BAB I
PENDAHULUAN

1.1 Latar Belakang

Broken Access Control (BAC) merupakan salah satu kerentanan keamanan kritikal yang terjadi ketika sistem gagal menerapkan mekanisme pembatasan akses secara benar dan konsisten (OWASP Top 10 Team, 2021). Dalam kondisi ini, pengguna yang tidak terautentikasi atau tidak memiliki wewenang dapat mengakses data, fungsi, atau sumber daya yang seharusnya berada di luar cakupan izin mereka. Kerentanan ini umumnya disebabkan oleh kesalahan desain sistem dalam pengelolaan hierarki hak akses atau mekanisme kontrol yang tidak diterapkan secara ketat pada lapisan aplikasi maupun API (PortSwigger, 2026). Sebagai contoh, pada aplikasi berbasis web, BAC dapat dieksploitasi ketika pengguna tanpa hak khusus memodifikasi URL, parameter, atau metode permintaan (*request method*) untuk menjangkau informasi sensitif atau fungsi administratif. Jika tidak segera dimitigasi, BAC membuka celah bagi akses ilegal ke area sensitif sistem, yang memungkinkan penyerang untuk memanipulasi atau mencuri data strategis.

Risiko yang ditimbulkan oleh BAC sangat signifikan terhadap postur keamanan dan integritas sistem. Eksploitasi terhadap celah ini dapat berujung pada kebocoran informasi rahasia (*data breach*), seperti data pribadi pengguna (*personally identifiable information*) atau data korporasi, serta memungkinkan modifikasi data secara tidak sah (Bakharev, 2024). Dalam skenario yang lebih fatal, BAC dapat memicu eskalasi hak akses (*privilege escalation*), dimana penyerang dengan akses terbatas dapat mengambil alih kendali penuh atas sistem. Tantangan utama dalam penanganan BAC adalah karakteristiknya yang sulit dideteksi. Mengingat serangan ini sering kali tidak menghasilkan pesan *error* yang eksplisit atau anomali lalu lintas jaringan yang mencolok, aktivitas penyerang kerap kali luput dari pemantauan sistem keamanan konvensional yang cenderung berfokus pada deteksi pola serangan berbasis *signature*. Dalam melakukan verifikasi manual terhadap mekanisme otorisasi ini, penguji sering kali berinteraksi dengan format representasi data tertentu, sehingga pemahaman terhadap efektivitas metode encoding dan decoding seperti algoritma *Base64* menjadi aspek teknis yang penting

dalam menganalisis manipulasi parameter antara klien dan peladen (Kurniawan dkk., 2023)

Identifikasi kerentanan BAC umumnya memerlukan pendekatan pengujian penetrasi (*penetration testing*) atau audit keamanan yang mendalam. Dalam pelaksanaannya, penguji berupaya memanipulasi vektor akses aplikasi melalui berbagai teknik, seperti modifikasi *input*, manipulasi parameter URL, atau perubahan token sesi untuk menguji ketahanan mekanisme proteksi sumber daya. Pada beberapa kasus, penguji harus melakukan analisis logika bisnis untuk memetakan alur otorisasi dan menemukan titik lemah dalam kontrol akses. Meskipun alat pemindai otomatis dapat membantu proses deteksi awal, sebagian besar kerentanan BAC yang kompleks hanya dapat ditemukan melalui verifikasi manual. Hal ini dikarenakan eksploitasi BAC sangat bergantung pada pemahaman kontekstual terhadap perilaku aplikasi dan skema hak akses pengguna yang unik pada setiap sistem (Anas dkk. 2024).

Kesulitan utama dalam mendeteksi BAC terletak pada sifatnya yang tersembunyi di dalam logika bisnis dan konfigurasi sistem. Berbeda dengan kerentanan teknis seperti *SQL Injection (SQLI)* atau *Cross-Site Scripting (XSS)* yang memiliki pola serangan *syntactical* yang jelas. BAC sering kali membutuhkan pengujian manual yang teliti karena melibatkan kompleksitas implementasi kontrol akses di berbagai lapisan arsitektur. Pengujian otomatis sering kali kurang efektif dalam mendeteksi kerentanan logis ini karena alat tersebut tidak memahami konteks "*siapa yang boleh mengakses apa*" dalam skenario nyata. Kompleksitas distribusi aturan akses dan dokumentasi sistem yang sering kali tidak lengkap semakin menambah tantangan dalam proses deteksi. Oleh karena itu, pendekatan pengujian manual yang komprehensif menjadi instrumen kunci dalam mengidentifikasi dan memvalidasi kerentanan ini secara akurat.

