BAB V
PENUTUP

5.1 Kesimpulan

Analisis kerentanan pada website Launchinpad Repository Management Project telah mengungkap sejumlah kerentanan yang dapat membahayakan keamanan dan integritas sistem. Temuan ini menyoroti pentingnya peninjauan keamanan secara teratur dalam pengelolaan website dan pengembangan perangkat lunak. Kerentanan seperti keterbukaan file *info.php* dan *IDOR URL Manipulation* menunjukan bahwa ada celah signifikan dalam proteksi keamanan sistem. Tindakan perbaikan yang tepat harus segera diambil untuk mengatasi kerentanan-kerentanan ini dan mencegah penyalahgunaan atau eksploitasi lebiih lanjut. Selain itu, penelitian ini menerapkan pentingnya kesadaran akan keamanan pada semua tahap pengembangan perangkat lunak. Tim pengembang perlu dilatih secara berkala untuk mengenali dan mengatasi kerentanan keamanan serta memprioritaskan keamanan sebagai bagian integral dari siklus pengembangan perangkat lunak.

Dengan mengambil tindakan yang tepat berdasarkan temuan analisis kerentanan, yang menggunakan atau mengelola website Launchinpad Repository Management Project dapat meningkatkan tingkat keamanan dan mengurangi risiko serangan serta pencurian data yang mungkin terjadi. Kesimpulannya, penelitian ini menegaskan pentingnya pengawasan keamanan yang berkelanjutan dalam pengelolaan website dan pengembang perangkat lunak serta memberikan dasar untuk perbaikan keamanan yang diperlukan untuk melindung sistem dari ancaman yang mungkin timbul.

5.2 Saran

Penelitian ini dilakukan dengan melakukan *penetration testing* dan metode *NIST* sehingga masih banyak cara yang digunakan berkaitan dengan metode tersebut. Saran ini menyajikan rangkuman temuan utama dari penelitian keamanan website beserta rekomendasi untuk meningkatkan keamanan secara keseluruhan dengan keterbatasan pada penelitian. Berikut saran yang dapat dilakukan :

1. Melakukan pengujian *penetration testing*
2. Melakukan *penetration testing* metodologi OWASP TOP 10, EXPLOIT-DB
3. Melaksanakan praktik pengembangan yang aman, termasuk pengguna input validasi, enkripsi data, dan manajemen sandi yang kuat
4. Melibatkan pengujian keamanan atau ahli sebagai *penetration tester* untuk mengidentifikasi dan memperbaiki kerentanan yang baru muncul
5. Memperbarui dan mengoptimalkan konfigurasi server untuk mengurangi potensi kerentanan dan meningkatkan keamanan