BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan kemajuan teknologi digital yang terus meluas, ancaman siber menjadi salah satu isu utama yang mempengaruhi banyak sektor industri. Teknologi operasional serta keamanan data perusahaan harus dijaga sebaik mungkin untuk melindungi seluruh informasi dari ancaman dan potensi kerusakan. Dalam konteks ini, PT Sekuriti Siber Indonesia memiliki pengaruh penting dalam menjaga keamanan siber melalui layanan yang disediakan, salah satunya adalah *Penetration Testing (Pentest)*.

Sebagai mahasiswa yang memiliki keterampilan dalam pengembangan aplikasi web, magang di PT Sekuriti Siber Indonesia memberikan pengetahuan baru secara langsung tentang pentingnya keamanan siber terhadap pengembangan aplikasi web. Secara teknis, pengetahuan yang didapatkan dan keterampilan yang dimiliki memang berbeda, namun kedua hal ini memiliki keterkaitan, khususnya dalam konteks melindungi aplikasi web dari ancaman dan potensi kerusakan dari serangan *siber*. Selama kegiatan magang, mahasiswa berkesempatan untuk belajar dan mempraktekkan teknik *Penetration Testing (Pentest)* yang bertujuan untuk memeriksa kerentanan dalam sistem aplikasi web.

Sementara itu, perusahaan juga mendapatkan manfaat dari partisipasi mahasiswa dalam pengembangan website *dummy* yang mirip dengan aplikasi web milik *perusahaan XYZ*. Website ini dibuat dengan celah keamanan yang disengaja

untuk di uji menggunakan metode *Penetration Testing*. Pengujian dilakukan untuk memberikan pemahaman tentang adanya celah keamanan yang ada pada website. Hasil dari pengujian ini memberikan beberapa manfaat, yaitu membantu perusahaan memahami cara meningkatkan keamanan sistem mereka, serta dapat melatih tim didalam perusahaan untuk menghadapi ancaman *siber* yang ada

Mahasiswa magang mendapatkan pengalaman pengujian keamanan aplikasi secara langsung sekaligus pemahaman mengenai pentingnya penerapan prinsip keamanan dalam pengembangan aplikasi web. Pengalaman ini menekankan bahwa keamanan menjadi elemen inti yang memastikan aplikasi yang dibuat tidak hanya berfungsi dengan baik, tetapi juga terlindung dari ancaman serta aman untuk digunakan. Oleh karena itu, selain memberikan kontribusi pada perusahaan, mengikuti program magang di PT Sekuriti Siber Indonesia juga memberikan landasan yang kuat bagi mahasiswa dalam penyusunan tugas akhir yang berfokus pada pemahaman dan implementasi konsep keamanan *siber* dalam pengembangan aplikasi web.

1.2 Deskripsi Pekerjaan

Selama magang di PT Sekuriti Siber Indonesia (Nemo Security), mahasiswa diberi tanggung jawab untuk mengembangkan website *dummy* yang akan digunakan sebagai objek untuk melakukan penetration testing. Website ini memiliki berbagai kerentanan keamanan yang umum ditemukan pada aplikasi web, yang bertujuan untuk menguji metode dan teknik yang digunakan dalam menemukan serta mengatasi celah keamanan. Tugas ini melibatkan beberapa tahap, dengan kompleksitas yang meningkat seiring dengan progres pekerjaan.

1. Pengembangan Website Perusahaan XYZ

   Mahasiswa terlibat dalam pembuatan website *dummy* yang menyerupai aplikasi web *perusahaan XYZ*. Website ini mencakup berbagai fitur dasar seperti formulir login, input data, dan pengolahan data, yang sengaja disisipi dengan kerentanan seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, dan konfigurasi keamanan yang lemah. Proses pengembangan ini memerlukan pemahaman tentang *code* aplikasi web yang aman, serta pengetahuan mengenai kerentanan yang sering muncul dalam pengembangan aplikasi web.

2. Penerapan Metode Penetration Testing

   Setelah *website dummy* selesai dibuat, mahasiswa melakukan penetration testing untuk mengidentifikasi dan mengeksploitasi kerentanan yang ada. Dalam tahap ini, mahasiswa menggunakan berbagai alat dan teknik yang diterapkan dalam dunia keamanan siber, seperti *Burp Suite*, dan *SQLMap*. Pengujian dilakukan secara manual dan otomatis untuk menemukan potensi celah keamanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Selain itu, pengujian dilakukan dengan fokus pada potensi ancaman yang paling umum dan berbahaya pada aplikasi web.

