BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Universitas adalah suatu institusi pendidikaan tinggi dan penelitian, yang memberikan gelar akademik dalam berbagai bidang. Universitas menyediakan pendidikan sarjana. Universitas Sahid Surakarta merupakan salah satu perguruan tinggi swasta terkemuka di Jawa Tengah. Dengan kualitas pendidikan yang tinggi, sehingga memberikan semangat mahasiswa dalam menempuh pendidikan sarjana. Untuk menjadi universitas yang baik Universitas Sahid Surakarta menyebarkan informasi secara cepat seputar pendidikan melewati *website* yang berdomain usahidsolo.ac.id dan memiliki subdomain penting seperti siakad.usahidsolo.ac.id dan admisi.usahidsolo.ac.id .

Namun dalam upaya pengelolaan website, harus berhati-hati terhadap penyerangan siber oleh pihak yang tidak bertanggung jawab, penyerang lebih sering dilakukan kepada Lembaga Pemerintahaan, Keuangan dan Berita, namun lembaga Pendidikan seperti Universitas Sahid Surakarta belum tentu aman dari serangan siber. Universitas Sahid Surakarta yang memanfaatkan website sebagai media untuk menyebarkan informasi tentang perkuliahan bisa juga mengalami serangan siber. Untuk mengecek histori dari salah satu bentuk penyerangan tersebut, dapat diketahui dari salah satu situs arsip *defacement,* yaitu http://zone-h.org , Zone-h adalah arsip yang berisi *mirror* dari sebagian besar situs web yang diretas. Berikut contoh arsip serangan terbaru yang telah terjadi pada web usahidsolo.ac.id menurut Zone-h pada tanggal 27 Desember 2020 terjadi redefacement pada domain usahidsolo.ac.id/xd.html oleh orang berinisial 0x1958 dan pada tanggal 17 Oktober 2013 awal mula terjadi homepage defacement dan mass defacement pada subdomain sistempkl.usahidsolo.ac.id oleh orang berinisial h4715 sebanyak 17 kali penyerangan.

Untuk mengatasi masalah ini salah satu langkah yang dapat ditempuh adalah dengan melakukan analisis terhadap sistem dan jaringan yang terdapat pada

Website Usahid Surakarta. Ada beberapa metode yang banyak digunakan untuk penetration testing salah satunya adalah metode OWASP 10. Metode ini cukup popular di dunia karena berisi daftar checklist yang berfungi untuk memastikan website telah aman atau belum. Penelitian ini berfokus pada pengumpulan informasi dan pengujian sistem yang ada dengan metode penetration testing berdasarkan metode Open Web Application Security Project Top 10 (OWASP 10) tahun 2017.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas maka perumusan masalah yang ditetapkan adalah "Bagaimana tingkat dan celah kerentanan keamanan pada domain website usahid.ac.id yang dapat merugikan Universitas Sahid Surakarta?".

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah dijelaskan di atas, batasan-batasan agar bisa terfokus dengan masalah yang ada maka batasan masalah dalam kasus ini adalah :

a. *Web* yang akan diuji adalah *web* yang menggunakan domain usahid.ac.id.
b. Pengujian dilakukan berdasarkan metode *Open Web Application Security Project* Top 10 (OWASP10) tahun 2017.
c. Tidak melakukan perbaikan program pada sisi keamanan terhadap *website* usahidsolo.ac.id.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dalam penelitian pengujian celah keamanan ini selain untuk menyelesaikan tugas akhir adalah Menguji keamanan website usahidsolo.ac.id terhadap serangan dari luar oleh orang yang tidak bertanggung jawab yang dapat merugikan pihak Universitas Sahid Surakarta.

