SECURITY VULNERABILITY REPORT

Universitas Syiah Kuala (usk.ac.id)

1. Informasi Pelapor

- Nama: Nabil Aulia Dika
- NPM: 250810701100090
- Program Studi: Informatika
- Tanggal Laporan: 29 April 2026

2. Ringkasan Eksekutif

Laporan ini memuat temuan kerentanan keamanan siber yang terdeteksi melalui teknik *Open Source Intelligence* (OSINT) menggunakan perangkat lunak sumber terbuka pada infrastruktur digital Universitas Syiah Kuala (usk.ac.id). Temuan utama mencakup jejak riwayat *Web Defacement* (injeksi konten perjudian) yang tercatat pada indeks mesin pencari, serta eksposur publik yang masif pada lingkungan pengembangan (*development*) dan alamat surel internal.

3. Temuan Detail

A. Riwayat Web Defacement & SEO Poisoning (Tingkat Keparahan: TINGGI)

Ditemukan jejak injeksi URL ilegal (perjudian/togel) pada beberapa subdomain. Meskipun status HTTP saat ini mungkin menunjukkan 404 (Not Found), jejak ini menandakan bahwa penyerang pernah berhasil mengeksploitasi celah (seperti *unrestricted file upload* atau kerentanan CMS) untuk menanamkan direktori asing. URL Terdampak dan Indikasi Ancaman:

- https://fkep.usk.ac.id/BABEJUDI/ (Riwayat Injeksi Judi Online)
- https://siakadup3ai.usk.ac.id/BABEJUDI/ (Riwayat Injeksi Judi Online)
- https://sibela.usk.ac.id/market/?kemajuan=Safnah (Backlink Togel / Spam SEO)
- https://sippan.usk.ac.id/kejora/?perkara=KOI-TOTO-TOGEL-LOGIN (Backlink Togel / Spam SEO)

B. Eksposur Data Publik (Tingkat Keparahan: SEDANG) Pemindaian OSINT mendeteksi 35 alamat surel institusi fungsional yang terekspos secara publik. Data ini rawan dimanfaatkan sebagai vektor serangan *Social Engineering* maupun *Spear Phishing* yang ditargetkan pada staf atau dosen USK.

- **Catatan:** Daftar lengkap 35 alamat surel fungsional yang terdampak telah dilampirkan pada dokumen pendukung: `full_hosts_scan_usk.txt`.

C. Pemetaan Subdomain / Potential Attack Surface (Tingkat Keparahan: SEDANG)
Pemindaian pasif menemukan total 893 subdomain/host aktif yang memetakan infrastruktur jaringan secara terbuka. Beberapa di antaranya memerlukan perhatian khusus karena menunjukkan indikasi lingkungan pengujian (*development environment*) yang dapat diakses publik tanpa autentikasi dasar.

- **Aset Berisiko Tinggi:** `dev.fk.usk.ac.id`, `perwaliandev.usk.ac.id`.
- **Catatan:** Pemetaan lengkap 893 host dan alamat IP terkait telah dilampirkan secara utuh pada dokumen pendukung: `full_hosts_scan_usk.txt`.

4. Rekomendasi Mitigasi (Berdasarkan Security Best Practices) Sebagai langkah mitigasi risiko preventif untuk melindungi aset digital universitas, berikut adalah beberapa penyesuaian keamanan yang disarankan:

1. **Pemeriksaan Integritas Sistem (File Auditing):** Disarankan untuk melakukan pemeriksaan menyeluruh pada direktori web fakultas yang tercatat memiliki riwayat *defacement*, guna memastikan tidak ada anomali atau skrip berbahaya (seperti *backdoor/web shell*) yang masih bersarang di dalam *server*.
2. **Pembatasan Lingkungan Pengembangan:** Direkomendasikan untuk menerapkan pembatasan akses secara ketat (misalnya melalui implementasi *IP Whitelisting* atau *VPN Campus*) pada seluruh subdomain yang diperuntukkan bagi fase *development* dan *testing*.
3. **Audit Pemetaan DNS (DNS Hygiene):** Meninjau kembali daftar *DNS records* dari hasil pemindaian terlampir dan mempertimbangkan untuk menonaktifkan (*deprovisioning*) subdomain maupun layanan yang sudah tidak beroperasi guna memitigasi risiko *Subdomain Takeover*.