Nomor Kasus		
Tanggal Laporan		16 Juni 2025
Disusun Oleh		Muhammad Mardiansyah
Klasifikasi		Rahasia / Internal

1. Ringkasan Eksekutif

Pada tanggal 16 Juni 2025, terdeteksi insiden keamanan siber yang mempengaruhi keamanan pada website fmcpakistan.com.

Jenis insiden: [akses tidak sah, sql injection, dan kebocoran data sensitif.].

Langkah mitigasi dilakukan pada tanggal 16 juni 2025, dan hasil analisis awal menunjukkan penyebab utamanya adalah sql injection dengan parameter products?category=5.

2. Deskripsi Insiden

a. Jenis Insiden : sql injection, pencurian data, akses tidak sah

b. Tanggal & Waktu Ditemukan : 16 Juli 2025

c. Perkiraan Waktu Awal Terjadi : 16 Juli 2025

d. Sistem/Lokasi Terdampak : http://fmcpakistan.com.pk

e. Metode Deteksi : Penggunaan tools sqlmap pada kali linux.

SQLMAP :

- Melakukan identifikasi parameter rentan SQL Injection.
- Menggunakan SQLMap untuk mengakses database backend secara otomatis.
- Menampilkan informasi sensitif seperti nama database, tabel, dan kolom.
- Melakukan dump/download isi dari tabel yang berisi data sensitif.
- Mencoba melakukan login dengan kredensial (username dan password) yang berhasil ditemukan melalui eksploitasi.

3. Dampak yang Dirasakan

a. Sistem Terpengaruh: Sistem basis data organisasi berhasil diakses tanpa otorisasi

b. Data yang Terlibat:

- Data pribadi pengguna (misalnya: nama, email, password hash).
- Informasi login (username dan password).

c. Pengguna Terdampak: 1

d. Layanan Terganggu: database berhasil diekstrak, tabel dan kolom yang berisi data sensitif berhasil dicuri.

e. Klasifikasi Dampak:

- Kerahasiaan : Tinggi
- Integritas : Tinggi
- Ketersediaan : Rendah
- Reputasi : [Rendah / Sedang / Tinggi]

4. Analisis Akar Masalah (Root Cause Analysis)

a. Vektor Serangan Awal : Terdapat parameter yang lemah terhadap sql injection pada url seperti products?category=5.

b. Faktor Kontributif : Tidak adanya mekanisme *prepared statements* atau ORM untuk query SQL. Tidak ada sistem WAF (Web Application Firewall) yang aktif untuk memblokir payload berbahaya.

c. Alat / Teknik Penyerang : Sqlmap

d. Asal Serangan :

5. Response dan Mitigasi

a. Langkah Awal yang Diambil:

- Pemindaian dan pembersihan malware untuk mendeteksi adanya kemungkinan malware atau file berbahaya.
- Melakukan reset atau pergantian password bagi akun yang terdampak.
- Pencatatan dan dokumentasi insiden.

b. Komunikasi:

- Pemberitahuan terhadap manajemen dan unit terkait
- Gunakan *prepared statements* atau ORM untuk query database.
- Aktifkan WAF untuk memblokir payload otomatis dan eksploitasi umum.
- Audit keamanan aplikasi web secara berkala.

c. Status Saat Ini : Terkendali

6. Rekomendasi dan Tindakan Perbaikan

No	Rekomendasi	Penanggung Jawab	Tenggat Waktu	Status
1	Aktifkan WAF untuk memblokir payload otomatis.	Tim IT	5 hari	Dalam proses
2	Menambahkan prepared statement	Tim IT	5 hari	Belum dimulai
3	Audit keamanan secara berkala	Infrastruktur	90 hari	Selesai

7. Evaluasi Pasca Insiden

a Diperlukan pemantauan keamanan website secara berkala.
b SOP respons insiden perlu ditinjau dan diuji berkala.
c Lakukan uji coba website setelah menambahkan prepared statement.
d Aktifkan WAF untuk blokir payload.

