Laporan Pengujian atau Hasil Pencarian Celah Keamanan oleh Peserta Bug Bounty 2024

No.	Poin (Indikator)	Hasil
1.	Nama Target	SIBI
2.	Nama Kerentanan	Broken Access Control
3.	Jenis Kerentanan	A01 Broken Access Control
4.	Deskripsi Kerentanan	Kerentanan broken access control adalah celah keamanan di mana pengguna dapat mengakses data atau fungsi yang seharusnya tidak mereka akses. Dalam skenario yang Anda sebutkan, dengan hanya mengubah nama pengguna menjadi sama dengan target yang diinginkan, seseorang dapat dengan mudah mengakses semua data sensitif yang seharusnya tidak mereka akses. Ini terjadi karena sistem gagal memvalidasi atau mengotorisasi dengan benar setiap permintaan akses. Ketika sistem tidak memeriksa dengan cermat identitas pengguna yang meminta akses, orang lain dapat memanipulasi input mereka untuk mendapatkan hak akses yang tidak seharusnya mereka miliki.
5.	Lokasi/URL	https://buku-sibi.netlify.app/
6.	*IP Address Source* (IP Address Peserta)	125.166.118.135
7.	Dampak	dengan hanya mengganti nama pengguna menjadi sama dengan target yang diinginkan, orang tersebut dapat melewati kontrol akses

		dan mendapatkan akses ke semua data sensitif yang dimiliki oleh target tersebut. Ini adalah contoh konkret dari bagaimana kerentanan broken access control dapat dimanfaatkan untuk mengakses informasi yang seharusnya aman.
8.	Langkah Penetrasi dan Tangkapan Layar (*Screenshots*)Temuan	1. Lakukan enumerasi username atau kita cari username orang lain dari website tersebut 2. Lakukan ubah username dengan melakukan request post pada updateUser sesuai nama target yang akan kita exploitasi 3. Kita berhasil mendapatkan semua informasi target. Bukti penetrasi akan saya lampirkan dengan video di bawah ini. https://jmp.sh/uwVrSUZ4
9.	Rekomendasi	Untuk mengatasi kerentanan broken access control, berikut beberapa rekomendasi yang dapat Anda pertimbangkan: 1. **Implementasi Prinsip Kepemilikan Paling Sedikit (Least Privilege)**: Berikan pengguna akses hanya pada data dan fungsi yang diperlukan untuk menyelesaikan tugas mereka. Ini meminimalkan risiko penyalahgunaan akses jika akun pengguna disalahgunakan. 2. **Pemeriksaan Akses yang Ketat**: Lakukan pemeriksaan yang ketat

		terhadap permintaan akses, termasuk verifikasi identitas pengguna dan otorisasi yang tepat sebelum memberikan akses ke data atau fungsi tertentu.
10.	Referensi	OWASP TOP TEN 2021