BAB V
KESIMPULAN DAN SARAN

1.2 Kesimpulan

Berdasarkan pengujian keamanan yang dilakukan pada sistem desa digital (Website Desa v2.0.6.24) menggunakan metode waterfal dan Penetration Testing Execution Standard (PTES), dapat disimpulkan bahwa:

1. Kerentanan yang ditemukan dapat mengakibatkan pelanggaran privasi, gangguan operasional, kehilangan kendali sistem, dan kerusakan reputasi. Data sensitif masyarakat, termasuk informasi pribadi, berpotensi disalahgunakan jika tidak ditangani dengan baik.
2. Untuk mengecek Kerentanan yang ditemukan, maka telah dilakukan Testing menggunakan *Hydra* dengan serangan *Hybrid Attack* (penggabungan antara *insider attack* dan *dictionary attack*) seperti yang terdapat pada tahap *Exploitation*.
3. Penggunaan teknologi seperti Visual Studio Code, XAMPP, MySQL, PHPMailer, Twilio, dan WGET dalam pengembangan mockup sistem keamanan memberikan kemudahan dalam pengujian dan implementasi mitigasi. Hal ini memungkinkan pengembang untuk fokus pada aspek keamanan tanpa terganggu oleh kompleksitas sistem asli.
4. Rekomendasi mitigasi yang diberikan, seperti penerapan MFA, pengelolaan akun yang lebih ketat, dan edukasi pengguna, telah dirancang dan diterapkan pada MockUp WEBSITE DESA yang baru. Pengujian pasca-mitigasi menunjukkan bahwa langkah-langkah tersebut efektif dalam mengurangi risiko serangan *hybrid attack*, dengan tidak ditemukannya password valid selama pengujian.

1.3 Saran

Berdasarkan hasil penelitian dan kesimpulan yang diperoleh, beberapa saran yang dapat diberikan untuk peneliti selanjutnya adalah:

1. Penggunaan Alat Analisis Kerentanan: Peneliti selanjutnya disarankan untuk menggunakan alat analisis kerentanan seperti Acunetix atau Nessus dalam pengujian keamanan. Alat-alat ini dapat memberikan analisis yang lebih mendalam mengenai kerentanan yang ada dalam aplikasi web, serta memberikan rekomendasi spesifik untuk perbaikan.
2. Implementasi AI untuk Deteksi Anomali: Penelitian selanjutnya dapat mengeksplorasi penggunaan teknologi kecerdasan buatan (AI) dalam mendeteksi anomali pada sistem logging. Dengan menerapkan algoritma pembelajaran mesin, peneliti dapat mengidentifikasi pola yang mencurigakan dan potensi serangan lebih awal, sehingga meningkatkan respons terhadap insiden keamanan.
3. Penerapan Metode Pengujian yang Beragam: Peneliti selanjutnya disarankan untuk menerapkan berbagai metode pengujian, seperti pengujian penetrasi otomatis dan manual, untuk mendapatkan gambaran yang lebih komprehensif mengenai kerentanan sistem. Kombinasi metode ini dapat membantu dalam mengidentifikasi kerentanan yang mungkin terlewatkan oleh satu metode saja.
4. Studi Kasus di Berbagai Sistem: Disarankan untuk melakukan studi kasus di berbagai sistem desa digital atau sistem serupa di sektor lain. Hal ini dapat membantu dalam memahami perbedaan dan kesamaan dalam kerentanan yang dihadapi, serta strategi mitigasi yang efektif.
5. Pengembangan Program Edukasi yang Lebih Komprehensif: Penelitian lebih lanjut dapat difokuskan pada pengembangan program edukasi dan kesadaran keamanan yang lebih efektif untuk pengguna sistem. Penelitian ini dapat mencakup metode pengajaran yang berbeda dan evaluasi dampaknya terhadap perilaku pengguna dalam menjaga keamanan akun.

Dengan menerapkan saran-saran di atas, diharapkan penelitian selanjutnya dapat memberikan kontribusi yang lebih besar dalam bidang keamanan informasi dan membantu meningkatkan keamanan sistem digital di berbagai sektor.