3. Analisis dan Dokumentasi Temuan Keamanan

   Setelah pengujian selesai, mahasiswa melakukan analisis terhadap hasil penetration testing, yang mencakup evaluasi tentang dampak dari kerentanan yang ditemukan. Setiap kerentanan yang terdeteksi dianalisis

untuk menentukan tingkat keparahannya serta potensi dampak terhadap keamanan aplikasi. Mahasiswa kemudian mendokumentasikan temuan tersebut, termasuk langkah-langkah eksploitasi yang dilakukan, dampaknya, serta rekomendasi mitigasi untuk setiap celah keamanan yang ditemukan. Dokumentasi ini akan menjadi acuan untuk memperbaiki kelemahan yang ada pada aplikasi web.

4. Penyusunan Laporan Akhir dan Rekomendasi

   Sebagai bagian dari tugas akhir magang, mahasiswa menyusun laporan lengkap yang berisi ringkasan dari setiap tahap yang telah dilakukan, temuan yang didapatkan, serta rekomendasi untuk perbaikan. Laporan ini mencakup hasil pengujian terhadap kerentanannya, solusi yang disarankan, dan langkah-langkah mitigasi yang dapat diterapkan untuk meningkatkan keamanan aplikasi web *perusahaan XYZ*. Laporan ini juga menjadi referensi bagi perusahaan untuk meningkatkan ketahanan terhadap potensi ancaman yang lebih besar.

Dengan kompleksitas pekerjaan yang mencakup pengembangan aplikasi web, penerapan teknik pengujian keamanan yang canggih, dan analisis temuan yang mendalam, tugas magang ini memberikan pengalaman langsung yang sangat berharga di dunia keamanan *siber*. Pekerjaan ini juga mencerminkan aplikasi nyata dari teori yang dipelajari selama masa kuliah dan menjadi fondasi untuk tugas akhir mahasiswa, yang bertujuan untuk meningkatkan kemampuan dan wawasan dalam menghadapi tantangan keamanan aplikasi web di dunia profesional.

1.3 Tujuan

Tujuan dari kegiatan magang ini adalah untuk memberikan pengalaman praktis kepada mahasiswa dalam bidang keamanan *siber*, khususnya dalam penerapan *penetration testing* pada aplikasi web. Adapun tujuan spesifik yang ingin dicapai selama kegiatan magang ini adalah sebagai berikut:

1. Meningkatkan Pemahaman tentang Keamanan Aplikasi Web

   Mahasiswa diharapkan dapat memahami berbagai jenis kerentanannya yang sering terjadi pada aplikasi web, seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, dan konfigurasi keamanan yang lemah. Dengan ini, mahasiswa dapat lebih memahami pentingnya pengujian keamanan dalam setiap tahap pengembangan aplikasi web.

2. Mengembangkan Kemampuan dalam Melakukan Penetration Testing

   Tujuan utama magang ini adalah untuk memfasilitasi mahasiswa dalam mempraktikkan metode *penetration testing* menggunakan berbagai alat keamanan yang umum digunakan di industri, seperti *Burp Suite* dan *SQLMap*. Mahasiswa akan melakukan pengujian untuk mengidentifikasi kerentanan dalam aplikasi web.

3. Menganalisis dan Menyusun Laporan Temuan Keamanan

   Mahasiswa bertujuan untuk menganalisis temuan dari *penetration testing* dan menyusun laporan yang mendokumentasikan temuan tersebut secara detail. Laporan ini meliputi tingkat keparahan kerentanannya, dampaknya terhadap aplikasi, serta rekomendasi perbaikan untuk mengatasi celah-celah yang

ditemukan. Laporan ini juga akan digunakan sebagai referensi untuk meningkatkan sistem keamanan aplikasi web.

4. Memberikan Kontribusi dalam Meningkatkan Keamanan Aplikasi Web Perusahaan XYZ

   Salah satu tujuan magang ini adalah untuk memberikan kontribusi nyata dalam meningkatkan keamanan aplikasi web *perusahaan XYZ* dengan cara mengidentifikasi dan menanggulangi kerentanannya yang ada. Hasil dari pengujian akan memberikan informasi berharga bagi perusahaan dalam upaya memperkuat ketahanan keamanan aplikasi mereka.

5. Mengembangkan Keterampilan dalam Dokumentasi dan Komunikasi Keamanan

   Selama magang, mahasiswa juga diarahkan untuk mengembangkan keterampilan dokumentasi yang baik serta kemampuan untuk mengkomunikasikan temuan-temuan keamanan secara jelas dan efektif, baik untuk tujuan internal tim maupun klien perusahaan. Keterampilan ini penting untuk menghasilkan laporan keamanan yang dapat diterima dan dipahami oleh berbagai pihak.