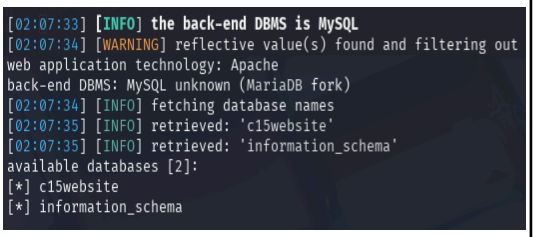
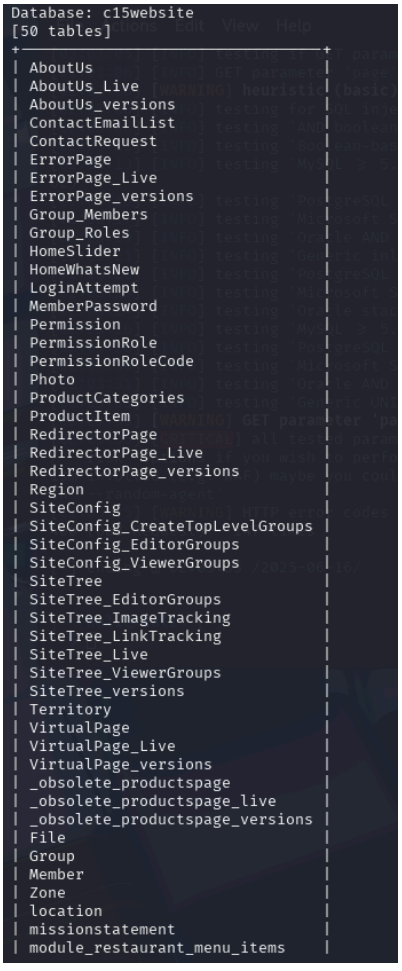
8. Lampiran dan Bukti Teknis

a Bukti visual (screenshot atau capture).
b Laporan hasil eksploitasi.

9. Kesimpulan

Insiden ini menunjukkan perlunya perbaikan dalam aspek tertentu seperti keamanan validasi input, pengelolaan akses terhadap parameter web, dan penerapan kontrol keamanan seperti WAF dan logging. Kerentanan SQL Injection yang berhasil dieksploitasi melalui parameter category=5 di URL merupakan bukti lemahnya pengamanan pada sisi server terhadap manipulasi input.

LAMPIRAN: BUKTI PENDUKUNG INSIDEN

No	Jenis Lampiran	Deskripsi	Status	Catatan / Referensi
A	Database Terdeteksi	Tangkapan layar dari database yang tersedia pada website.	✓	
B	Tabel Terdeteksi	Tangkapan layar dari tabel yang tersedia pada database C15website.	✓	

No	Jenis Lampiran	Deskripsi	Status	Catatan / Referensi
C	Kolom dari tabel member	Tangkapan layar dari kolom yang tersedia pada tabel Member.	✓	Database: c15website Table: Member [23 columns] +---+---+ | Column | Type | +---+---+ | AutoLoginExpired | datetime | | AutoLoginHash | varchar(160) | | ClassName | enum('Member') | | Created | datetime | | DateFormat | varchar(30) | | Email | varchar(254) | | FailedLoginCount | int(11) | | FirstName | varchar(50) | | ID | int(11) | | LastEdited | datetime | | LastVisited | datetime | | Locale | varchar(6) | | LockedOutUntil | datetime | | NumVisit | int(11) | | Password | varchar(160) | | PasswordEncryption | varchar(50) | | PasswordExpiry | date | | RememberLoginToken | varchar(160) | | Salt | varchar(50) | | Surname | varchar(50) | | TempIDExpired | datetime | | TempIDHash | varchar(160) | | TimeFormat | varchar(30) | +---+---+
D	Isi dari kolom member	Tangkapan layar dari kolom Suname, email, password. password menggunakan teknik hashing bcrypt.	✓	Database: c15website Table: Member [3 entries] +---+---+---+ | Surname | Email | Password | +---+---+---+ | NULL | admin | $2y$10$3e6fbe7c4d8ad9cf4810euXpnqmJiWF3KC.h5MZeK1Nc.jna.VNGK | | Akhtar | maham.akhtar@fmc.com | $2y$10$671a4e089b465409c4996ejK.BGVhmksqxKMVeEqYHw9vXyOlId3. | | Asghar | urooj.asghar@fmc.com | $2y$10$7e347b80e37a420a5c7580tsm85sDUZxe5qCcZmTSJPEWSLcTGa7i | +---+---+---+

Catatan:

- Kolom **Status** bisa diisi ✓ (tersedia) atau ✗ (belum tersedia).
- Kolom **Catatan/Referensi** digunakan untuk merujuk lokasi penyimpanan, link internal, atau ID artefak.
- Format ini fleksibel dan bisa dikembangkan sesuai kebutuhan tim keamanan atau pihak auditor