BAB IV
KESIMPULAN

4.1.Kesimpulan

Penulis telah melakukan pengujian VAPT pada sistem informasi BPD dan BPR menggunakan metode *black-box testing*, yang berhasil mengidentifikasi berbagai kerentanan yang dapat mengancam keamanan sistem perusahaan tersebut. Beberapa kerentanan utama yang ditemukan meliputi SQL *Injection*, *Cross-Site Scripting* (XSS), *weak credentials*, dan *information disclosure* seperti *directory listing*, *phpinfo()*, serta kerentanan pada perangkat jaringan seperti *MikroTik*.

Melalui penerapan metode *black-box testing*, yang mensimulasikan serangan dari perspektif eksternal, pengujian ini berhasil memberikan gambaran nyata tentang potensi ancaman yang dihadapi oleh sistem tanpa memerlukan akses internal. Kemudian penggunaan CVSS dalam evaluasi kerentanannya memungkinkan penentuan tingkat keparahan yang objektif, membantu pihak terkait untuk memprioritaskan perbaikan berdasarkan risiko yang ditimbulkan.

Berdasarkan hasil evaluasi, penulis merekomendasikan langkah-langkah mitigasi yang dapat diambil untuk mengatasi setiap kerentanan yang ditemukan, termasuk pembaruan perangkat lunak, perbaikan konfigurasi sistem, dan memperkuat akses kontrol. Secara keseluruhan, hasil pengujian ini memberikan kontribusi yang sangat penting dalam memperkuat ketahanan sistem terhadap potensi ancaman keamanan di masa mendatang, sekaligus memberikan informasi bagi pemangku kepentingan BPD dan BPR untuk meningkatkan kebijakan dan prosedur keamanan yang sudah ada agar menjadi lebih baik.

4.2.Saran

Berdasarkan hasil temuan dan kesimpulan yang diperoleh dalam proses VAPT ini, penulis memberikan beberapa saran untuk meningkatkan keamanan sistem informasi yang diuji, baik untuk pihak pengelola sistem maupun pihak lain yang terlibat dalam pengelolaan keamanan siber:

1. Pihak BPD dan BPR sangat disarankan untuk melaksanakan program pelatihan dan *workshop* mengenai keamanan siber secara berkala untuk seluruh jajaran karyawan, termasuk manajemen. Program ini bertujuan untuk memperkenalkan potensi ancaman yang dapat memengaruhi *confidentiality*, *integrity*, dan *availability* sistem informasi, serta mengedukasi praktik terbaik dalam pengelolaan dan perlindungan data sensitif. Peningkatan kesadaran terhadap ancaman seperti teknik *phishing*, rekayasa sosial, dan kebocoran data pribadi dapat secara signifikan mengurangi kemungkinan kesalahan manusia yang dapat memperburuk kondisi keamanan sistem.
2. Sangat direkomendasikan agar pihak BPD dan BPR secara rutin melakukan simulasi serangan siber untuk menguji ketahanan sistem serta kesiapan karyawan dalam menghadapi potensi ancaman yang sebenarnya. Uji coba semacam ini dapat dilakukan melalui *penetration testing* atau *red teaming* untuk mengevaluasi efektivitas kontrol yang ada serta kesiapan tim dalam merespons insiden keamanan. Melalui evaluasi ini, organisasi dapat mengidentifikasi titik lemah pada sistem dan prosedur yang perlu diperbaiki guna memperkuat ketahanan terhadap ancaman yang lebih besar.