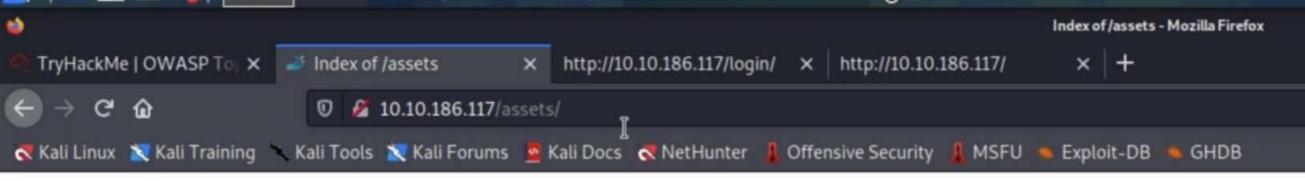


SENSITIVE DATA EXPOSURE





Index of /assets

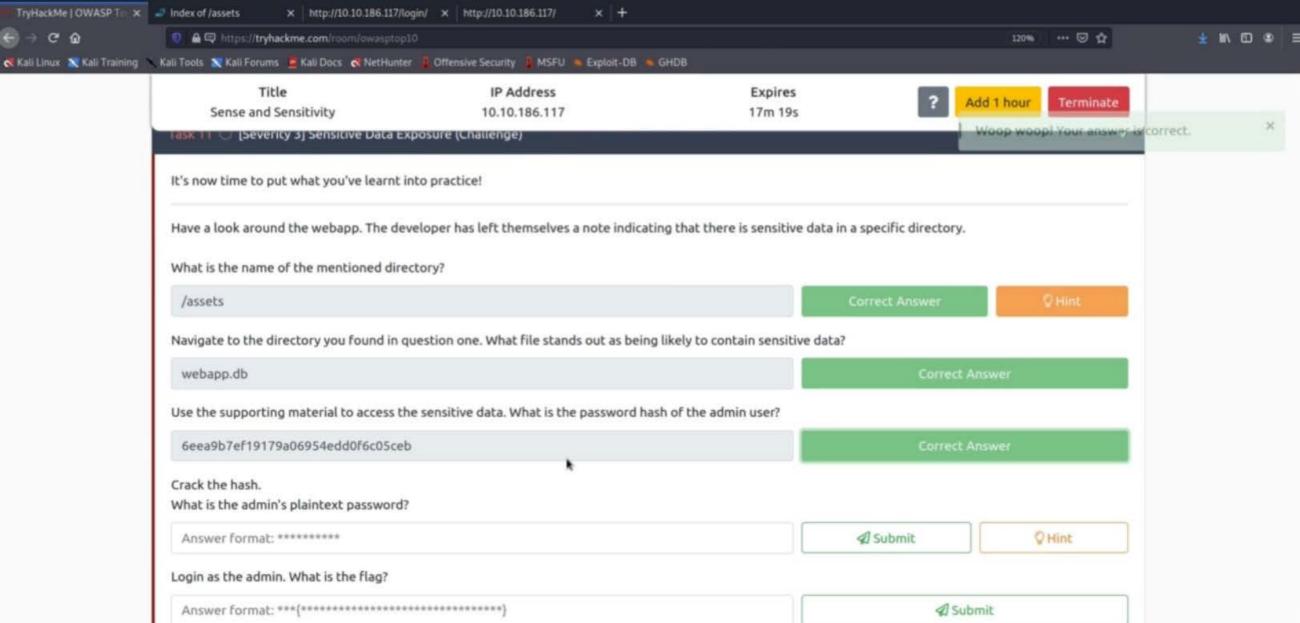
Name	Last modified	Size Description
Parent Directory		
css/	2020-07-14 17:52	-
fonts/	2020-07-14 15:42	
images/	2020-07-14 15:42	
<u>js/</u>	2020-07-14 15:52	
php/	2020-07-14 15:42	
webapp.db	2020-07-14 17:52	28K

