BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi membuat berbagai aktivitas manusia menjadi lebih mudah. Salah satu teknologi yang sering digunakan dalam aktivitas sehari-hari adalah *website* atau situs web, sehingga keamanan *website* saat ini menjadi salah satu perhatian utama dalam pengembangan dan pemeliharaan sistem digital, dikarenakan *website* yang aman tidak hanya melindungi informasi yang sensitif, tetapi juga menjaga kredibilitas dan kepercayaan pengguna terhadap sistem tersebut [1]. Salah satu *website* yang sangat perlu dijaga keamanannya yaitu *website* sistem informasi Pangkalan Data Pendidikan Tinggi (PDDikti). *Website* Pangkalan Data Pendidikan Tinggi (PDDikti) ini berfungsi sebagai platform penting yang menyediakan data dan informasi terkait institusi pendidikan di Indonesia [2]. Namun, dengan meningkatnya penggunaan teknologi informasi, ancaman terhadap keamanan *website* juga semakin meningkat. Serangan siber seperti peretasan, pencurian data, dan serangan *DDoS* dapat mengakibatkan kerugian yang sangat signifikan bagi pengguna serta penyedia layanan.

Maka dari itu, *website* PDDikti yang merupakan sumber informasi resmi sangat rentan menjadi target dari berbagai jenis serangan siber seperti *SQL injection*, *Cross-Site Scripting (XSS)*, dan serangan *Denial of Service (DoS)*. Penelitian sebelumnya menunjukkan bahwa banyak aplikasi web di lingkungan pendidikan tinggi memiliki celah keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Misalnya, analisis celah keamanan pada aplikasi *e-learning* di berbagai universitas mengungkapkan adanya kerentanan seperti *Cross-Site Request Forgery (CSRF)* dan penggunaan enkripsi *HTTPS* yang lemah [3]. Kejadian pelanggaran keamanan dapat berpotensi menimbulkan dampak yang cukup serius, baik dalam hal kerugian materil

maupun kerugian reputasi. Oleh karena itu, untuk menjaga integritas sistem dan melindungi data yang sensitif, evaluasi keamanan secara menyeluruh perlu dilakukan.

Salah satu cara yang paling umum digunakan untuk mengidentifikasi celah keamanan adalah dengan melakukan *penetration testing* atau uji penetrasi. Metode ini memungkinkan pengujian kerentanan secara menyeluruh pada sistem melalui simulasi serangan, yang dilakukan oleh individu atau tim dengan izin tertentu. Dalam penelitian ini, metode *penetration testing* yang digunakan akan dipadukan dengan kerangka kerja (*framework*) *Information Security Assessment Framework (ISSAF)*. Penggunaan *framework ISSAF* memberikan struktur yang sistematis dalam melakukan penilaian keamanan. *Framework* ini mencakup berbagai aspek penting dari keamanan informasi, mulai dari identifikasi resiko hingga pengujian kontrol keamanan yang ada.

Sebelumnya, sudah ada penelitian lain yang memiliki tujuan yang sama, yaitu menganalisis kerentanan keamanan pada laman PDDikti yang dilakukan oleh Hassanah, Ryansyah, Setiawan, dan Alamsyah pada 2025. Fokus penelitian ini bertujuan mengidentifikasi kerentanan pada halaman PDDikti menggunakan kombinasi *OWASP ZAP* dan pengujian manual [4].

Berdasarkan latar belakang yang telah disampaikan, dapat disimpulkan bahwa dengan meningkatnya penggunaan teknologi, ancaman terhadap informasi serta keamanan *website* juga semakin meningkat. Serangan siber seperti peretasan, pencurian data, dan serangan *DDoS* dapat mengakibatkan kerugian yang signifikan bagi pengguna maupun penyedia layanan. Oleh karena itu, dalam penelitian ini, peneliti tidak hanya akan menganalisis kerentanan keamanan, tetapi juga akan melakukan *penetration testing* terhadap laman PDDikti, dengan tujuan untuk mengetahui apakah laman tersebut sudah aman dan layak digunakan.

