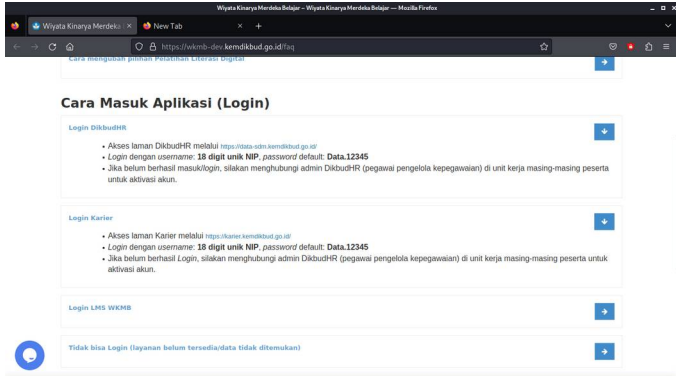
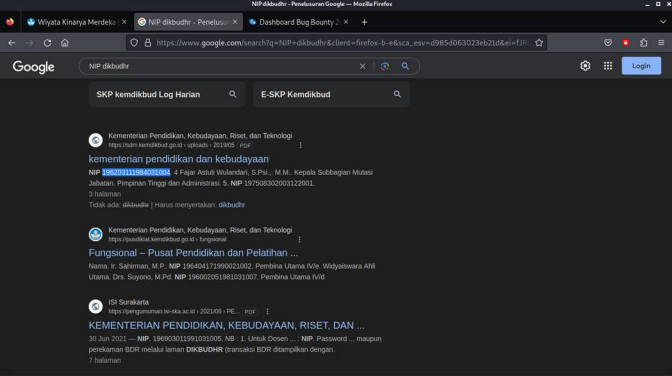
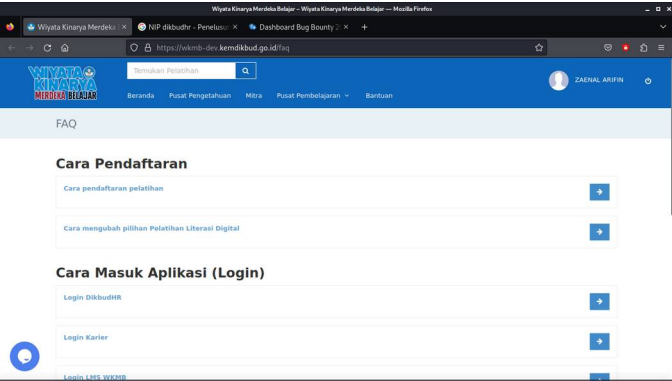


Laporan Pengujian atau Hasil Pencarian Celah Keamanan oleh Peserta Bug Bounty 2024

No.	Poin (Indikator)	Hasil
1.	Nama Target	WKMB
2.	Nama Kerentanan	Broken access control
3.	Jenis Kerentanan	A01 Broken access control
4.	Deskripsi Kerentanan	<p>Saya ingin memberitahukan tentang temuan kerentanan yang telah saya identifikasi pada sistem login kami. Kerentanan ini terkait dengan aturan login default yang memungkinkan akses ke sistem kepada semua pengguna yang memiliki nomor induk, dengan menggunakan password default yang sama.</p> <p>Analisis saya menunjukkan bahwa banyak nomor induk pengguna telah tersebar luas di internet, meningkatkan risiko akses tidak sah ke dalam sistem kami. Hal ini dapat mengakibatkan kerugian serius terhadap keamanan data dan integritas sistem.</p>
5.	Lokasi/URL	https://wkmb-dev.kemdikbud.go.id/faq
6.	<i>IP Address Source</i> (IP Address Peserta)	125.166.118.135
7.	Dampak	Saya telah berhasil mengeksploitasi kerentanan ini dengan menggunakan data pengguna yang tidak sah yang saya dapatkan dari internet, termasuk nomor induk pegawai

		<p>(NIP) yang tersebar luas. Dengan menggunakan data ini, saya login dengan akun orang lain, mengakibatkan potensi akses tidak sah terhadap data sensitif dan integritas sistem.</p>
8.	<p>Langkah Penetrasi dan Tangkapan Layar (Screenshots) Temuan</p>	<p>1. Pertama saya menemukan aturan pada website tersebut bahwa jika ingin login pada website yang telah di jelaskan pada bagian url https://wkmb-dev.kemdikbud.go.id/faq tersebut dengan NIP yang banyak tersebar di internet dan dengan default password</p> <p>2. Kemudian saya mencoba untuk login tanpa otorisasi yang sah. Dan saya berhasil melakukan hal tersebut.</p>  <p>Kemudian saya mencari data dari NIP dari internet</p>

		 <p>setelah saya menemukan data tersebut saya mencoba untuk melakukan login yang tidak sah</p> 
9.	Rekomendasi	<p>Langkah-langkah yang kami rekomendasikan untuk mengatasi kerentanan ini adalah:</p> <ol style="list-style-type: none"> 1. Perbaikan segera: Segera ubah aturan login default dan ganti dengan sistem autentikasi yang lebih aman, dengan memakai kata sandi yang kuat dan unik. 2. Pemberitahuan Pengguna: Segera informasikan kepada semua pengguna tentang perubahan aturan login dan pentingnya mengamankan akun mereka dengan kata sandi yang kuat. 3. Pemindaian Nomer Induk: Lakukan pemindaian secara menyeluruh di internet untuk mencari nomor induk yang terpublikasi dan berpotensi terpapar, serta

		<p>ambil langkah-langkah untuk mengurangi risiko akses tidak sah.</p> <p>4. Pelatihan Keamanan: Sediakan pelatihan kepada pengguna mengenai praktik keamanan yang baik, termasuk pentingnya menggunakan kata sandi yang kuat dan tidak membagikan informasi login dengan orang lain.</p> <p>5. Pemantauan Aktivitas: Aktif pantau aktivitas login dan identifikasi pola atau kejanggalan yang mencurigakan.</p> <p>6. Pembaruan Regulasi: Perbarui peraturan keamanan dan regulasi internal untuk mencegah terulangnya kerentanan serupa di masa depan.</p>
10.	Referensi	OWASP TOP TEN 2021