Tantangan keamanan siber juga dihadapi oleh institusi pendidikan tinggi, termasuk Universitas Pendidikan Ganesha (Undiksha). Berdasarkan hasil wawancara pendahuluan, sistem informasi di lingkungan Undiksha terindikasi pernah menjadi target berbagai ancaman keamanan, termasuk serangan XSS dan *Distributed Denial of Service (DDoS)*. Pentingnya mitigasi terhadap serangan XSS dan penguatan mekanisme pembatasan akses seperti *rate limiting* menjadi krusial

untuk mencegah eksploitasi yang merugikan integritas *website* institusi (Dewangkara dkk. 2022). Insiden ini mengindikasikan bahwa tata kelola keamanan sistem di Undiksha masih memerlukan atensi khusus dan evaluasi berkelanjutan. Hal ini krusial mengingat pelanggaran keamanan tidak hanya berdampak pada kegagalan teknis, tetapi juga berisiko tinggi terhadap pencurian data strategis, kerugian finansial, hingga rusaknya reputasi institusi di mata publik (Mahendra dkk., 2022). Oleh karena itu, penerapan metode pengujian yang terstruktur menjadi kebutuhan mendesak untuk memetakan titik lemah pada sistem keamanan *website* universitas. Urgensi audit keamanan mendalam ini sejalan dengan temuan Listartha & Saskara (2024), yang mengungkapkan bahwa meskipun perangkat jaringan secara fungsional berjalan normal, konfigurasi keamanan yang lemah sering kali tidak terdeteksi tanpa adanya pengujian penetrasi aktif.

Selain kerentanan pada aspek teknis infrastruktur, faktor manusia juga menjadi variabel risiko yang signifikan. Listartha dkk. (2025) dalam studi pengabdiannya menyoroti bahwa kelompok pelajar dan mahasiswa, yang merupakan pengguna mayoritas sistem akademik, sering kali masih memiliki tingkat kesadaran keamanan digital yang rendah, sehingga rentan menjadi korban serangan siber. Dalam konteks ini, pengamanan sistem melalui *penetration testing* tidak hanya berfungsi sebagai langkah perbaikan teknis, tetapi juga sebagai upaya preventif krusial untuk melindungi ekosistem pengguna yang mungkin belum memiliki literasi digital yang memadai.

Untuk menjawab kebutuhan evaluasi keamanan tersebut, penelitian ini mengadopsi kerangka kerja *Penetration Testing Execution Standard (PTES)*. PTES menawarkan panduan metodologis yang terstruktur dan sistematis untuk melaksanakan uji penetrasi secara komprehensif. Standar ini dirancang untuk memandu penguji melalui tahapan proses yang terstandarisasi, mulai dari perencanaan hingga pelaporan, guna mengidentifikasi dan mengeksploitasi kerentanan pada berbagai platform, termasuk aplikasi web. Keunggulan PTES terletak pada pendekatan metodisnya yang tidak hanya memberikan instruksi teknis, tetapi juga kerangka berpikir analitis untuk memastikan setiap aspek keamanan diuji secara menyeluruh (GeeksforGeeks, 2022b). Penggunaan kerangka kerja yang terstandarisasi seperti PTES menjadi sangat penting karena pengujian keamanan

yang dilakukan langsung pada sistem produksi tanpa prosedur yang tepat dapat bersinggungan dengan aspek hukum (Saskara dkk., 2024). Dengan mengikuti fase interaksi awal dalam PTES, batasan hukum dan ruang lingkup pengujian dapat didefinisikan secara jelas untuk menghindari dampak negatif terhadap sistem maupun organisasi. Kerangka kerja ini mencakup tujuh fase utama, dimulai dari interaksi awal dan pengumpulan informasi untuk memahami arsitektur target, hingga analisis kerentanan dan eksploitasi. Fokus PTES pada tahapan eksploitasi sangat relevan untuk penelitian ini karena memungkinkan simulasi serangan nyata yang diperlukan untuk mengungkap kelemahan logika bisnis seperti BAC.

Efektivitas PTES juga didukung oleh penelitian komparatif sebelumnya. Prasetyo dkk. (2024) menunjukkan bahwa PTES memiliki keunggulan dibandingkan kerangka kerja lain seperti *Information Systems Security Assessment Framework (ISSAF)* dalam hal fleksibilitas dan efektivitas eksploitasi. Dalam studi kasus pada jaringan perhotelan, PTES terbukti mampu mengidentifikasi spektrum kerentanan yang luas, mulai dari *port* terbuka hingga kelemahan autentikasi. Karakteristik fleksibilitas ini menjadikan PTES sebagai metode yang sangat relevan untuk diaplikasikan dalam deteksi BAC yang membutuhkan eksplorasi manual mendalam.

