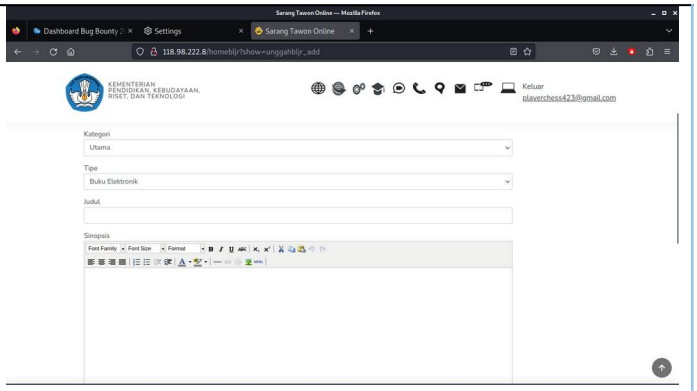
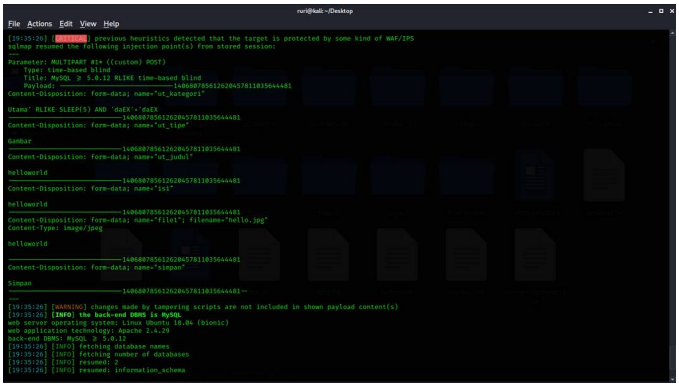
Laporan Pengujian atau Hasil Pencarian Celah Keamanan oleh Peserta Bug Bounty 2024

No.	Poin (Indikator)	Hasil
1.	Nama Target	BIPA Daring
2.	Nama Kerentanan	SQL Injection
3.	Jenis Kerentanan	A03 Injection
4.	Deskripsi Kerentanan	Kerentanan SQL injection adalah kelemahan dalam aplikasi web yang memungkinkan penyerang untuk menyisipkan kode SQL berbahaya ke dalam pernyataan SQL yang dieksekusi oleh aplikasi. Ini dapat terjadi ketika aplikasi tidak memvalidasi input pengguna dengan benar sebelum mengirimkannya ke server basis data. Dengan memanfaatkan kerentanan ini, penyerang dapat melakukan berbagai tindakan berbahaya, termasuk penghapusan atau modifikasi data, mengungkapkan informasi sensitif, atau bahkan mengambil alih kontrol server basis data.
5.	Lokasi/URL	http://118.98.222.8/homebljr?show=unggahbljr_add
6.	*IP Address Source* (IP Address Peserta)	125.166.118.135
7.	Dampak	Kerentanan SQL injection membuka pintu bagi serangkaian dampak yang serius dan merugikan, termasuk: • **Kehilangan Data**: Penyerang dapat

