BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian terhadap *Website* Pemerintah Kabupaten Bima menggunakan metode *Vulnerability Assessment* dengan *tools* Who.is, NsLookup, dan OWASP ZAP, ditemukan 13 kerentanan dengan tingkat risiko bervariasi. Salah satu kerentanan dengan tingkat risiko tinggi adalah *PII Disclosure* yang berpotensi membocorkan informasi pribadi pengguna. Selain itu, ditemukan kerentanan lainnya seperti *Missing Anti-clickjacking Header, Content Security Policy Not Set, dan Cross-Domain JavaScript Inclusion* yang termasuk dalam risiko sedang hingga rendah. Semua temuan dikategorikan sesuai dengan standar OWASP Top 10 versi 2021.

Penelitian ini menunjukkan bahwa *website* pemerintah daerah masih memiliki celah keamanan signifikan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab jika tidak segera ditangani. Dengan demikian, pengujian keamanan secara berkala sangat disarankan.

5.2 Saran

Berdasarkan Kesimpulan dan Keterbatasan penelitian yang sudah dijelaskan diatas saran penelitian sebagai berikut:

1. Perlu dilakukan peninjauan berkala terhadap keamanan *website* Pemerintah Kabupaten Bima, khususnya terhadap kerentanan dengan risiko tinggi seperti *PII Disclosure*, agar data pribadi pengguna tidak bocor dan dapat dilindungi dengan baik.
2. Penerapan kebijakan keamanan server secara menyeluruh sangat disarankan, seperti penambahan header keamanan (*Content Security Policy, X-Frame-Options, Strict-Transport-Security*, dan lainnya) serta penggunaan sertifikat SSL yang valid agar *website* dapat memenuhi standar keamanan minimal OWASP.
3. Sebaiknya pihak pengelola sistem informasi melakukan pelatihan atau workshop keamanan informasi untuk meningkatkan pemahaman dan

kesadaran tim pengelola IT terhadap praktik pengamanan sistem berbasis web.

4. Penelitian lanjutan dapat dilakukan dengan memperluas metode uji keamanan, misalnya menggunakan pendekatan penetration testing, red teaming, atau framework NIST SP 800-115 secara penuh, agar pengujian mencakup eksploitasi dan validasi celah keamanan.
5. Dalam proses penelitian, peneliti mengalami keterbatasan dalam pengujian secara menyeluruh, terutama karena pendekatan yang digunakan bersifat *non-intrusive*, sehingga hanya mendeteksi potensi kerentanan tanpa melakukan eksploitasi langsung. Oleh karena itu, kolaborasi dengan tim keamanan dari instansi terkait akan sangat membantu dalam mendapatkan hasil yang lebih lengkap dan valid.
6. Diharapkan skripsi ini dapat menjadi referensi awal bagi penelitian di bidang keamanan siber, terutama bagi instansi pemerintah daerah lain yang ingin memulai evaluasi keamanan terhadap sistem informasi publik yang mereka miliki.