BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, perkembangan teknologi informasi cukup luas dan telah menghasilkan perubahan yang signifikan di berbagai bidang, termasuk pendidikan. Banyak institusi pendidikan yang telah menggunakan aplikasi berbasis web untuk mendukung pengumpulan data dan administrasi sekolah. Salah satu contohnya adalah aplikasi Sistem Manajemen Siswa yang digunakan untuk mencatat informasi siswa, nilai, absensi, dan administrasi keuangan. Aplikasi seperti ini dimaksudkan untuk mempermudah pekerjaan staf administrasi dan meningkatkan efisiensi dalam pemrosesan informasi. Namun, terlepas dari semua kemudahan yang ditawarkan oleh aplikasi berbasis web, ada satu aspek penting yang sering menarik perhatian: keamanan aplikasi itu sendiri. Kebanyakan pengembangan aplikasi lebih difokuskan pada fungsionalitas dan tampilan tanpa mempertimbangkan sisi keamanan. Padahal, keamanan informasi sangat penting untuk menjaga data sensitif agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Ada banyak kasus kehilangan data dan peretasan yang terjadi karena adanya celah keamanan pada aplikasi yang bisa langsung terdeteksi.

Sejak tahun 2005 hingga akhir 2021, sektor pendidikan di Amerika Serikat telah mengalami sebanyak 2.691 insiden kebocoran data(data breach) yang melibatkan distrik sekolah K-12 dan universitas/perguruan tinggi, dengan total sekitar 32 juta data pribadi yang bocor—mayoritas berasal dari institusi pendidikan tinggi(K12Dive, 2021). Pada tahun 2021 saja tercatat 783 insiden, yang saat itu menjadi rekor tertinggi(Comparitech, 2021). Tren ini terus meningkat, di mana pada tahun 2023 jumlahnya melonjak hingga 954 insiden, naik drastis dari 139 insiden di tahun sebelumnya(GenzPrivacy, 2023). Laporan lain juga menyebutkan bahwa 87% lembaga pendidikan mengalami setidaknya satu serangan siber setiap tahunnya, menunjukkan

tingginya risiko keamanan digital di sektor ini(StealthLabs, 2023). Dampak finansial dari serangan ini pun tidak kecil—rata-rata biaya per insiden mencapai USD 4,77 juta, menjadikannya beban signifikan bagi institusi pendidikan yang sebagian besar memiliki sumber daya terbatas(AllCovered, 2024).

Beberapa jenis serangan yang sering ditemui pada aplikasi web antara lain *SQL Injection, Insecure Direct Object References* (IDOR), dan kerentanan pada fitur file upload. SQL Injection bisa dimanfaatkan oleh penyerang untuk membaca, memodifikasi, atau bahkan menghapus data yang ada di dalam database. Sedangkan IDOR bisa memungkinkan seseorang mengakses data milik pengguna lain tanpa izin. Sementara itu, celah pada fitur file upload bisa dimanfaatkan untuk mengunggah file berbahaya yang bisa merusak sistem. Semua celah tersebut, jika tidak diperbaiki, bisa membawa dampak besar bagi institusi yang menggunakan aplikasi tersebut.

Berdasarkan masalah tersebut, penelitian ini bertujuan untuk menilai keamanan aplikasi web Python internal dengan menggunakan studi kasus Sistem Manajemen Siswa. Metode penetration testing yang digunakan dalam penelitian ini mengikuti standar OWASP ASVS, sehingga penelitian dapat dilakukan dengan aman dan sesuai dengan standar keamanan informasi internasional. Pengujian dilakukan dengan bantuan beberapa alat, salah satunya Burp Suite, untuk mendeteksi potensi kerentanan yang ada pada aplikasi. Setelah celah keamanan ditemukan, penelitian ini juga memberikan rekomendasi langkah mitigasi yang dapat diterapkan agar aplikasi menjadi lebih aman dan handal.

1.2 Deskripsi Pekerjaan

Tujuan dari penelitian ini adalah untuk melakukan analisis keamanan pada aplikasi web Python internal dengan menggunakan studi kasus pada Sistem Manajemen Siswa. Aplikasi ini dirancang untuk mendukung data siswa dan tugas-tugas administrasi di dalam institusi pendidikan, seperti identitas siswa, nilai, dan absensi, serta tugas-tugas administrasi keuangan. Karena aplikasi ini menggunakan data-data yang sensitif, seperti informasi pribadi siswa,

maka aspek keamanan menjadi sangat penting agar data-data tersebut tidak mudah diakses atau digunakan oleh pihak-pihak yang tidak bertanggung jawab.