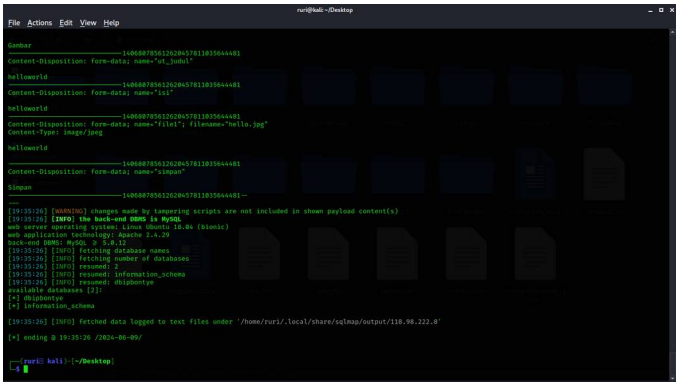
		mengakses, memodifikasi, atau menghapus data dari basis data yang terkena dampak. Ini dapat mengakibatkan kehilangan informasi krusial seperti detail pengguna, informasi keuangan, atau catatan transaksi. • **Pelanggaran Keamanan**: Akses tak sah ke data sensitif atau modifikasi struktur basis data dapat menyebabkan pelanggaran keamanan yang serius. Konsekuensinya bisa meliputi dampak hukum, denda, dan kerugian reputasi yang signifikan. • **Kehilangan Integritas Data**: Modifikasi tidak sah pada data dapat menyebabkan kehilangan integritas data. Ini dapat mengganggu operasional bisnis atau menyebabkan analisis yang tidak akurat. • **Pengungkapan Informasi Sensitif**: Penyerang dapat memperoleh akses ke informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya. Hal ini dapat mengarah pada pencurian identitas, penipuan, atau penyalahgunaan lainnya. • **Kerugian Keuangan**: Dampak kerentanan SQL injection bisa sangat mahal, termasuk biaya untuk memperbaiki kerentanan, memulihkan data yang hilang atau rusak, serta denda dan kerugian reputasi yang signifikan. Penting untuk segera menanggapi kerentanan SQL injection dan mengambil langkah-langkah proaktif untuk melindungi data dan sistem dari serangan serupa di masa depan.
8.	Langkah Penetrasi dan Tangkapan Layar (*Screenshots*)Temuan	1. saya mencoba untuk mengunggah data pada lokasi url http://118.98.222.8/homebljr?show=unggahbljr_add.



2. setelah itu saya coba untuk menginjeksi payload sqli dengan burp suite pada input kategori dengan teknik time based blind.



3. Injeksi berhasil dilakukan kemudian saya menggunakan sqlmap untuk melanjutkan melakukan exploitasi.



9.	Rekomendasi	1. **Pemindaian Keamanan Berkala**: Lakukan pemindaian keamanan secara berkala menggunakan alat pemindaian keamanan seperti SQLMap atau Burp Suite untuk mendeteksi kerentanan SQL injection dan kerentanan keamanan lainnya. 2. **Validasi Input**: Pastikan semua input yang diterima dari pengguna divalidasi dengan benar sebelum digunakan dalam pernyataan SQL. Gunakan metode pengamanan seperti parameterized queries atau ORM (Object-Relational Mapping) yang aman untuk mencegah serangan SQL injection. 3. **Penerapan Prinsip Kebutuhan Terkecil**: Berikan hak akses terendah yang diperlukan untuk pengguna dan aplikasi. Ini akan membatasi potensi kerusakan jika terjadi pelanggaran keamanan. 4. **Pemantauan Aktivitas**: Terapkan sistem pemantauan yang efektif untuk memantau aktivitas abnormal atau upaya serangan terhadap sistem Anda. Ini akan membantu Anda mendeteksi dan menanggapi serangan SQL injection dengan cepat. 5. **Pembaruan Perangkat Lunak**: Pastikan semua perangkat lunak, termasuk sistem basis data, aplikasi web, dan perangkat lunak pendukung lainnya, diperbarui secara teratur dengan patch keamanan terbaru untuk mengurangi risiko eksploitasi kerentanan yang diketahui. 6. **Pendidikan dan Pelatihan**: Berikan pelatihan kepada pengembang dan administrator sistem tentang praktik pengembangan yang aman, termasuk cara menghindari kerentanan SQL injection dan tindakan pencegahan keamanan lainnya. 7. **Audit Keamanan**: Lakukan audit keamanan secara teratur untuk mengidentifikasi dan memperbaiki kerentanan keamanan yang ada. Gunakan hasil audit untuk meningkatkan keamanan sistem Anda

		secara keseluruhan. 8. **Implementasi Firewall Aplikasi Web (WAF)**: Pertimbangkan untuk menggunakan firewall aplikasi web (WAF) untuk menangkap dan memblokir serangan SQL injection serta serangan web lainnya sebelum mencapai aplikasi Anda. Dengan menerapkan langkah-langkah ini, Anda dapat mengurangi risiko kerentanan SQL injection dan meningkatkan keamanan sistem Anda secara keseluruhan.
10.	Referensi	OWASP TOP TEN 2021