1.4.2 Manfaat

Adapun manfaat yang dapat diambil dalam penelitian ini antara lain sebagai berikut ini :

a. Bagi Penulis

1) Penulis dapat mengimplementasikan ilmu pengetahuan yang selama ini diperoleh di perkuliahan.
2) Penulis mendapatkan wawasan dalam pembelajaran tentang OWASP.

b. Bagi Universitas Sahid Surakarta

1) Universitas dapat mengetahui seberapa rentang *web* Universitas Sahid Surakarta terhadap serangan yang tidak bertanggung jawab.
2) Universitas dapat mengetahui celah keamanan dari *web* Universitas Sahid Surakarta sehingga dapat melakukan penanggulang sejak dini.

1.5 Metodologi Penelitian

Metode yang digunakan dalam penyusunan tugas akhir ini adalah :

1.5.1 Teknik Pengumpulan Data

1) Observasi

Obrservasi adalah suatu cara untuk mengumpulkan data dengan melakukan penelitian secara langsung dengan datang ke staf bagian IT di Universitas Sahid Surakarta, hal ini untuk mengamati dan mencatat keadaan objek penelitian yang sedang diselidiki.

2) Wawancara

Wawancara merupakan proses komunikasi atau interaksi untuk mengumpulkan informasi dengan cara tanya jawab antara peneliti dengan informan atau subjek penelitian dengan kemajuan teknologi informasi seperti saat ini, wawancara bisa saja dilakukan tanpa tatap muka yakni melalui media telekomunikasi (Yuniati, 2017). Dalam tahap ini dilakukan proses tanya jawab dalam hubungan tatap muka dengan pihak *internal* Universitas dalam mengumpulkan data dan informasi mengenai *website* Universitas Sahid Surakarta.

3) Metode Literatur

Metode Literatur adalah metode pengambilan data dengan mempelajari literatur yang berupa buku, jurnal atau artikel ilmiah yang berhubungan dengan objek yang diteliti (Yuniati, 2017).

4) Metode Pengujian Sistem

Dalam pengujian penetration testing pada web berdomain usahidsolo.ac.id menggunakan metode OWASP tahun 2017 yang berfokus pada OWASP Top 10. OWASP Top 10 adalah panduan bagi para security team tentang kelemahan-kelemahan pada web yang mudah diserang dan harus segera disiasati. Terdapat 10 ancaman keamanan web yang ada pada OWASP Top 10 tahun 2017 yaitu : *Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Control, Security Misconfiguration, Cross Site Scripting, Insecure Deserialization, Using Components With Known Vulnerabilities, Insufficient Logging and Monitoring.*

1.6 Sistematika Penulisan

Sistematika penulisan dalam laporan Tugas Akhir nanti akan digambarkan secara menyeluruh mengenai masalah yang akan dibahas, secara garis besar dapat dilihat dari sistematika pembahasan dibawah ini :

BAB I PENDAHULUAN

Bab pendahuluan berisi tentang latar Latar Belakang, Perumusan Masalah, Batasan Masalah, Tujuan dan Manfaat Penulisan, Metodologi Penelitian serta Sistematika Penulisan Laporan.

BAB II LANDASAN TEORI

Bab ini menjelaskan mengenai gambaran umum tentang teori yang diterapkan dalam *penetration testing* menggunakan OWASP 10. Selain itu dalam bab ini juga menjelaskan tentang kerangka pikir, metode dan *tools* yang digunakan untuk melakukan *penetration testing.*

BAB III METODOLOGI

Bab ini peneliti akan menjelaskan tentang metode yang dilakukan dalam penelitian. Metode tersebut adalah pengumpulan data, analisis kebutuhan serta termasuk pengujian yang dilakukan secara sistematis.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang langkah-langkah proses pengujian yang dilakukan dan hasil yang didapat dari proses pengujian yang dilakukan terhadap beberapa target yang sudah ditentukan.

BAB V SIMPULAN DAN SARAN

Bab ini merupakan penutup, yang berisi kesimpulan dan rangkuman dari hasil pengujian yang telah dilakukan sebelumnya yang berupa hasil analisis pengujian, serta berisi saran-saran dari hasil pengujian..

DAFTAR PUSTAKA

LAMPIRAN