Penerapan PTES dalam konteks akademis juga telah banyak didokumentasikan. Dasmen dkk. (2023) berhasil menerapkan metode PTES dikombinasikan dengan pengujian *Black Box* untuk mengaudit keamanan *website e-learning* Universitas Bina Darma, dimana penelitian tersebut berhasil mengidentifikasi dan merekomendasikan perbaikan untuk kerentanan XSS. Senada dengan itu, Fikri, Zen, Adhitama, & Firdaus (2023) menggunakan PTES untuk menganalisis keamanan *website* sekolah dan berhasil mengungkap kerentanan kritis *SQL Injection* yang membahayakan basis data siswa. Lebih lanjut, Sunaringtyas & Prayoga (2021) membuktikan bahwa PTES efektif diterapkan pada sistem otentikasi terpusat (*Single Sign-On*), menghasilkan rekomendasi perbaikan konfigurasi keamanan yang spesifik. Rangkaian penelitian terdahulu ini memberikan landasan empiris bahwa PTES merupakan metode yang andal untuk audit keamanan sistem informasi.

Berdasarkan paparan di atas, penelitian ini difokuskan untuk mengevaluasi efektivitas penerapan metode PTES secara spesifik dalam mendeteksi kerentanan

BAC. Dengan mengikuti alur kerja sistematis PTES, penelitian ini bertujuan untuk membuktikan bahwa pendekatan manual yang terstruktur mampu mengidentifikasi kelemahan logika akses yang sering kali lolos dari deteksi alat otomatis. Hasil penelitian ini diharapkan dapat memberikan kontribusi nyata bagi penguatan sistem keamanan Undiksha. Selain itu, melalui identifikasi kerentanan yang sistematis, pengelola sistem dapat mengestimasi tingkat probabilitas dan dampak serangan guna menentukan prioritas perbaikan keamanan berdasarkan kategori risiko yang ditemukan (Listartha dkk. 2022). Hal ini juga diharapkan dapat memperkaya literatur mengenai penerapan PTES dalam konteks kerentanan logika bisnis.

1.2 Rumusan Masalah

BAC merupakan kerentanan yang sulit dideteksi karena karakteristiknya yang tersembunyi di dalam logika bisnis dan konfigurasi kontrol akses sistem. Meskipun metode pengujian penetrasi seperti PTES telah digunakan secara luas, penelitian-penelitian terdahulu umumnya lebih menitikberatkan pada deteksi kerentanan teknis seperti SQLI dan XSS. Oleh karena itu, penelitian ini bertujuan untuk mengeksplorasi efektivitas implementasi PTES secara spesifik dalam mendeteksi kerentanan BAC, mengingat dampak kritikal yang dapat ditimbulkannya, yaitu eskalasi hak akses dan kebocoran data.

Berdasarkan latar belakang tersebut, adapun rumusan masalah yang akan dikaji dalam penelitian ini adalah sebagai berikut:

1. Bagaimana implementasi metode *Penetration Testing Execution Standard (PTES)* dalam menemukan kerentanan *Broken Access Control (BAC)* pada *website* Universitas Pendidikan Ganesha?
2. Bagaimana tingkat risiko dari kerentanan *Broken Access Control (BAC)* terhadap *website* Universitas Pendidikan Ganesha?
3. Apa rekomendasi yang dapat diberikan untuk meningkatkan keamanan *website* Universitas Pendidikan Ganesha dari *Broken Access Control (BAC)* berdasarkan hasil *penetration testing*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, adapun tujuan penelitian ini adalah sebagai berikut:

1. Mengimplementasikan metode PTES dalam menemukan kerentanan BAC.
2. Menganalisis tingkat risiko dari kerentanan BAC.
3. Menyusun rekomendasi untuk meningkatkan keamanan *website* berdasarkan hasil *penetration testing*.

1.4 Ruang Lingkup Penelitian

Penelitian ini membatasi ruang lingkup analisis pada identifikasi dan eksploitasi kerentanan BAC pada ekosistem *website* Universitas Pendidikan Ganesha dengan mengacu pada standar PTES. Adapun batasan dan ruang lingkup penelitian ini dijabarkan sebagai berikut:

1. Objek Penelitian

   Objek penelitian difokuskan pada *subdomain website* di lingkungan Universitas Pendidikan Ganesha yang telah diklasifikasikan berdasarkan kriteria teknis tertentu dan memiliki fitur interaksi pengguna yang relevan untuk pengujian hak akses.
2. Metode Penelitian

   Metodologi pengujian mengadopsi kerangka kerja PTES secara utuh, yang mencakup 7 tahapan standar, yaitu *Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-exploitation,* dan *Reporting*. Fokus utama pengujian adalah pada deteksi celah logika bisnis dan kontrol akses.
3. Batasan Waktu
   a) Penelitian dilaksanakan dalam durasi enam bulan, meliputi fase persiapan administratif, pelaksanaan pengujian teknis, analisis data, hingga penyusunan laporan akhir.
   b) Periode aktif pengujian penetrasi (*active scanning* dan *exploitation*) dilakukan sesuai dengan jadwal operasional yang telah disepakati bersama Unit Penunjang Akademik Teknologi Informasi dan Komunikasi (UPA TIK) Undiksha untuk meminimalisasi gangguan pada layanan.