Pekerjaan dimulai dengan proses pengumpulan informasi untuk memahami sepenuhnya aplikasi pekerjaan. Langkah ini melibatkan *information gathering* tentang setiap aspek aplikasi, baik melalui antarmuka pengguna atau interaksi dengan database dan server. Memahami aplikasi secara mendalam sangat penting untuk memastikan bahwa pengujian keamanan dapat dilakukan sepenuhnya dan tanpa masalah yang tersisa.

Memahami aplikasi secara mendalam sangat penting untuk memastikan bahwa pengujian keamanan dapat dilakukan sepenuhnya dan tanpa masalah yang tersisa.

1. Identifikasi dan Pemetaan Sistem

   Langkah awal penelitian adalah melakukan analisis mendalam terhadap arsitektur aplikasi untuk memahami alur data, proses bisnis, serta titik-titik krusial yang rawan dieksploitasi. Penulis mengidentifikasi seluruh *endpoint*, parameter input, autentikasi, dan fitur yang memungkinkan pengguna mengunggah file. Tujuan dari langkah ini adalah untuk memprioritaskan area yang akan dievaluasi dan menentukan *attack vector*. Hal ini dilakukan untuk memastikan bahwa proses pengujian dilakukan secara sistematis.

2. Penetapan Prioritas Celah Berdasarkan Tingkat Ancaman

   Dalam menentukan fokus pengujian, penelitian ini merujuk pada standar internasional, yaitu OWASP Application Security Verification Standard (ASVS) dan OWASP Top Ten 2021, yang mencatat bahwa mayoritas aplikasi web di dunia masih memiliki kelemahan pada aspek kontrol akses, validasi input, serta proteksi terhadap serangan injeksi. Adapun tiga kerentanan utama yang diangkat dalam penelitian ini meliputi:

   A. SQL Injection (SQLi)

      Jenis serangan klasik yang hingga kini masih ditemukan

pada aplikasi web di seluruh dunia, dengan 94 % aplikasi rentan terhadap setidaknya satu bentuk serangan injeksi (OWASP, 2021). Serangan ini memungkinkan pelaku untuk membaca, memodifikasi, hingga menghapus data di database dengan cara menyisipkan perintah SQL berbahaya ke dalam input pengguna.

B. *Insecure Direct Object References (IDOR)*

Kerentanan ini tergolong dalam *Broken Access Control*, yang menempati peringkat nomor 1 OWASP Top Ten. IDOR memungkinkan pelaku untuk mengakses data milik pengguna lain hanya dengan memanipulasi parameter seperti ID atau nomor referensi.

C. *Kelemahan Fitur File Upload*

File upload tanpa validasi yang baik dapat membuka peluang untuk serangan seperti Remote Code Execution (RCE) atau penyisipan Web Shell.

3. Pelaksanaan Penetration Testing

Pengujian keamanan dilakukan dengan pendekatan *white-box*(pengetahuan sistem) dan *grey-box* (dengan akses terbatas), menggunakan beberapa *tools* profesional seperti Burp Suite dan SQLMap.

4. Penilaian Risiko (Risk Assessment)

Setiap temuan dievaluasi dengan menggunakan *Common Vulnerability Scoring System* (CVSS) v3.1 untuk menentukan tingkat keparahan. Rata-rata skor SQL Injection masuk kategori *High* (7.5–8.6). IDOR dan kelemahan *upload file* juga rata-rata masuk kategori *High* karena memungkinkan pelanggaran data massal atau eskalasi hak akses. Evaluasi risiko ini tidak hanya teknis, tetapi juga mempertimbangkan dampak bisnis dan hukum, terutama jika sistem menyimpan data pribadi, yang di Indonesia dilindungi oleh UU Perlindungan Data Pribadi No. 27 Tahun 2022.

5. Rekomendasi Mitigasi

   Berdasarkan temuan pengujian, penelitian ini menyusun strategi mitigasi yang konkret dan dapat langsung diimplementasikan oleh tim pengembang, salah satunya seperti implementasi *Prepared Statements* atau ORM untuk mencegah SQL Injection.

6. Dokumentasi Teknis

   Seluruh proses pengujian dan hasilnya dikompilasi dalam dokumentasi. Dokumentasi ini disusun agar dapat dipahami oleh baik tim pengembang, manajemen IT, maupun auditor keamanan.

1.3 Tujuan

Tujuan dari penelitian ini adalah untuk melakukan investigasi terhadap keamanan aplikasi web internal berbasis Python bernama Sistem Manajemen Siswa, yang digunakan untuk mendukung kegiatan administrasi di lingkungan pendidikan, seperti entri data siswa, nilai, absensi, dan bahan administrasi keuangan. Tujuan utama dari penelitian ini adalah:

A. Melakukan Identifikasi Kerentanan (Vulnerability Assessment).
B. Melakukan Pengujian Keamanan (Penetration Testing).
C. Menganalisis Dampak dan Tingkat Risiko.
D. Memberikan Rekomendasi Mitigasi.

