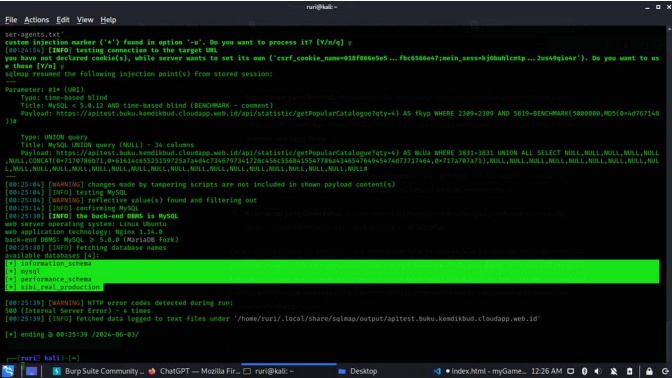


Laporan Pengujian atau Hasil Pencarian Celah Keamanan oleh Peserta Bug Bounty 2024

No.	Poin (Indikator)	Hasil
1.	Nama Target	SIBI
2.	Nama Kerentanan	SQL Injection
3.	Jenis Kerentanan	A03 Injection
4.	Deskripsi Kerentanan	Saya ingin memberitahu bahwa saya telah menemukan kerentanan SQL injection yang mengkhawatirkan pada bagian API dari aplikasi web SIBI kita. Setelah melakukan serangkaian pengujian, saya berhasil mengeksploitasi kerentanan ini dan mendapatkan akses tidak sah ke dalam database yang digunakan oleh API.
5.	Lokasi/URL	https:// apitest.buku.kemdikbud.cloudapp.web.id/api/ statistic/getPopularCatalogue?qty=4
6.	<i>IP Address Source</i> (IP Address Peserta)	125.166.118.135
7.	Dampak	Kerentanan ini memperlihatkan risiko yang serius bagi keamanan sistem kita. Dengan eksploitasi kerentanan ini, seorang penyerang berpotensi untuk mengakses, mengubah, atau bahkan menghapus data sensitif yang disimpan dalam database kami. Tindakan pencegahan dan perbaikan segera harus diambil untuk memperkuat pertahanan sistem

		kami terhadap ancaman seperti ini.
8.	Langkah Penetrasi dan Tangkapan Layar (Screenshots) Temuan	<p>1. Penelitian Awal:</p> <ul style="list-style-type: none"> • Saya mulai dengan melakukan penelitian pada parameter 'qty' dalam API aplikasi web SIBI. • Setelah menguji parameter ini, saya mencoba memasukkan karakter tanda kutip tunggal (') untuk melihat apakah terjadi anomali atau error. <p>2. Pemantauan Anomali:</p> <ul style="list-style-type: none"> • Ketika saya memberikan tanda kutip tunggal pada parameter 'qty', saya melihat adanya error yang tidak semestinya. Ini menunjukkan kemungkinan adanya kerentanan SQL injection. <p>3. Eksploitasi Manual:</p> <ul style="list-style-type: none"> • Berdasarkan hasil penelitian awal, saya mengambil langkah selanjutnya dengan mencoba mengeksploitasi kerentanan ini secara manual menggunakan SQLMap, alat otomatis untuk mendeteksi dan mengeksploitasi kerentanan SQL injection. • Dengan menggunakan SQLMap, saya berhasil menjalankan serangan SQL injection yang memanfaatkan kerentanan pada parameter 'qty'. <p>4. Sukses Eksploitasi:</p> <ul style="list-style-type: none"> • Melalui serangan yang berhasil, saya dapat memperoleh akses ke dalam database aplikasi web SIBI Anda. <p>Ini memberikan saya kemampuan untuk mengekstraksi, memanipulasi, atau bahkan menghapus data yang disimpan dalam database, yang merupakan ancaman serius</p>

		<p>terhadap keamanan aplikasi Anda.</p> 
9.	Rekomendasi	<p>Pencegahan dan Perbaikan:</p> <ul style="list-style-type: none"> • Penggunaan Input Filtering: Kami akan segera menerapkan mekanisme pemfilteran input yang kuat untuk memastikan bahwa data yang diterima dari pengguna tidak mengandung karakter-karakter yang berpotensi membahayakan seperti tanda kutip tunggal ('). Hal ini dapat dilakukan dengan menggunakan fungsi-fungsi pemfilteran dan validasi input yang disediakan oleh kerangka kerja aplikasi atau dengan menulis kode kustom sesuai kebutuhan. • Penggunaan Parameterized Queries: Kami akan mengonversi kueri-kueri SQL yang saat ini digunakan dalam aplikasi menjadi kueri-kueri parameterized. Dengan menggunakan parameterized queries, kita dapat memastikan bahwa input dari pengguna tidak dianggap sebagai bagian dari pernyataan SQL, sehingga mengurangi risiko serangan SQL injection. • Penggunaan Alat Pemindaian Keamanan: Kami akan secara teratur menggunakan alat-alat pemindaian keamanan seperti SQLMap untuk mengidentifikasi kerentanan potensial dalam aplikasi kami. Dengan melakukan pemindaian keamanan secara teratur, kita dapat mendeteksi dan

		<p>memperbaiki kerentanan sebelum mereka dapat dimanfaatkan oleh penyerang.</p> <ul style="list-style-type: none"> • Peningkatan Kesadaran Keamanan: Kami akan memberikan pelatihan dan sumber daya yang diperlukan kepada tim pengembang dan administrasi sistem untuk meningkatkan kesadaran tentang praktik keamanan yang baik, termasuk ancaman SQL injection dan cara menghindarinya. Hal ini akan membantu mencegah terjadinya kerentanan di masa mendatang dan memastikan bahwa tim kami siap untuk menangani ancaman keamanan dengan cepat dan efektif.
10.	Referensi	OWASP TOP TEN