BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk dunia bisnis dan transaksi digital. *Website* menjadi salah satu sarana utama dalam komunikasi, penyebaran informasi, serta transaksi daring. Namun, di balik kemudahan dan manfaat yang ditawarkan, terdapat ancaman keamanan yang dapat membahayakan data serta sistem informasi yang tersimpan di dalamnya.

BagiBagi.co merupakan platform berbasis *website* yang digunakan dalam operasional bisnisnya. Platform ini menangani berbagai transaksi dan menyimpan data sensitif pengguna, seperti informasi pribadi, kredensial akun, serta riwayat transaksi. Keberadaan data-data ini menjadikan BagiBagi.co sebagai target potensial bagi serangan *cyber* yang bertujuan mencuri, merusak, atau mengeksploitasi sistem yang ada.

Ancaman terhadap *website* dapat berbentuk serangan seperti *SQL Injection*, pemindaian dengan *Nmap*, eksploitasi kerentanan menggunakan *Nessus*, serta serangan berbasis *WordPress* dengan *WPScan*. Jika serangan tersebut berhasil, maka dapat berakibat serius terhadap integritas, ketersediaan, serta kerahasiaan data di dalam BagiBagi.co. Oleh karena itu, untuk mengidentifikasi dan mengevaluasi tingkat keamanan website ini, diperlukan pengujian keamanan menggunakan metode Vulnerability assessment (VA).

Beberapa penelitian sebelumnya telah membahas aspek keamanan *website* dengan pendekatan yang beragam. Hasibuan et al. (2022) menggunakan *OWASP ZAP* untuk menganalisis kerentanan *website* melalui *vulnerability assessment*. Meskipun metode ini efektif dalam mendeteksi

celah keamanan berbasis web, penelitian ini belum mengulas eksploitasi lanjutan maupun mitigasi secara komprehensif.

Penelitian yang dilakukan oleh Medianto (2022) lebih menyoroti keamanan jaringan lokal dengan pendekatan *penetration testing* menggunakan *DHCP Snooping*. Meskipun penelitian ini memberikan wawasan tentang pencegahan serangan berbasis jaringan, cakupannya belum menyentuh eksploitasi pada aplikasi berbasis web yang menjadi fokus dalam penelitian ini.

Sofyan et al. (2022) menerapkan *penetration testing* pada *website* institusi pendidikan menggunakan metode *OWASP* dan *ISAAF*. Hasil pengujian menunjukkan adanya kerentanan dengan tingkat risiko tinggi, sedang, dan rendah. Namun, penelitian ini hanya menggunakan *Acunetix* sebagai alat pengujian, sehingga analisisnya masih dapat diperluas dengan pendekatan lain yang lebih beragam.

Sementara itu, penelitian yang dilakukan oleh Wakida dan Servandab (2022) meneliti penggunaan *Nessus* dalam mengidentifikasi celah keamanan pada perangkat komputer. Hasilnya menunjukkan bahwa *Nessus* efektif dalam mendeteksi berbagai jenis kerentanan, termasuk pada sistem operasi dan aplikasi. Namun, penelitian ini terbatas pada perangkat komputer dan belum mengupas keamanan *website* secara khusus.

Penelitian ini menerapkan pendekatan vulnerability assessment berdasarkan metodologi *NIST SP 800-115* dengan menggunakan *Kali Linux* sebagai sistem operasi utama. Berbagai alat digunakan dalam pengujian ini, seperti *WhatWeb*, *OWASP ZAP*, *WhatWaf*, *Whois*, *SQLMap*, *DIRB*, *Python Custom Script*, dan *Nessus*. Diharapkan pengujian ini dapat mengidentifikasi tingkat kerentanan *website* BagiBagi.co terhadap berbagai ancaman *cyber* serta memberikan rekomendasi solusi untuk meningkatkan keamanan sistemnya. Selain itu, penelitian ini menawarkan kontribusi dengan mengombinasikan berbagai alat *vulnerability assessment* serta melakukan

eksploitasi lebih lanjut guna memberikan analisis yang lebih mendalam dibandingkan penelitian sebelumnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disajikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Apa saja kerentanan yang ditemukan pada *website* BagiBagi.co ?
2. Bagaimana penerapan metode *Vulnerability assessment* berbasis *NIST SP 800115* dalam mengidentifikasi kerentanan ?
3. Apa saja rekomendasi yang tepat untuk meningkatkan keamanan *website* BagiBagi.co ?

1.3 Tujuan Penelitian

Adapun tujuan yang diharapkan dapat tercapai dari penelitian ini sebagai berikut:

1. Mengidentifikasi tingkat kerentanan pada *website* BagiBagi.co.
2. Menerapkan metode *Vulnerability assessment* sesuai dengan *NIST SP 800115*.
3. Memberikan rekomendasi untuk memperbaiki sistem keamanan

1.4 Manfaat

Penelitian ini diharapkan dapat memberikan informasi mendalam terkait kerentanan dalam keamanan *website* BagiBagi.co, sehingga pengelola dapat melakukan perbaikan dan penguatan sistem keamanan guna untuk mencegah ancaman serangan *cyber*.

1.5 Batasan Masalah

1. Penelitian ini hanya mengacu berdasarkan *OWASP TOP 10* tahun 2021.
2. Pada metodelogi yang dipakai dipenelitian ini, dilakukan dengan menggunakan metode *NIST SP 800-115 Vulnerability assessment.*
3. Pengujian hanya dilakukan dengan menggunakan *black box security testing*.