

1. We are given with website.html and a hash to be cracked for a password
2. Now to get the words out of the html file, we will host it on localhost and then run cewl on it using
`python3 -m http.server 8000`
<http://localhost:8000>
3. Now we can use a tool called cewl to get the words out of the website. Using
`cewl -w wordlist.txt` <http://localhost:8000/website.html>

4. We can use munging on the wordlist to get the closer enough wordlist of the potential passwords
5. For this we gitclone munge directory and then run `python munge3.py -l 3 -i wordlist.txt -o munged.txt`

6. Now we have a close wnoh wordlist, now we will crack password using john using
7. john target.hash --wordlist=Munged.txt --rules OneRuleToRuleThemStill.rule where
oneruletorulethemall.rule contains the rules on which most passwords are based.
8. On running this script for almost 20 min, we get the password as sw4shbucker13

```
File Actions Edit View Help
kali@kali:~/Desktop
# 0:00:10:01 1.15% (ETA: 2025-10-27 10:13) 8g/s 16.18p/s 16.18c/s 16.18C/s med10007..med1015
# 0:00:10:26 1.15% (ETA: 2025-10-27 10:12) 8g/s 16.12p/s 16.12c/s 16.12C/s med1101..med12011
# 0:00:10:43 1.17% (ETA: 2025-10-27 10:11) 8g/s 16.12p/s 16.12c/s 16.12C/s meqgm3..meqgm91
# 0:00:10:34 1.20% (ETA: 2025-10-27 10:09) 8g/s 16.12p/s 16.12c/s 16.12C/s mynicall12345..myth
12325
# 0:00:10:43 1.23% (ETA: 2025-10-27 10:07) 8g/s 16.12p/s 16.12c/s 16.12C/s pqular...pqular5
# 0:00:10:21 1.23% (ETA: 2025-10-27 10:06) 8g/s 16.12p/s 16.12c/s 16.12C/s p44022..p44040
# 0:00:12:00 1.20% (ETA: 2025-10-27 10:06) 8g/s 16.12p/s 16.12c/s 16.12C/s personal1901..pers
onal1909
# 0:00:12:43 1.20% (ETA: 2025-10-27 10:05) 8g/s 16.12p/s 16.12c/s 16.12C/s piratex18..piratex7
8
# 0:00:14:00 1.24% (ETA: 2025-10-27 10:05) 8g/s 16.12p/s 16.12c/s 16.12C/s priv00000000..priv
00000000
# 0:00:14:20 1.20% (ETA: 2025-10-27 10:06) 8g/s 16.12p/s 16.12c/s 16.12C/s que112..que1508
# 0:00:14:45 1.20% (ETA: 2025-10-27 10:06) 8g/s 16.12p/s 16.12c/s 16.12C/s r10000..r10520
# 0:00:14:55 1.20% (ETA: 2025-10-27 10:06) 8g/s 16.12p/s 16.12c/s 16.12C/s r3cruiting123..r3cr
uiting
# 0:00:15:04 1.27% (ETA: 2025-10-27 10:05) 8g/s 16.12p/s 16.12c/s 16.12C/s refcom123..refcom
1
# 0:00:15:22 1.27% (ETA: 2025-10-27 10:06) 8g/s 16.12p/s 16.12c/s 16.12C/s refcom00..refcom4
# 0:00:15:28 1.20% (ETA: 2025-10-27 10:06) 8g/s 16.12p/s 16.12c/s 16.12C/s real00..recruiting0
# 0:00:15:40 1.10% (ETA: 2025-10-27 10:05) 8g/s 16.12p/s 16.12c/s 16.12C/s repayr..repayr111
# 0:00:15:44 1.20% (ETA: 2025-10-27 10:05) 8g/s 16.12p/s 16.12c/s 16.12C/s r000111111..r0002
0
# 0:00:16:01 1.10% (ETA: 2025-10-27 10:07) 8g/s 16.12p/s 16.12c/s 16.12C/s ritual00..ritual101
# 0:00:16:28 1.40% (ETA: 2025-10-27 10:10) 8g/s 16.12p/s 16.12c/s 16.12C/s route227..route394
# 0:00:16:49 1.42% (ETA: 2025-10-27 10:11) 8g/s 16.12p/s 16.12c/s 16.12C/s r040123456789..r04
0130
# 0:00:16:51 1.42% (ETA: 2025-10-27 10:12) 8g/s 16.12p/s 16.12c/s 16.12C/s rule004..rule009
# 0:00:17:18 1.45% (ETA: 2025-10-27 10:13) 8g/s 16.12p/s 16.12c/s 16.12C/s slarck..slarck5
# 0:00:17:37 1.44% (ETA: 2025-10-27 10:17) 8g/s 16.12p/s 16.12c/s 16.12C/s sal104..sal104r12
# 0:00:18:01 1.45% (ETA: 2025-10-27 10:19) 8g/s 16.12p/s 16.12c/s 16.12C/s sbm025..sbm03
# 0:00:18:18 1.40% (ETA: 2025-10-27 10:21) 8g/s 16.02p/s 16.02c/s 16.02C/s sal104r12345678..sa
104r12
# 0:00:18:54 1.47% (ETA: 2025-10-27 10:24) 8g/s 16.02p/s 16.02c/s 16.02C/s s0012345678..s0020
# 0:00:19:24 1.40% (ETA: 2025-10-27 10:26) 8g/s 16.02p/s 16.02c/s 16.02C/s s01001..s01009
# 0:00:19:43 1.30% (ETA: 2025-10-27 10:28) 8g/s 16.02p/s 16.02c/s 16.02C/s sl10018..sl10027
# 0:00:19:24 1.52% (ETA: 2025-10-27 10:30) 8g/s 16.02p/s 16.02c/s 16.02C/s sp3cific0..sp3cific4
0
# 0:00:19:53 1.52% (ETA: 2025-10-27 10:34) 8g/s 16.02p/s 16.02c/s 16.02C/s spring11..spring24
# 0:00:21:16 1.54% (ETA: 2025-10-27 10:36) 8g/s 16.02p/s 16.02c/s 16.02C/s str0mp0r0..str0mp0
r01
# 0:00:21:43 1.55% (ETA: 2025-10-27 10:37) 8g/s 16.02p/s 16.02c/s 16.02C/s superstitious06..su
perstitious05
# 0:00:21:44 1.55% (ETA: 2025-10-27 10:37) 8g/s 16.02p/s 16.02c/s 16.02C/s superstitious00..sup
erstitious05
# 0:00:21:54 1.50% (ETA: 2025-10-27 10:38) 8g/s 16.02p/s 16.02c/s 16.02C/s sw001234..sw001234
buckler13
# 0:00:21:56 DONE (2025-10-25 03:56) 0.000228g/s 16.02p/s 16.02c/s 16.02C/s sw001234buckler13..sw0
01234buckler13
Use the "-show" option to display all of the cracked passwords reliably
Session completed.
```

- 9.
10. Now we have the password=sw4shbuckler13, we can submit this as flag in the flag format.