BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan hasil pengujian keamanan yang telah dilakukan terhadap website ERP PT. XYZ pada halaman yang bisa diakses oleh pengguna dengan role SPV Marketing dengan teknik *penetration testing* menggunakan metode PTES berdasarklan OWASP Top 10, maka diperoleh beberapa kesimpulan sebagai berikut:

1. Pengujian keamanan website ERP PT. XYZ pada halaman yang dapat diakses oleh pengguna dengan *role* SPV Marketing dilakukan menggunakan metode PTES, yang menyediakan kerangka kerja *penetration testing* yang sistematis. Proses pengujian ini mencakup tujuh tahapan utama, dimulai dari *pre-engagement interaction*, *intelligence gathering*, *threat modeling*, *vulnerability analysis*, *exploitation*, *post-exploitation*, dan *reporting*. Setiap tahapan memiliki peran penting dalam keseluruhan proses pengujian. Tahapan pertama, *pre-engagement interaction*, berfokus pada pengaturan legalitas dan persetujuan pengujian. Pada tahap *intelligence gathering*, informasi terkait target yang akan diuji dikumpulkan. Selanjutnya, tahap *threat modeling* digunakan untuk mengidentifikasi aset serta aktor yang dapat mengancam aset yang telah diidentifikasi. Pada tahap *vulnerability analysis*, pemindaian kerentanan dilakukan menggunakan OWASP ZAP untuk menemukan potensi celah keamanan. Tahap *exploitation* menguji validitas kerentanan pada web target berdasarkan kerentanan yang telah diidentifikasi pada tahap sebelumnya. Tahap *post-exploitation* berfokus pada eksploitasi lebih lanjut untuk mengakses informasi sensitif dan mempertahankan hak akses. Tahap terakhir, *reporting*, menyajikan hasil temuan selama proses pengujian serta rekomendasi perbaikan. Selain itu, OWASP Top 10 digunakan untuk mengkategorikan kerentanannya yang ditemukan selama pemindaian menggunakan OWASP ZAP, serta memberikan panduan perbaikan terhadap kerentanannya yang telah teridentifikasi.
2. Hasil pemindaian OWASP ZAP pada website ERP PT. XYZ pada halaman yang dapat diakses oleh *role* SPV Marketing menunjukkan adanya 23 celah keamanan, yang terdiri dari 2 kerentanan dengan risiko tinggi, 6 kerentanan dengan risiko sedang, 9 kerentanan dengan risiko rendah, dan 4 kerentanan *informational*. Sehingga dari jumlah tersebut terdapat 18 kerentanan yang termasuk dalam kategori

OWASP Top 10, yakni *Broken Access Control*, *Injection*, *Insecure Design*, *Security Misconfiguration*, *Vulnerable and Outdated Components*, *Software and Data Integrity Failures*. Pengujian dilakukan terhadap kerentanan dengan risiko tinggi yang terdiri dari *Cloud Metadata Potentially Exposed* dan *Vulnerable JS Library*. Kemudian pengujian juga dilakukan pada kerentanan dengan risiko sedang yang terdiri dari *Absence of Anti-CSRF Tokens*, *Application Error Disclosure*, *CSP Header Not Set*, *Missing Anti-clickjacking Header*, dan *Vulnerable JS Library*. Selain itu, pengujian juga dilakukan pada kerentanan dengan risiko rendah yang terdiri dari *Big Redirect Detected*, *Cookie No HttpOnly Flag*, *Cookie Without Secure Flag*, *Cookie without SameSite Attribute*, *Cross-Domain Javascript Source File Inclusion*, *Server Leaks Version Information via "Server" HTTP Response*, *Strict-Transport-Security Header Not Set*, *Timestamp Disclosure – Unix,* dan *X-Content-Type-Options Header Missing*.

5.2. Saran

Berdasarkan hasil pengujian keamanan yang telah dilakukan, saran terhadap penelitian selanjutnya diharapkan dapat menambah alat pemindaian yang lebih bervariasi. Sehingga selain menggunakan OWASP ZAP, dapat dipertimbangkan untuk mengkombinasikan dengan alat pemindaian lainnya, seperti Acunetix, Nikto, dan Nessus, agar memberikan perspektif berbeda dalam mengidentifikasi kerentanan.