ABSTRAK

Keamanan telah menjadi aspek mendasar dalam evolusi teknologi website. Perannya sangat penting untuk memangkas risiko insiden siber di suatu institusi. Universitas Malikussaleh memiliki suatu Sistem Informasi Pegawai yang secara partikular digunakan oleh para dosen dan staf untuk mengakses berbagai informasi seperti; data pegawai, laporan, absensi, dan lain-lain, secara daring. Antarmuka SIMPEG UNIMAL dirancang bangun menggunakan bahasa seperti HTML, CSS, dan JavaScript. Pemilihan bahasa tersebut, membuka peluang bagi penyerang untuk mendeteksi kerentanan. Memastikan keamanannya menjadi sangat krusial karena menyimpan kredensial pengguna. Sebab itu, diperlukan pengujian keamanan untuk mengidentifikasi potensi kerentanan di dalamnya. Pengujian diterapkan dengan merujuk pada OWASP WSTG v4.2: *Client-side Testing*, melibatkan 13 jenis pengujian dan memakai *Client Role* sebagai Dosen. Selain itu, penelitian dibagi menjadi 3 fase, yaitu; *Vulnerability Scanning*, *Penetration Testing*, dan *Reporting*, serta didukung alat OWASP ZAP dan Burp Suite untuk mengoptimalkan proses pengujiannya. Keluaran yang diperoleh dari penelitian ini yaitu SIMPEG UNIMAL memiliki kerentanan *Cross-site Scripting* karena tidak adanya konversi terhadap *output* yang ditampilkan kepada pengguna, dan terdapat juga kerentanan *Clickjacking* karena kurangnya penerapan *Header* yang dapat melindungi *website* dari jenis serangan tersebut.

Kata kunci: **Pengujian Keamanan, OWASP, WSTG v4.2: *Client-side Testing*, Sistem Informasi Pegawai**

ABSTRACT

Security has become a fundamental aspect in the evolution of website technology. Its role is very important to reduce the risk of cyber incidents in an institution. Malikussaleh University has an Employee Information System which is particularly used by lecturers and staff to access various information such as; employee data, reports, attendance, etc., by online. The SIMPEG UNIMAL interface was designed using languages such as HTML, CSS, and JavaScript. The choice of these languages opens up opportunities for attackers to detect vulnerabilities. Ensuring its security is crucial because it stores users credentials. Therefore, security testing is needed to identify potential vulnerabilities in it. Testing is implemented by referring to OWASP WSTG v4.2: Client-side Testing, involving 13 types of testing and using the Client Role as Lecturer. In addition, the research is divided into 3 phases, namely; Vulnerability Scanning, Penetration Testing, and Reporting, and supported by OWASP ZAP and Burp Suite tools to optimize the testing process. As the output obtained from this research is SIMPEG UNIMAL has the Cross-site Scripting vulnerability due to the lack of conversion of the output displayed to the user, and there is also the Clickjacking vulnerability due to the lack of implementation of Headers that can protect the website from this type of attack.

Keywords: ***Security Testing, OWASP, WSTG v4.2: Client-side Testing, Employee Information System***