BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era globalisasi saat ini, pertukaran informasi yang cepat dan akses informasi yang mudah telah menjadi suatu keharusan bagi masyarakat. Sebelumnya, jika seseorang ingin mencari tahu tentang lokasi wisata di suatu daerah, mereka harus mencari buku atau majalah yang membahas tentang daerah tersebut, namun saat ini seseorang tersebut dapat mencari informasi yang dia butuhkan di internet. Semua kalangan masyarakat sudah tidak asing dengan keberadaan internet, bahkan internet telah menjadi kebutuhan dalam kegiatan sehari-hari. Salah satu contoh penggunaan dan pemanfaatan internet adalah *website*.

Website merupakan sebuah sistem yang menyimpan dan menyajikan informasi dalam bentuk teks, gambar, suara, dan lain-lain yang kemudian disimpan dalam bentuk dokumen dinamis. *Website* memiliki peran penting dalam pertukaran informasi, karena dapat menyajikan informasi secara cepat dan tepat. Penyebaran informasi melalui *website* juga sangat cepat, mencakup area yang luas, serta tidak dibatasi oleh jarak dan waktu. Dengan kelebihan tersebut, tidak heran jika semakin banyak yang menggunakan *website* sebagai media informasi. Namun, seperti teknologi pada umumnya, *website* juga memiliki kekurangan. Jika pengembang melakukan kesalahan dalam *coding* atau kesalahan konfigurasi, *website* akan

memiliki kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab[1].

Vulnerability atau kerentanan pada *website* merupakan sebuah celah keamanan yang terbentuk dari kesalahan *coding*, kesalahan konfigurasi, atau kelemahan dalam komponen dan proses dari suatu *website*. Kerentanan tersebut dapat dimanfaatkan oleh penyerang untuk mendapatkan akses kedalam sistem atau data[2]. Berdasarkan laporan bulanan dari BSSN, pada tahun 2022, kasus peretasan *website* di Indonesia mencapai 89 kasus untuk bulan Desember tahun 2022. Tingginya jumlah kasus peretasan di Indonesia menunjukkan bahwa kerentanan pada *website* bukanlah hal yang dapat dianggap remeh. Kerentanan dalam *website* dapat diketahui dengan melakukan evaluasi pada *website* tersebut. Salah satu cara untuk melakukan evaluasi adalah dengan melakukan vulnerability scanning.

Vulnerability scanning adalah proses untuk mencari celah keamanan pada suatu sistem dengan menggunakan tools atau alat yang berjalan otomatis. *Vulnerability scanning* biasanya dilakukan oleh departemen IT dalam suatu perusahaan atau perusahaan yang menawarkan jasa *cyber security*. Proses scanning ini juga dilakukan oleh penyerang untuk mencari celah masuk ke sistem. Berbeda dengan *penetration testing*, dimana seorang pentester diharuskan untuk menggali kerentanan tersebut lebih dalam dengan melakukan *exploit* dan menganalisis penyebab dari kerentanan pada sistem[1]. *Vulnerability scanning* hanya mencari kelemahan dan celah pada sistem, melakukan analisis terhadap *vulnerability* yang ditemukan dan kemudian melaporkan hasilnya.

Berdasarkan uraian-uraian di atas, penulis ingin melakukan analisis keamanan pada *website* milik Direktorat Inovasi dan Inkubator Bisnis Universitas Bina Darma, yaitu SIDESPIN dengan alamat web www.sidespin.id. *Website* SIDESPIN adalah media yang menyediakan informasi seputar desa, terutama pada desa di daerah terdepan, terluar, dan terdalam. Tujuan dari *website* SIDESPIN adalah untuk membantu desa tersebut lebih dikenal banyak orang dengan menyediakan informasi tentang sejarah, adat dan budaya, serta lokasi wisata di desa tersebut. Penulis akan melakukan analisis keamanan pada *website* ini menggunakan teknik *vulnerability scanning*. Kerentanan yang penulis temukan nantinya akan dianalisis lebih lanjut berdasarkan standar OWASP, setelahnya akan dibuat kesimpulan serta memberikan rekomendasi untuk mengatasi kerentanan tersebut. Penulis akan membuat penelitian ini dalam bentuk skripsi yang berjudul "Analisis Keamanan *Website* SIDESPIN menggunakan Teknik *Vulnerability Scanning*".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka permasalahan yang akan dibahas dalam penelitian ini adalah bagaimana cara mencari celah keamanan pada *website* Sidespin dan *website* resmi milik Universitas Bina Darma menggunakan teknik *vulnerability scanning* serta memberikan rekomendasi untuk memperbaiki celah keamanan tersebut.

1.3 Tujuan Penelitian

Pada penelitian ini penulis memiliki tujuan seperti berikut:

1. Melakukan pemindaian celah keamanan pada *website* SIDESPIN menggunakan tools scanning Owasp Zap, Nikto, dan Nessus.
2. Melakukan analisis kerentanan *website* SIDESPIN berdasarkan hasil pemindaian celah keamanan dari tools scanning yang digunakan.
3. Menjelaskan dan membuat laporan tentang keamanan yang ditemukan pada *website* SIDESPIN serta memberikan rekomendasi untuk mengurangi atau memperbaiki kerentanan tersebut.