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana metode *penetration testing* dapat diterapkan guna untuk menganalisis celah keamanan pada website PDDikti?
2. Apa saja celah keamanan yang terdapat pada *website* PDDikti?
3. Bagaimana *framework ISSAF* dapat membantu dalam melakukan *penetration testing* secara terstruktur pada *website* PDDikti?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Penelitian ini akan membatasi penggnunaan metode *penetration testing* dengan hanya menggunakan teknik-teknik dasar yang sesuai dengan standar keamanan *web* umum, seperti pengujian *Cross-site Scripting (XSS), DDoS Attack* dan serangan *port* 21 menggunakan *Metasploit*.
2. Analisis celah kemanan pada penelitian ini hanya akan mencakupi kerentanan yang sangat umum ditemukan pada aplikasi *web* dan yang cukup relevan dengan sistem PDDikti. Tidak semua jenis kerentanan keamanan akan diuji dikarenakan focus penelitian ini akan dibatasi pada identifikasi dan analisis kerentanan yang dapat terdeteksi dengan metode *penetration testing* menggunakan *ISSAF.*
3. Penerapan *framework ISSAF* yang akan digunakan dalam penelitian ini dibatasi pada tahap-tahap utama yang meliputi perencanaan, pengumpulan informasi, dan identifikasi kerentanan. Penelitian ini tidak akan mencakup seluruh modul *ISSAF* secata lengkap, tetapi hanya komponen yang paling relevan dengan keamanan aplikasi *web* untuk memastikan uji penetrasi dapat dilakukan secara terstruktur dan sesuai prosedur.

Dengan batasan-batasan ini, penelitian diharapkan dapat memberikan hasil yang fokus dan relevan dalam konteks keamanan *website* PDDikti tanpa melebihi ruang lingkup yang ada.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisis celah keamanan yang ada pada website PDDikti dengan menggunakan metode *penetration testing* dan *framework ISSAF.* Dengan melakukan analisis ini, diharapkan dapat ditemukan celah-celah keamanan yang ada serta dapat memberikan rekomendasi (saran) untuk perbaikan yang diperlukan guna menigkatkan keamanan *website* PDDikti. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi yang cukup signifikan pada pengembangan sistem keamanan *website*, khususnya pada situs yang memiliki peran penting dalam manajemen data Pendidikan tinggi di Indonesia.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi kerentanan (kelemahan) serta celah keamanan yang ada pada situs *web* PDDikti. Dengan mengetahui kerentanan tersebut, diharapkan pihak pengelola *website* dapat mengambil langkah-langkah yang tepat guna memperbaiki situs *web* agar menjadi lebih aman.
2. Penelitian ini diharapkan dapat menjadi panduan praktis bagi pengelola situs *web* PDDikti dalam memahami dan menerapkan metode *penetration testing* serta *framework ISSAF.* Hal ini dapat membantu pengelola situs *web* dalam melakukan evaluasi keamanan secara berkelanjutan.
3. Penelitian ini diharapkan dapat berkontribusi terhadap peningkatan keamanan informasi terutama disektor pendidikan tinggi, khususnya di Indonesia. Hal ini penting untuk melindungi data sensitif yang sedang dikelola oleh institusi pendidikan.

4. Hasil penelitian ini dapat menjadi dasar bagi penelitian lebih lanjut dibidang keamanan siber, khususnya dalam konteks aplikasi *web* di lingkungan pendidikan. Ini dapat membuka peluang untuk studi yang lebih mendalam mengenai aspek-aspek lain dari keamanan informasi.

Dengan manfaat-manfaat tersebut penelitian ini diharapkan tidak hanya berfokus pada analisa teknis, namun juga pada aspek praktis yang dapat diterapkan guna untuk meningkatkan kemanaan situs *web* PDDikti secara menyeluruh.

1.6 Sistematika Penulisan

Sistematika penulisan pada penelitian ini adalah sebagai berikut:

1. BAB 1 PENDAHULUAN

   Bab ini berisikan penjelasan latar belakang penelitian, rumusan dan batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

2. BAB 2 TINJAUAN PUSTAKA

   Bab ini berisikan tinjauan pustaka yang berkaitan dengan penelitian yang dilakukan.

3. BAB 3 METODOLOGI PENELITIAN

   Bab ini berisikan langkah-langkah serta penjelasan dari metodologi penelitian yang digunakan dalam penelitian ini.

4. BAB 4 HASIL DAN PEMBAHASAN

   Bab ini berisikan hasil dari penelitian yang dilakukan serta pembahasan dari hasil yang telah diperoleh.

5. BAB 5 SIMPULAN DAN SARAN

   Bab ini berisikan kesimpulan dari penelitian yang telah dilakukan serta saran untuk penelitian selanjutnya.