6. Mempersiapkan Tugas Akhir dengan Mengaplikasikan Pengetahuan Keamanan Siber

   Melalui kegiatan magang ini, mahasiswa akan memperoleh pemahaman yang lebih mendalam tentang pengujian keamanan aplikasi web yang dapat diaplikasikan dalam penyusunan tugas akhir. Pengalaman ini juga akan

memperkaya perspektif mahasiswa tentang pentingnya pengamanan aplikasi dalam siklus hidup pengembangan perangkat lunak.

1.4 Manfaat

Setelah menyelesaikan kegiatan magang ini, mahasiswa akan memperoleh berbagai manfaat yang berhubungan dengan peningkatan keterampilan, pengetahuan, serta pengalaman praktis di bidang keamanan *siber*. Adapun manfaat yang diperoleh antara lain:

1. Peningkatan Kemampuan Praktis dalam Keamanan Aplikasi Web

   Melalui magang ini, mahasiswa akan memperoleh pemahaman yang lebih mendalam tentang kerentanannya yang sering muncul pada aplikasi web serta cara-cara untuk mengidentifikasi dan mengatasi masalah tersebut. Pengetahuan ini akan sangat berguna untuk meningkatkan keterampilan dalam mengamankan aplikasi web, yang menjadi kompetensi penting di dunia kerja.

2. Pengalaman Langsung dalam Melakukan Penetration Testing

   Salah satu manfaat utama dari magang ini adalah kesempatan untuk mempraktikkan keterampilan *penetration testing* menggunakan berbagai alat yang umum digunakan dalam industri, seperti *Burp Suite* dan *SQLMap*. Pengalaman langsung dalam melakukan pengujian keamanan ini akan meningkatkan kemampuan teknis mahasiswa dalam menghadapi tantangan keamanan *siber* yang nyata di dunia profesional.

3. Kemampuan Menganalisis dan Menyusun Laporan Keamanan

   Selama magang, mahasiswa akan belajar untuk menganalisis hasil *penetration testing*, mengidentifikasi kerentanannya, dan menyusun laporan yang komprehensif. Kemampuan untuk menyusun laporan yang jelas dan efektif sangat penting dalam profesi keamanan *siber*, karena laporan tersebut menjadi acuan bagi pengembangan solusi dan perbaikan keamanan

4. Peningkatan Keterampilan Komunikasi dan Dokumentasi Keamanan

   Magang ini juga memberikan manfaat berupa peningkatan keterampilan komunikasi dan dokumentasi yang baik. Mahasiswa akan belajar untuk menyampaikan hasil temuan serta rekomendasi perbaikan dalam bentuk laporan yang mudah dipahami oleh berbagai pihak, termasuk tim teknis dan klien. Kemampuan ini akan meningkatkan nilai mahasiswa di mata perusahaan atau klien yang membutuhkan laporan keamanan yang jelas dan terstruktur.

5. Peningkatan Kemampuan untuk Bekerja dalam Tim Profesional

   Selain keterampilan teknis, mahasiswa juga mendapatkan pengalaman berkolaborasi dalam tim profesional yang bekerja di bidang keamanan *siber*. Hal ini akan meningkatkan kemampuan mahasiswa dalam bekerja sama, berbagi pengetahuan, serta menyelesaikan masalah secara kolektif, yang sangat berharga dalam dunia kerja.

6. Peluang Karir di Bidang Keamanan Siber

   Pengalaman magang ini membuka peluang bagi mahasiswa untuk memulai

karir di bidang keamanan *siber*. Melalui tugas-tugas yang dilakukan selama magang, mahasiswa dapat memperoleh pemahaman yang lebih baik tentang industri ini dan dapat memanfaatkan kesempatan untuk membangun jaringan profesional yang dapat membantu dalam pengembangan karir di bidang keamanan *siber*.

7. Penyelesaian Tugas Akhir dengan Implementasi yang Relevan

   Magang ini memberikan kesempatan untuk menerapkan pengetahuan yang didapatkan selama perkuliahan dalam bentuk tugas akhir yang relevan dengan dunia industri. Mahasiswa dapat menggunakan hasil magang sebagai bagian dari tugas akhir untuk menunjukkan kemampuan mereka dalam mengatasi masalah nyata di bidang keamanan *siber*.