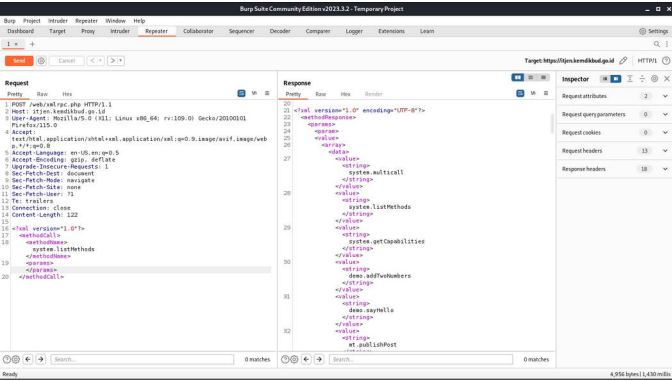


## Laporan Pengujian atau Hasil Pencarian Celah Keamanan oleh Peserta Bug Bounty 2024

No.	Poin (Indikator)	Hasil
1.	Nama Target	Website Itjen
2.	Nama Kerentanan	Security Misconfiguration
3.	Jenis Kerentanan	A05 Security Misconfiguration
4.	Deskripsi Kerentanan	XML-RPC (XML Remote Procedure Call) adalah protokol yang memungkinkan komunikasi antara aplikasi web yang berjalan pada platform yang berbeda. Namun, penggunaan XMLRPC yang tidak terlindungi dapat memungkinkan serangan jarak jauh seperti injeksi kode, eksekusi kode tak terduga, atau serangan brute force terhadap kata sandi.
5.	Lokasi/URL	<a href="https://itjen.kemdikbud.go.id/web/xmlrpc.php">https://itjen.kemdikbud.go.id/web/xmlrpc.php</a>
6.	IP Address Source (IP Address Peserta)	125.166.118.135
7.	Dampak	Jika kerentanan ini dieksploitasi, dapat mengakibatkan penggunaan situs web yang tidak sah, peretasan, atau pencurian data. Hal ini dapat merugikan pengguna situs web dan merusak reputasi situs tersebut.
8.	Langkah Penetrasi dan Tangkapan Layar (Screenshots) Temuan	<ol style="list-style-type: none"> <li><b>Penemuan file xmlrpc.php:</b> Langkah pertama dalam proses penetrasi adalah mencari file xmlrpc.php pada website target. File ini sering digunakan dalam implementasi XML-RPC (Remote Procedure</li> </ol>

		<p>Call) di WordPress dan beberapa platform lainnya. Penggunaan file ini dapat memberikan peluang untuk mengeksploitasi kerentanan keamanan.</p> <p>2. <b>Injeksi kode XML:</b> Setelah menemukan file xmlrpc.php, langkah berikutnya adalah melakukan injeksi kode XML pada website tersebut. Ini bisa dilakukan untuk mencoba menemukan metode-metode apa saja yang tersedia pada website tersebut. Dengan mengirimkan permintaan XML yang disesuaikan, penetrator dapat mencoba mengeksplorasi kerentanan atau celah keamanan yang mungkin ada dalam metode-metode yang tersedia.</p> 
9.	Rekomendasi	<ol style="list-style-type: none"><li>1. Saya merekomendasikan untuk memperbarui atau menonaktifkan layanan XMLRPC jika tidak digunakan secara aktif.</li><li>2. Terapkan pengaturan keamanan yang ketat pada server web untuk mencegah serangan brute force atau akses tidak sah.</li><li>3. Melakukan audit keamanan secara berkala dan memperbarui perangkat lunak serta plugin yang digunakan oleh situs web.</li></ol>

10.	Referensi	OWASP TOP TEN 2021