ABSTRAK

Meningkatnya risiko serangan keamanan data berbasis website menjadi perhatian berbagai pihak, termasuk PT. XYZ merupakan perusahaan yang mengembangkan *software* untuk apotek dan klinik yang telah membantu lebih dari 2500 apotek dan klinik di lebih dari 400 kota di Indonesia. Data yang disimpan didalamnya mencakup informasi sensitif seperti data perusahaan dan informasi pelanggan, yang harus dijaga dengan ketat agar tidak jatuh ke tangan yang salah. Tujuan penelitian ini adalah mengidentifikasi kerentanan dalam sistem informasi PT. XYZ dan memberikan rekomendasi untuk meningkatkan keamanan. Metode *penetration testing* dengan *OWASP Top 10 2021* yang masih sangat relevan dan populer. *OWASP Top 10 2021* berisi sepuluh risiko keamanan aplikasi *web* yang paling kritis yang diidentifikasi oleh para ahli keamanan. Dalam metode *Penetration Testing*, terdapat tahapan-tahapan seperti *scope*, *reconnaissance*, *vulnerability detection*, *information analysis and planning*, *penetration testing*, privilege escalation, result analysis, reporting, dan *clean-up*. Parameter keberhasilan penelitian ini meliputi tingkat kerentanan yang teridentifikasi, tingkat keberhasilan serangan, dan rekomendasi yang diterima untuk meningkatkan keamanan sistem. Dengan penelitian ini PT. XYZ dapat meningkatkan keamanan sistem informasinya dan melindungi data pelanggan dengan lebih efektif. Berdasarkan hasil pengujian dengan metode *penetration testing* dengan *OWASP Top 10 2021*, ditemukan beberapa kerentanan signifikan, antara lain masalah pada kontrol akses yang rusak, kegagalan kriptografi, *SQL Injection*, potensi XSS melalui *header Referer*, serta masalah konfigurasi keamanan seperti kurangnya *header* CSP dan *X-Frame-Options*. Beberapa komponen juga ditemukan rentan, seperti versi *jQuery* yang usang dan CVE pada komponen sistem. Selain itu, masalah terkait validasi otentikasi dan kegagalan dalam *logging* dan *monitoring* juga teridentifikasi. Rekomendasi perbaikan meliputi penguatan kontrol akses, konfigurasi kriptografi yang lebih aman, penggunaan *parameterized queries* untuk mencegah *SQL Injection*, perbaikan konfigurasi header keamanan seperti CSP dan *X-Frame-Options*, pembaruan komponen sistem, serta peningkatan mekanisme otentikasi dan sistem logging serta monitoring untuk mendeteksi aktivitas serangan lebih efektif.

Kata Kunci:. **Keamanan sistem website, Keamanan sistem informasi, Owasp top 10, Penetration testing, PT XYZ**