed so that it can be known whether a website has a potential XSS vulnerability or not. The results obtained in this research include the discovery of 22 types of vulnerabilities on the Art Gallery Management System (AGMS) website, one of which is the XSS vulnerability. In addition, by exploiting the XSS vulnerability, the user username and password used as login access on the AGMS website were obtained.

Keywords: XSS, Identification, OWASP, ZAP, Website.