1.4 Ruang Lingkup dan Batasan Masalah

Ruang lingkup dan batasan masalah biasanya diberikan agar penelitian dapat terfokus dan tetap pada tujuan yang sudah diuraikan sebelumnya. Beberapa batasan yang akan penulis berikan dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini akan melakukan analisis celah keamanan berdasarkan teknik *vulnerability scanning* tanpa *social engineering*.
2. Jika celah keamanan ditemukan, penulis tidak akan melakukan *exploit* untuk masuk ke dalam sistem.
3. Penerapan rekomendasi akan penulis serahkan pada pengelola *website* sidespin.id.

1.5 Manfaat Penelitian

Pada penelitian ini diharapkan dapat memberikan manfaat sebagai berikut ini:

1. Dapat mengetahui kondisi serta tingkat kerentanan *website* sidespin.id.
2. Dapat meningkatkan keamanan *website* dengan memberikan rekomendasi berdasarkan analisis celah keamanan.

1.6 Metodologi Penelitian

1.6.1 Tempat dan Waktu Penelitian

Penelitian ini dilakukan di Universitas Bina Darma Palembang pada bulan Juli sampai Oktober 2023.

1.6.2 Metode Penelitian

Penelitian ini menggunakan metode Action Research atau penelitian tindakan. Menurut (Susanto, 2020), a*ction research* adalah metode yang dimana peneliti masuk ke dalam subjek penelitian dan melakukan intervensi di dalam subjek penelitian serta mengamati dan mendokumentasi apa yang terjadi. Berdasarkan pendapat di atas, maka dapat penulis simpulkan bahwa *Action Research* adalah metode yang mengharuskan peneliti untuk ikut terlibat dengan subjek penelitiannya untuk mengamati dan mendokumentasikan setiap peristiwa yang terjadi pada subjeknya, serta melakukan intervensi jika diperlukan.

1.6.3 Metode Pengujian dan Analisis

Penelitian ini akan menggabungkan teknik *footprinting* dan *information gathering* untuk mencari informasi lebih lanjut tentang target sebelum melakukan *vulnerability scanning*. Penulis telah menyesuaikan metode dan teknik tersebut dengan tahapan penelitian yang dibagi dalam lima tahapan. Tahapan tersebut sebagai berikut:

1. *Scope* (Ruang Lingkup)

   Penelitian ini akan diawali dengan menentukan batasan atau *scope* terhadap *website* yang akan diuji. Dalam penelitian ini penulis hanya akan melakukan *vulnerability scanning* tanpa melakukan *social engineering* dan *exploit* pada sistem seperti mengubah tampilan, mencoba masuk ke *admin panel*, dan lain-lain.

2. *Footprinting* dan *Information Gathering*

   Tahapan ini dilakukan untuk mencari dan mendapatkan informasi sebanyak mungkin tentang target. Seperti versi sistem operasi, IP *address*, *port* yang terbuka, dan lain-lain.

3. *Vulnerability Scanning*

   Tahapan utama dalam penelitian ini. Penulis akan memanfaatkan berbagai tools dan *vulnerability scanner online* untuk mencari celah keamanan pada *website* yang diuji.

4. *Vulnerability Analysis*

   Pada tahap ini penulis akan menganalisis informasi vulnerability yang ditemukan setelah proses *scanning* serta memberikan rekomendasi untuk memperbaiki *vulnerability* yang ditemukan.

5. *Report* (Dokumentasi dan Laporan)

   Di tahap ini penulis akan mendokumentasikan hasil analisa celah keamanan agar pengelola dapat mengetahui apa saja yang telah dilakukan penulis.

1.6 Jadwal Penelitian

Jadwal penelitian adalah serangkaian tabel yang memperlihatkan tahapan secara lengkap dan sistematis. Berikut ini adalah jadwal penelitian yang telah dilakukan penulis.

Tabel 1.1 *Jadwal Penelitian*

		Tahun 2023			
No	Kegiatan	Juli	Agustus	September	Oktober
1	*Scope*				
2	*Footprinting and InformationGathering*				
3	*Vulnerability Scanning*				
4	*Vulnerability Analysis*				
5	*Report*				

Keterangan:

Belum Dilakukan Telah Dilakukan

1.8 Sistematika Penulisan

Untuk mempermudah pemahaman yang lebih terperinci mengenai tulisan yang akan dijelaskan, penulis menguraikan secara ringkas sistem penulisan menjadi beberapa bagian utama. Struktur ini memberikan gambaran lebih rinci tentang organisasi penulisan dalam beberapa bab yang terlihat sebagai berikut:

BAB I: PENDAHULUAN

Pada Bab ini menjelaskan tentang Latar Belakang, Perumusan Masalah, Tujuan Penelitian, Batasan Masalah, Manfaat Penelitian, Metodologi Penelitian dan Sistematika Penulisan.

BAB II: TINJAUAN PUSTAKA

Dalam Bab ini menjelaskan hasil-hasil dari penelitian terdahulu yang menginspirasi dan melandasi pelaksanaan penelitian serta mengulas landasan teoritik yang berhubungan dengan penelitian yang dilakukan.

BAB III: METODOLOGI PENELITIAN

Bab ini akan menjelaskan tentang metode penelitian, metode pengujian dan analisis yang penulis gunakan serta tahapan-tahapan dalam penelitian ini.

BAB IV: HASIL DAN PEMBAHASAN

Pada Bab ini memberikan penjelasan tentang pengujian dan analisis pada *website* www.sidespin.id serta membahas tentang celah keamanan yang ditemukaan.

BAB V: KESIMPULAN DAN SARAN

Pada Bab ini memberikan penjelasan tentang uraian kesimpulan dan saran dari keseluruhan Bab yang dibuat serta mencoba memberikan saran-saran yang diharapkan berguna untuk mengatasi masakah yang dihadapi.