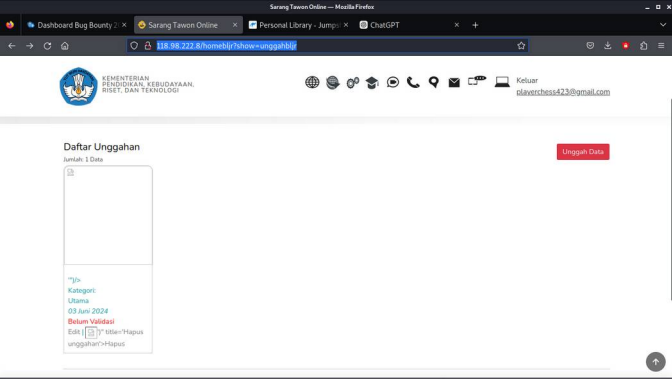


Laporan Pengujian atau Hasil Pencarian Celah Keamanan oleh Peserta Bug Bounty 2024

No.	Poin (Indikator)	Hasil
1.	Nama Target	BIPA Daring
2.	Nama Kerentanan	Stored XSS Pada Unggah Data / Postingan
3.	Jenis Kerentanan	A03 Injection
4.	Deskripsi Kerentanan	Kerentanan ini terletak pada kemungkinan disisipkannya skrip berbahaya ke dalam postingan pengguna. Skrip yang disisipkan ini dieksekusi setiap kali konten tersebut ditampilkan kepada pengguna lain. Hal ini dapat dimanfaatkan oleh penyerang untuk melakukan serangan phishing, mencuri sesi pengguna, atau menyebarkan malware.
5.	Lokasi/URL	http://118.98.222.8/homebljr?show=unggahbljr
6.	<i>IP Address Source</i> (IP Address Peserta)	125.166.118.135
7.	Dampak	Stored Cross-Site Scripting (XSS) adalah kerentanan keamanan yang memungkinkan penyerang menyisipkan skrip berbahaya ke dalam aplikasi web atau basis data yang akan dieksekusi setiap kali konten itu ditampilkan kepada pengguna lain. Dampak dari kerentanan ini dapat sangat serius dan berpotensi merugikan baik bagi pengguna individu maupun organisasi secara keseluruhan. Berikut adalah beberapa dampak

		<p>utama yang dapat terjadi akibat kerentanan Stored XSS:</p> <ol style="list-style-type: none"> 1. Eksplorasi Identitas Pengguna: Penyerang dapat menggunakan kerentanan ini untuk mencuri identitas pengguna yang terautentikasi. Dengan menyisipkan skrip berbahaya ke dalam halaman profil pengguna atau formulir lainnya, penyerang dapat mengalihkan informasi otentikasi, seperti token sesi atau kredensial login, ke server yang dikendalikan oleh mereka. 2. Serangan Phishing: Penyerang dapat memanfaatkan kerentanan ini untuk melakukan serangan phishing dengan menyajikan halaman palsu yang tampaknya sah kepada pengguna. Hal ini dapat mengelabui pengguna untuk memasukkan informasi sensitif, seperti kata sandi atau informasi kartu kredit, ke dalam formulir palsu yang sebenarnya dikendalikan oleh penyerang. 3. Penyebaran Malware: Melalui kerentanan ini, penyerang dapat menyisipkan skrip yang memicu pengunduhan dan instalasi malware secara otomatis pada perangkat pengguna ketika mereka mengakses halaman yang terinfeksi. Ini dapat mengakibatkan kerusakan pada sistem pengguna, pencurian data, atau pengambilalihan kontrol atas perangkat mereka. 4. Manipulasi Konten: Penyerang dapat menggunakan kerentanan ini untuk menyisipkan atau memodifikasi konten pada halaman web yang ditampilkan kepada pengguna lain. Hal ini dapat mengakibatkan pencemaran reputasi atau merusak pengalaman pengguna dengan menampilkan konten yang tidak diinginkan atau berbahaya. 5. Kerugian Reputasi dan Keuangan: Jika kerentanan ini dieksploitasi oleh penyerang dan mengakibatkan kerugian data pengguna, pencurian informasi rahasia,
--	--	---

		atau gangguan layanan, hal ini dapat berdampak serius terhadap reputasi dan keuangan organisasi yang terkena dampak.
8.	Langkah Penetrasi dan Tangkapan Layar (Screenshots) Temuan	<p>saya akan menjabarkan langkah-langkah yang Anda lakukan serta hasil eksploitasi tersebut:</p> <ol style="list-style-type: none">1. Replikasi Kerentanan: Anda melakukan tindakan replikasi kerentanan dengan mengunggah data dan memasukkan payload <code>'")/></code> pada input judul.2. Konfirmasi Eksekusi Payload: Anda mengonfirmasi bahwa payload tersebut berhasil dieksekusi oleh situs web, menunjukkan adanya kerentanan Stored XSS. Payload ini menyebabkan sebuah alert muncul di situs web, menandakan bahwa skrip yang disisipkan dieksekusi dengan sukses.  <p>https://jmp.sh/L2xiaLJ6</p> <p>link diatas adalah vidio contoh payload berhasil dijalankan</p>

9.	Rekomendasi	<ol style="list-style-type: none"> 1. Validasi dan Sanitasi Input: Pastikan bahwa semua input yang diterima dari pengguna disaring dan divalidasi dengan cermat sebelum disimpan dalam basis data atau ditampilkan kembali kepada pengguna lain. Gunakan metode sanitasi yang sesuai, seperti encoding HTML atau membuang tag dan karakter yang tidak diinginkan. 2. Penerapan Content Security Policy (CSP): Implementasikan kebijakan keamanan konten (CSP) untuk membatasi sumber yang dapat dimuat oleh halaman web. Ini dapat membantu mencegah eksekusi skrip yang tidak diinginkan, termasuk skrip yang disisipkan oleh serangan XSS. 3. Pemutakhiran Framework dan Library: Pastikan bahwa semua framework, library, dan komponen pihak ketiga yang digunakan dalam pengembangan situs web diperbarui secara teratur untuk memperbaiki kerentanan keamanan yang ditemukan. Hal ini termasuk memperbarui plugin, tema, dan komponen lainnya. 4. Penerapan Metode Keamanan yang Kuat: Terapkan prinsip keamanan pengembangan perangkat lunak yang kuat, seperti prinsip "secure by default" dan "least privilege". Ini termasuk penggunaan mekanisme otentikasi yang kuat, manajemen sesi yang aman, dan pembatasan akses ke fitur atau data sensitif. 5. Pendidikan dan Pelatihan: Berikan pelatihan kepada tim pengembangan tentang praktik pengembangan keamanan yang baik dan berikan pemahaman yang lebih baik tentang potensi kerentanan XSS. Pendidikan ini dapat membantu mengurangi risiko terhadap kerentanan di masa

		<p>mendatang.</p> <p>6. Pengujian Keamanan Reguler: Lakukan pengujian keamanan secara teratur, termasuk pengujian penetrasi dan pemindaian keamanan, untuk mengidentifikasi dan mengatasi kerentanan yang ada. Ini dapat membantu memastikan bahwa situs web tetap aman dari ancaman yang berkembang.</p>
10.	Referensi	OWASP TOP TEN