1.4 Manfaat

Manfaat pertama adalah untuk membantu mereka yang mengembangkan aplikasi, terutama mereka yang terlibat dalam pengembangan Sistem Manajemen Siswa, untuk lebih memahami berbagai aspek keamanan yang mungkin terlewatkan selama proses ini.

Kedua, penelitian ini bermanfaat bagi institusi pendidikan itu sendiri. Saat ini, banyak sekolah dan guru yang mulai menggunakan teknologi digital dalam tugas-tugas administratif, tetapi mereka masih kurang mempertimbangkan keamanan informasi. Hasil penelitian ini diharapkan mampu meningkatkan kesadaran para pengelola IT sekolah tentang pentingnya menjaga kerahasiaan dan integritas data siswa, terlebih data pribadi yang dilindungi secara hukum.

BAB II
PROFIL INSTANSI TEMPAT MAGANG

2.1 Sejarah Singkat Perusahaan

PT Sekuriti Siber Indonesia adalah sebuah perusahaan konsultan keamanan siber yang berdiri sejak tahun 2017 dan berbasis di Jakarta. Perusahaan ini berfokus pada penyediaan berbagai layanan keamanan siber yang mencakup *penetration testing*, *security assessment*, *compliance security*, *security monitoring*, dan *security training*. Sejak awal berdirinya, PT Sekuriti Siber Indonesia memiliki tujuan untuk membantu berbagai organisasi dan perusahaan dalam meningkatkan ketahanan digital mereka terhadap ancaman dan serangan siber yang kian kompleks dan terus berkembang.

Dengan pengalaman dan dedikasi yang kuat, PT Sekuriti Siber Indonesia telah berkontribusi dalam mengamankan banyak aplikasi yang digunakan secara luas, sehingga membantu menurunkan risiko kerentanan dan mencegah aplikasi-aplikasi tersebut masuk ke dalam daftar aplikasi rentan atau terdampak serangan.

2.2 Visi dan Misi Perusahaan

Visi:

Menjadi perusahaan keamanan siber yang diakui secara global, meningkatkan standar keamanan siber di Indonesia, dan membina generasi baru yang terampil dan berintegritas.

Misi:

1. Memberikan solusi keamanan siber berkualitas tinggi Menyediakan solusi inovatif untuk melindungi organisasi dan individu dari ancaman siber yang terus berkembang.
2. Meningkatkan kesadaran keamanan siber: Melalui edukasi, lokakarya, dan pelatihan, perusahaan berkomitmen untuk meningkatkan pengetahuan masyarakat mengenai pentingnya keamanan siber.
3. Mengembangkan talenta keamanan siber: Memberikan kesempatan

karir dan pengembangan keahlian melalui program magang dan bimbingan profesional.

4. Membangun kemitraan strategis: Menjalin kerja sama dengan pemerintah, organisasi swasta, dan institusi pendidikan untuk memperkuat ekosistem keamanan siber nasional.
5. Menjunjung tinggi etika dan integritas: Mengedepankan transparansi, kepatuhan hukum, dan tanggung jawab sosial dalam setiap lini bisnis dan operasional.

2.3 Layanan Utama PT Sekuriti Siber Indonesia

Untuk mendukung misi dalam meningkatkan keamanan digital di berbagai sektor, PT Sekuriti Siber Indonesia menyediakan beberapa layanan utama, yaitu:

1. Penetration Testing (Pengujian Penetrasi)
   Layanan ini bertujuan untuk mengidentifikasi dan mengevaluasi celah keamanan pada sistem atau aplikasi dengan mensimulasikan serangan siber nyata. Tim melakukan pengujian dari sisi internal maupun eksternal, agar organisasi memahami potensi risiko yang ada.
2. Security Assessment (Penilaian Keamanan)
   Melakukan evaluasi komprehensif terhadap sistem, jaringan, maupun aplikasi untuk mengetahui apakah telah memenuhi standar keamanan yang berlaku, seperti OWASP, ISO 27001, maupun PCI DSS. Hasil *assessment* digunakan sebagai dasar perbaikan dan penguatan keamanan.
3. Security Operation Center (SOC)
   Menyediakan layanan pemantauan keamanan 24/7 melalui pusat operasi keamanan yang dilengkapi dengan SIEM *(Security Information and Event Management)* untuk mendeteksi, menganalisis, dan merespons ancaman siber secara real-time.
4. System Hardening
   Layanan ini berfokus pada penguatan sistem TI agar lebih tahan terhadap serangan siber, dengan cara menghapus konfigurasi yang

