BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan untuk mengevaluasi kesiapan keamanan informasi pada website Bakpia Tamansari dan Semakar Adventure Shop menggunakan tools metasploit, nmap, SQLmap, nikto, OWASP ZAP. Dapat disimpulkan bahwa kedua website memiliki kesiapan yang berbeda dalam penerapan kontrol keamanan informasi.

1. **Kesiapan Keamanan Web Bakpia Tamansari:** Website Bakpia Tamansari menunjukkan tingkat kesiapan yang lebih baik dalam mengimplementasikan beberapa kontrol keamanan dasar, seperti pengelolaan akses dan perlindungan terhadap serangan SQL Injection. Pemindaian Metasploit dan SQLMap mengungkapkan bahwa tidak ada kerentanan SQL Injection yang ditemukan, dan risiko terkait serangan brute-force pada port SSH dapat diminimalkan dengan penerapan autentikasi multifaktor (MFA). Namun, kelemahan pada header keamanan seperti X-Frame-Options dan X-Content-Type-Options menunjukkan perlunya peningkatan perlindungan terhadap serangan berbasis web seperti clickjacking.
2. **Kesiapan Keamanan Web Semakar Adventure Shop:** Semakar Adventure Shop menunjukkan beberapa kelemahan signifikan, terutama dalam pengungkapan informasi sensitif seperti file composer.lock dan potensi serangan CSRF pada beberapa formulir. Selain itu, hasil pemindaian menunjukkan kurangnya implementasi kontrol teknis seperti header keamanan, yang meningkatkan risiko serangan clickjacking. Sama seperti Bakpia Tamansari, tidak ditemukan kerentanan SQL Injection, namun pengelolaan akses perlu diperkuat untuk melindungi port terbuka seperti FTP dan SSH.

5.2 Saran

Berdasarkan temuan dalam penelitian ini, saran yang dapat diberikan untuk meningkatkan keamanan informasi pada kedua website adalah sebagai berikut:

1. **Implementasi Multi-Factor Authentication (MFA):** Untuk mengurangi risiko akses tidak sah melalui port SSH, disarankan agar kedua website mengimplementasikan MFA untuk memperkuat autentikasi dan melindungi akses jarak jauh.
2. **Peningkatan Proteksi Header Keamanan:** Kedua website perlu menambahkan header keamanan yang penting seperti X-Frame-Options dan X-Content-Type-Options untuk mencegah serangan clickjacking dan MIME type confusion. Langkah ini akan meningkatkan keamanan dari potensi serangan berbasis web.
3. **Peningkatan Sistem Deteksi Anomali:** Disarankan agar kedua website menerapkan sistem deteksi intrusi (IDS) dan pemantauan aktif yang dapat mengidentifikasi dan merespons aktivitas mencurigakan secara real-time. Hal ini penting untuk mendeteksi serangan berbasis web atau upaya brute-force pada akses FTP dan SSH.
4. **Penguatan Prosedur Penanganan Insiden:** Prosedur penanganan insiden perlu diperkuat dengan dokumentasi yang jelas dan sistem logging yang lebih mendalam. Penanganan insiden yang cepat dan baik akan memastikan bahwa setiap ancaman dapat dikelola dengan baik sebelum menyebabkan kerusakan lebih lanjut.
5. **Proteksi Data Sensitif:** Semakar Adventure Shop perlu segera memperbaiki pengungkapan file sensitif seperti composer.lock dan memastikan bahwa file-file ini tidak dapat diakses secara publik. Melakukan audit rutin terhadap file yang tersedia di server akan membantu mengurangi risiko serangan yang memanfaatkan informasi sensitif.

Dengan menerapkan saran-saran di atas, diharapkan kedua website dapat meningkatkan keamanan informasi mereka secara signifikan sesuai dengan

standar kemanan informasi yang berlaku, sehingga dapat melindungi data pengguna dan aset informasi mereka dengan lebih baik.