****

**JUDUL TEMUAN**

**28 Juli 2018**

**Oleh** **Anda**

|  |  |
| --- | --- |
| **Deskripsi** | **SQL Injection** adalah kerentanan yang terjadi pada aplikasi yang memungkinkan penyerang dapat membaca database SQL.  *dan seterusnya….* |
| **URL / Aplikasi** | **https://www.\*.fostiums.org/?id=2** |
| **Dampak** | 1. Data sensitif terpublikasi 2. Dapat masuk ke halaman adminsitrator |
| **Langkah-langkah** | 1. Masukkan query union select 1,2,user(),4 2. Setelah user terlihat, gunakan user tersebut untuk masuk ke admin 3. Cari halaman admin, dan masuk sebagai admin |
| **Bukti Temuan** | *Screenshot* gambar |
| **Remediasi / Rekomendasi** | 1. Variabel id harus divalidasi 2. Jangan menggunakan database SQL |
| **Referensi** | 1. [https://www.owasp.org/index.php/SQLInjection](https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)) |