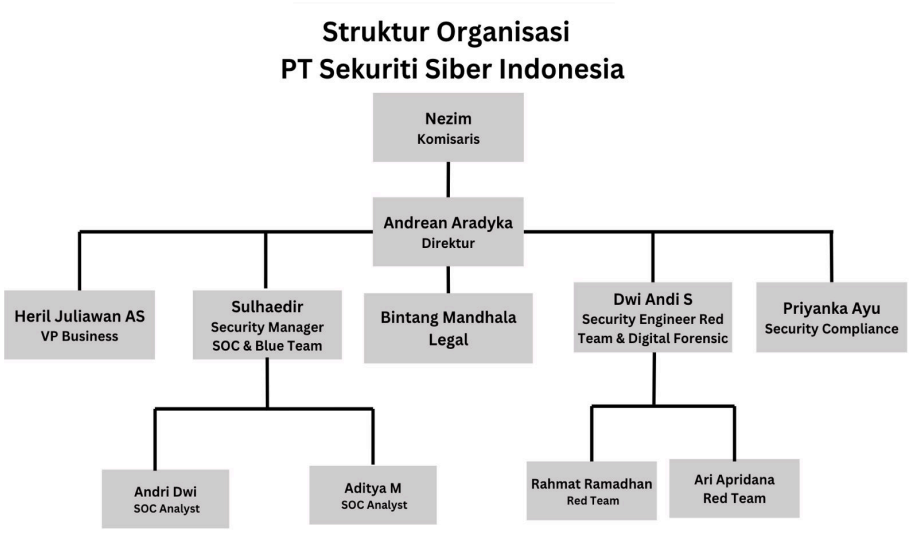
tidak aman, memperbarui *patch* keamanan, serta menerapkan kontrol akses yang ketat.

5. Digital Forensic (Forensik Digital)

   Menyediakan layanan investigasi insiden siber dengan cara mengumpulkan, menganalisis, dan melaporkan bukti digital yang valid. Layanan ini sangat penting untuk menangani kasus pelanggaran data, kebocoran informasi, maupun kejahatan siber lainnya.

2.4 Struktur Organisasi

Struktur organisasi di bawah ini dibentuk oleh Nemo Security pada tahun 2017, dan disahkan secara aklamasi menjadi PT. Sekuriti Siber Indonesia pada tahun 2018, dengan susunan organisasi sebagai berikut:



Gambar 2. 1 Struktur Organisasi

Struktur organisasi di PT Sekuriti Siber Indonesia dipimpin oleh seorang Komisaris, yang berperan sebagai pengawas dan penentu arah strategis perusahaan. Komisaris bertanggung jawab dalam memastikan bahwa seluruh kegiatan perusahaan berjalan sesuai dengan visi dan misi yang telah ditetapkan. Di bawah Komisaris, terdapat Direktur yang memiliki peran sentral dalam mengelola dan mengkoordinasikan seluruh aktivitas operasional perusahaan secara menyeluruh. Direktur ini membawahi beberapa divisi

utama yang masing-masing memiliki peran dan tanggung jawab yang spesifik, yaitu:

1. VP Business, yang berfokus pada pengembangan bisnis, pengelolaan relasi dengan klien, serta ekspansi layanan dan peluang pasar baru.
2. Security Manager SOC (Security Operation Center), yang bertanggung jawab atas pengawasan keamanan siber secara real-time, termasuk mendeteksi, menganalisis, dan merespons ancaman keamanan yang mungkin terjadi.
3. Divisi Legal, yang mengatur segala aspek hukum, mulai dari kontrak, kepatuhan terhadap peraturan, hingga penyelesaian permasalahan hukum terkait insiden keamanan informasi.
4. Security Engineer Red Team & Digital Forensic, divisi yang memiliki dua peran vital yaitu melakukan simulasi serangan siber melalui Red Team untuk menguji ketahanan sistem, serta melakukan analisis forensik digital guna mengungkap dan menangani insiden keamanan.

Setiap divisi menjalankan fungsi dan perannya masing-masing, namun tetap saling berkolaborasi dalam rangka menjaga keamanan dan keberlangsungan bisnis perusahaan. Keterpaduan antar divisi inilah yang memungkinkan PT Sekuriti Siber Indonesia untuk memberikan layanan keamanan siber yang komprehensif, profesional, dan sesuai dengan kebutuhan klien di era digital yang penuh ancaman seperti saat ini.

2.5 Budaya dan Nilai Perusahaan

PT Sekuriti Siber Indonesia menjunjung tinggi budaya kerja yang mengutamakan integritas, inovasi, dan profesionalisme. Selain itu, perusahaan ini juga aktif mendorong pengembangan talenta muda melalui program magang dan pelatihan yang bertujuan mencetak generasi profesional keamanan siber yang andal dan beretika.

Selain sebagai penyedia layanan, perusahaan ini juga memiliki misi sosial melalui kegiatan edukasi publik mengenai keamanan digital agar masyarakat Indonesia lebih peka dan sadar terhadap potensi ancaman di dunia maya.