BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini segala kegiatan manusia sangat dimudahkan dengan kehadiran teknologi. Muncul pula aplikasi-aplikasi popular yang dapat menyelesaikan masalah yang terdapat pada cara tradisional seperti perusahan penyedia aplikasi transportasi, *e-commerce*, *dashboard* mahasiswa.

Berkembangnya industri ini dengan secara cepat menyebabkan masalah yang besar pada sisi *security* dibanding waktu dulu. Ditambah ancaman yang disebabkan oleh virus atau malware semakin berkembang dan juga pengembangan aplikasi dari sisi *developer* yang kurang memikirkan sisi keamananya menyebabkan user sangat rentan untuk terserang kejahatan siber. Salah satu kasus serangan siber yaitu serangan deface yang terjdi pada website uinsgd.ac.id.

Adanya kesalahan manusia atau *human error* dalam pengembangan aplikasi ini perlu adanya penelitian sebagai solusi ataupun referensi yang dapat dipakai oleh *developer* dalam pengembagan aplikasinya. Salah satu organisasi terkait penanganan dan pencegahan masalah kemanan sistem adalah owasp. Owasp merupakan organisasi yang membahas segala sesuatu mengenai keamanan sistem, melalui owasp *top* 10, owasp merangkum kerentanan apa saja yang sering di eksploitasi oleh *hacker*. Oleh karena itu owasp top 10 menjadi rujukan mengenai keamanan sistem oleh banyak *cyber security expert*.

Penelitian terkini terkait dengan security pada aplikasi website masih sangat minim. Pada penelitian ini membahas mengenai keamanan pada aplikasi website beserta kerentanan yang sering disalahgunakan oleh *hacker*. Berdasarkan latar belakang di atas, maka pada penelitian ini diusulkan penelitian yang berjudul **"Pengujian Celah Keamanan**

Menggunakan Owasp Top 10 pada Domain uinsgd.ac.id Dengan Menerapkan Penetration Testing"

1.2 Perumusan Masalah

Berdasarkan latar belakang yang dipaparkan di atas, penulis memiliki beberapa rumusan masalah terkait dalam permasalahan tersebut, yaitu:

1. Apakah domain dan domain uinsgd memiliki celah?
2. Bagaimana cara mencari celah keamanan di website Universitas Islam Negeri Sunan Gunung Djati Bandung?

1.3 Tujuan Tugas Akhir

Berdasarkan rumusan masalah yang dipaparkan di atas, penulis memiliki beberapa tujuan terkait dalam permasalahan tersebut, yaitu:

1. Mengetahui domain dan domain memiliki celah keamanan atau tidak.
2. Mengetahui bagaimana *attacker/hacker* melancarkan serangan terhadap domain dan domain uinsgd.ac.id

1.4 Batasan Masalah

Berdasarkan rumusan masalah yang telah dipaparkan di atas, penulis membatasi masalah yang akan dianalisa pada pembuatan sistem ini. Adapun batasan-batasan tersebut yaitu:

1. Pengujian celah keamanan berdasarkan *owasp top 10* 2017 meliputi: *injection, sensitive data exposure, broken access control, security misconfiguration, cross site scripting(XSS)* dan *using component with known vulnerabilities.*
2. Pengujian celah keamanan di 2 domain uinsgd.ac.id, yaitu lms.uinsgd.ac.id/ dan https://salam.uinsgd.ac.id/portal/salam/

1.5 Metodologi

Metodologi yang digunakan dalam penelitian ini yaitu sebagai berikut:

1. Analisis Celah Keamanan

   Pada tahap ini merupakan tahap dimana penulis melakukan analisis terhadap aplikasi web yang bertujuan untuk menemukan celah keamanan atau kerentanan pada aplikasi web yang akan diuji.

2. Pengujian

   Pada tahap ini merupakan tahap dimana penulis melakukan pengujian terhadap aplikasi web dengan celah keamanan atau kerentanan yang diperoleh yang memiliki tingkat risiko paling tinggi serta melakukan pengujian yang mengacu pada literatur yang sudah ada.

3. Hasil Pengujian

   Pada tahap ini merupakan tahap penjelasan mengenai pengujian yang telah dilakukan terhadap aplikasi web yang diperoleh dari tahap sebelumnya.

4. Kesimpulan dan Saran

   Pada tahap ini merupakan tahap dimana akan dijelaskan mengenai kesimpulan dari hasil pengujian yang telah dilakukan pada aplikasi web yang diuji serta saran bagi penelitian selanjutnya.