BAB V
PENUTUP

5.1 Simpulan

Penelitian ini memberikan kontribusi penting dalam memastikan keamanan website MyApp melalui pendekatan penetration testing yang komprehensif. Beberapa simpulan yang dapat diambil adalah sebagai berikut:

1. Pengembangan *Website* yang Berorientasi pada Kemudahan dan Efisiensi, Website MyApp dirancang untuk mengintegrasikan fitur profil, chat, top-up, dan transaksi dalam satu sistem yang mudah digunakan. Hal ini bertujuan memberikan kemudahan bagi pengguna dalam mengelola informasi pribadi, berkomunikasi, dan melakukan transaksi secara efisien.
2. Identifikasi Kerentanan sebagai Langkah Awal Keamanan dengan penggunaan *tools* seperti *Burp Suite* dan *SQL Map* terbukti efektif dalam mendeteksi celah keamanan pada sistem. Identifikasi awal terhadap kerentanan menjadi langkah fundamental untuk meminimalkan risiko *eksploitasi*.
3. Hasil penetration testing dapat berbeda antara lingkungan lokal dan hosting karena adanya perbedaan konfigurasi keamanan yang diterapkan. Pada lingkungan lokal, sistem umumnya memiliki pengaturan keamanan yang lebih longgar dan hak akses database yang lebih luas, yang memungkinkan eksploitasi lebih mudah dilakukan, misalnya dengan menggunakan SQLMap. Namun, di lingkungan hosting, penyedia layanan biasanya menambahkan

proteksi tambahan, seperti mod_security, IDS/IPS, serta pembatasan hak akses database, yang dapat mencegah serangan SQL Injection. Selain itu, faktor lain seperti penggunaan HTTPS, enkripsi data, dan perbedaan konfigurasi aplikasi juga berperan dalam kegagalan eksploitasi di hosting.

4. Simulasi Serangan *Siber* untuk Menguji Ketahanan Sistem dengan melakukan pengujian serangan yang melibatkan ancaman nyata seperti *SQL Injection, HTML Injection*, dan *IDOR* menunjukkan sejauh mana celah keamanan dapat dieksploitasi. Hal ini memberikan gambaran tingkat risiko yang dihadapi *website* MyApp.
5. Hasil pengujian *penetration testing* memberikan data yang berharga untuk mengevaluasi tingkat keamanan MyApp. Analisis mendalam terhadap data tersebut memungkinkan identifikasi tingkat risiko spesifik untuk setiap kerentanan yang ditemukan.
6. Solusi yang dirancang berdasarkan hasil pengujian berhasil menutup celah keamanan yang ditemukan. Solusi tersebut dirancang untuk meningkatkan perlindungan data dan sistem MyApp, sekaligus memastikan efektivitas implementasinya.
7. Evaluasi keberhasilan langkah-langkah yang diambil memastikan bahwa solusi tidak hanya mengatasi kerentanan saat ini tetapi juga mencegah ancaman serupa di masa mendatang.

5.2 Saran

Agar keamanan *website* MyApp dapat terjamin melalui penetration testing, diperlukan strategi komprehensif yang mencakup pengembangan, identifikasi kerentanan, simulasi serangan, analisis data, implementasi solusi, dan evaluasi.

1. Pastikan pengembangan fitur utama website (profil, chat, top-up, dan transaksi) memprioritaskan fungsionalitas dan keamanan. Fitur-fitur tersebut harus dirancang dengan mempertimbangkan skenario pengguna nyata, menggunakan teknologi terkini, dan didukung dengan validasi input untuk mencegah serangan seperti *cross-site scripting* (XSS) atau *injection attacks*.
2. Gunakan alat-alat yang andal seperti *Burp Suite, SQLMap, dan OWASP ZAP* untuk mengidentifikasi potensi celah keamanan. *Tools* ini dapat membantu dalam pemindaian otomatis dan memberikan laporan rinci terkait kerentanan yang ditemukan, sehingga memungkinkan tim untuk memahami prioritas perbaikan.
3. Lakukan simulasi dengan ancaman realistis seperti *SQL Injection, HTML Injection, dan IDOR,* secara terkendali. Simulasi serangan ini bertujuan untuk mengukur tingkat resistansi website terhadap serangan nyata tanpa membahayakan sistem produksi, sehingga risiko dapat dipetakan secara akurat.
4. Analisis hasil pengujian dengan pendekatan kuantitatif dan kualitatif untuk memahami tingkat risiko. Data hasil testing, seperti laporan

eksploitasi atau log keamanan, harus dianalisis untuk mengetahui skala ancaman, area kerentanan, dan kemungkinan dampaknya terhadap operasional website.

5. Lakukan evaluasi menyeluruh terhadap langkah-langkah keamanan yang telah diambil, termasuk pengujian ulang. Evaluasi ini memastikan bahwa solusi yang diterapkan tidak hanya efektif dalam menutup celah keamanan yang ditemukan tetapi juga mencegah potensi ancaman di masa mendatang.
6. Keamanan sistem, penting untuk memperketat pengaturan di lingkungan lokal dengan membatasi hak akses database dan mengaktifkan proteksi seperti mod_security guna mencegah potensi serangan. Selain itu, penggunaan protokol HTTPS dan enkripsi data harus diterapkan untuk melindungi informasi sensitif dari eksploitasi. Pembaruan dan konfigurasi aplikasi serta sistem secara berkala, baik di lingkungan lokal maupun hosting, juga menjadi langkah krusial dalam menjaga perlindungan terhadap kerentanan. Selain itu, penerapan layanan monitoring seperti IDS/IPS dapat membantu dalam mendeteksi dan mencegah potensi ancaman yang muncul di lingkungan produksi.