ABSTRAK

Gerakan digitalisasi membuat banyak organisasi membangun aplikasi sistem informasi. Namun dengan meningkatnya proses digitalisasi juga memicu penigkatan serangan siber, pada tahun 2022 Indonesia mengalami peningkatan dalam kasus serangan siber yaitu pada kasus kebocoran data, selain itu serangan terhadap *website* juga menjadi tiga insiden serangan teratas yang masuk ke data BSSN, serangan siber seperti kebocoran data maupun serangan terhadap *website* mampu menyebabkan kerugian pagi perusahaan. Penelitian ini melakukan uji penetrasi terhadap tiga aplikasi berbasis *website* pada PT XYZ. Uji penetrasi adalah salah satu cara untuk melihat tingkat keamanan sebuah sistem, pengujian dilakukan dengan membuat simulasi serangan terhadap aplikasi yang akan diuji. Uji penetrasi pada penelitian ini akan mengikuti petunjuk dari *Open Worldwide Security Project - Web Security Testing Guide (OWASP - WSTG),* pengujian meliputi dua kategori pengujian yaitu *Authentication Testing* dan *Input Validation Testing*. Hasil dari pengujian menemukan adanya sembilan kerentanan pada tiga aplikasi yang diuji, kerentanan dengan risiko tertinggi berdasarkan *OWASP Risk methodology* adalah kerentanan terkait *SQL injection* dan *cross site scripting*. Kerentanan tertinggi yang ditemukan mampu memberikan kemungkinan bagi penyerang untuk mendapatkan informasi dari *database* aplikasi dan pada kasus tertentu mampu mengubah atau merusak konten pada halaman aplikasi *website*. Beberapa cara untuk memperbaiki kerentanan keamanan tersebut adalah dengan mengikuti standar keamanan yang telah disarankan oleh *framework website* yang digunakan serta selalu mengupdate *plugin* atau teknologi yang dipakai ke versi terbaru.

Kata Kunci: Keamanan Sistem Informasi, *Penetration Testing*, *web* security, OWASP, WSTG

ABSTRACT

The digitalization movement has led many organizations to build information system applications. However, with the increase in digitalization processes, there has also been an increase in cyber attacks. In 2022, Indonesia experienced an increase in cyber attack cases, such as data breaches. In addition, attacks on websites have also become one of the top three incidents reported to BSSN. Cyber attacks such as data breaches and website attacks can cause financial losses for companies. This study conducted a penetration test on three web-based applications at PT XYZ. Penetration testing is one way to assess the security level of a system by simulating an attack on the application being tested. The penetration test in this study followed the guidelines of the Open Worldwide Security Project - Web Security Testing Guide (OWASP - WSTG), and included two testing categories: Authentication Testing and Input Validation Testing. The results of the test found nine vulnerabilities in the three applications tested, with the highest risk vulnerabilities according to the OWASP Risk methodology being related to SQL injection and cross-site scripting. The highest vulnerability found could allow an attacker to obtain information from the application's database and, in some cases, alter or damage the content of the website's application page. Some ways to fix these security vulnerabilities include following the security standards recommended by the website framework used and always updating plugins or technologies to the latest version.

Keywords: Information System Security, Penetration Testing, web security, OWASP, WSTG