4. Batasan Etika dan Legal
   a) Seluruh aktivitas pengujian dilakukan berdasarkan izin tertulis resmi dari pihak berwenang di Universitas Pendidikan Ganesha dan mematuhi prinsip *White Hat Hacking*.
   b) Tindakan eksploitasi dilakukan semata-mata sebagai *proof of concept* untuk memvalidasi kerentanan. Penelitian ini menjamin tidak adanya perusakan, perubahan permanen, atau publikasi data sensitif milik pengguna tanpa penyamaran (*masking*) atau persetujuan pihak terkait.
5. Hasil Penelitian
   a) Luaran penelitian berupa dokumen laporan teknis yang memetakan tingkat risiko kerentanan berdasarkan standar OWASP *Risk Rating*.
   b) Laporan tersebut disertai dengan rekomendasi mitigasi dan perbaikan sistem (*patching*) yang diserahkan kepada pengelola sistem Undiksha sebagai bahan evaluasi keamanan.

Melalui penetapan ruang lingkup ini, penelitian diharapkan dapat berjalan secara terarah, legal, dan menghasilkan rekomendasi yang implementatif bagi penguatan postur keamanan siber Universitas Pendidikan Ganesha.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi yang signifikan, baik dalam ranah akademis maupun praktis, dengan rincian manfaat sebagai berikut:

1. Manfaat Teoritis
   a) Memperkaya literatur dan khazanah keilmuan mengenai efektivitas penerapan standar *Penetration Testing Execution Standard (PTES)*, khususnya dalam mendeteksi kerentanan logika bisnis seperti *Broken Access Control (BAC)*.
   b) Memberikan bukti empiris mengenai pola kerentanan keamanan pada sistem informasi di lingkungan institusi pendidikan tinggi, yang memiliki karakteristik pengguna unik dibandingkan sektor industri lainnya.
   c) Menjadi referensi komparatif bagi peneliti selanjutnya yang hendak mengkaji topik keamanan siber, *penetration testing*, maupun audit sistem informasi berbasis *website*.

2. Manfaat Praktis
   A. Bagi Universitas Pendidikan Ganesha
      a) Menyediakan informasi mendalam mengenai postur keamanan *website* universitas saat ini, termasuk pemetaan titik-titik kerentanan kritis yang memerlukan penanganan segera.
      b) Memberikan landasan teknis bagi pemangku kebijakan universitas dalam merumuskan strategi penguatan sistem pertahanan siber guna meminimalisasi risiko kebocoran data dan gangguan layanan.
   B. Bagi Pengelola Sistem dan Teknologi Informasi
      a) Menghasilkan rekomendasi mitigasi teknis dan perbaikan konfigurasi yang spesifik dan dapat langsung diterapkan untuk menutup celah keamanan yang ditemukan.
      b) Mendorong adopsi prosedur *penetration testing* rutin sebagai bagian dari Standar Operasional Prosedur (SOP) pemeliharaan sistem untuk menjamin keberlanjutan keamanan (*security sustainability*).
   C. Bagi Sivitas Akademika dan Mahasiswa
      a) Meningkatkan kesadaran keamanan siber (*security awareness*) di kalangan mahasiswa dan dosen mengenai risiko penggunaan sistem informasi, serta mendorong perilaku digital yang lebih aman.
      b) Menyediakan studi kasus riil yang dapat dijadikan materi pembelajaran atau diskusi dalam mata kuliah terkait keamanan jaringan dan sistem informasi.
3. Manfaat Sosial
   a) Menjaga dan meningkatkan kepercayaan publik, termasuk orang tua mahasiswa dan mitra kerjasama, terhadap integritas dan keamanan data yang dikelola oleh Universitas Pendidikan Ganesha.
   b) Berkontribusi dalam menciptakan ekosistem digital pendidikan nasional yang aman, sehingga dapat menekan dampak negatif kejahatan siber terhadap keberlangsungan proses pendidikan.

Melalui penjabaran manfaat tersebut, penelitian ini diharapkan tidak hanya menjadi dokumen akademis semata, melainkan juga menjadi instrumen perbaikan nyata bagi keamanan sistem informasi di lingkungan pendidikan.