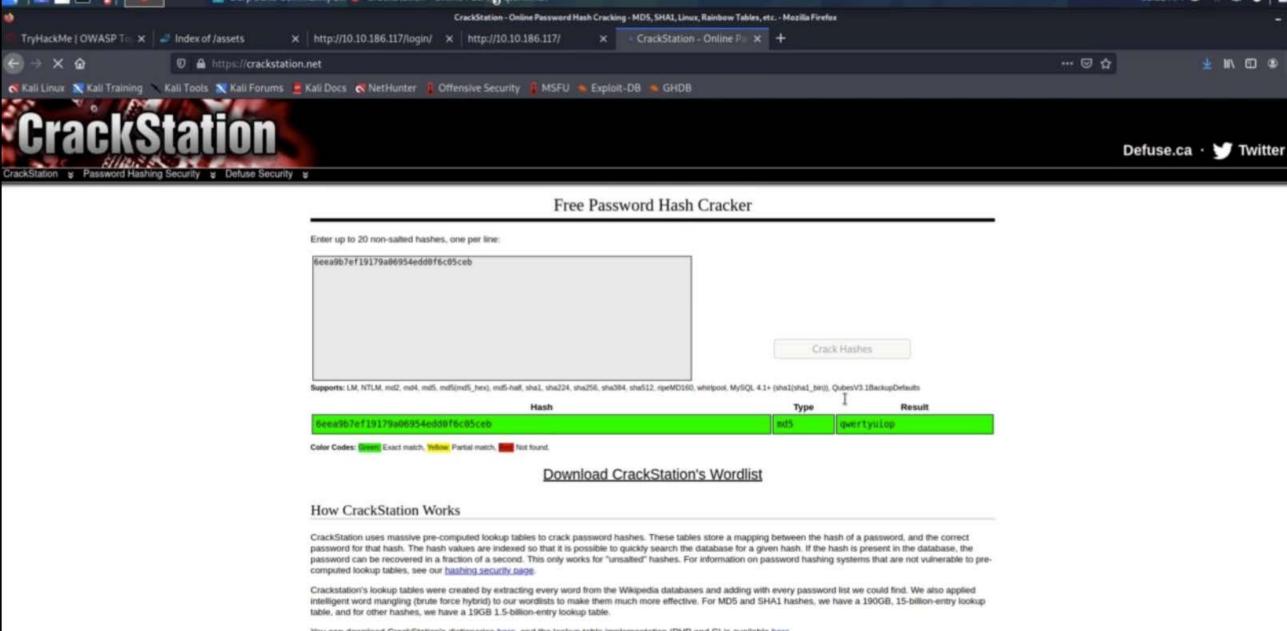
Apache/2.4.29 (Ubuntu) Server at 10.10.186.117 Port 80

```
File Actions Edit View Help
   (mrhacker⊗ kali)-[~]
   cd Downloads
   (mrhacker * kali) - [~/Downloads]
cacert.der
            printmrhacker.ovpn webapp.db
   (mrhacker⊕ kali) - [~/Downloads]
  $ sqlite3 webapp.db
```

```
cd Downloads
(mrhacker & kali) - [~/Downloads]
cacert.der printmrhacker.ovpn webapp.db
(mrhacker ** kali) - [~/Downloads]
sqlite3 webapp.db
SQLite version 3.34.1 2021-01-20 14:10:07
Enter ".help" for usage hints.
sqlite> .tables
sessions users
sqlite> SELECT * FROM users;
4413096d9c933359b898b6202288a650|admin|6eea9b7ef19179a06954edd0f6c05ceb|1
23023b67a32488588db1e28579ced7ec|Bob|ad0234829205b9033196ba818f7a872b|1
4e8423b514eef575394ff78caed3254d|Alice|268b38ca7b84f44fa0a6cdc86e6301e0|0
sqlite>
```

(mrhacker⊕kali)-[~]





₩ M CD 🕸 🗏

Free Password Hash Cracker

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



Color Codes: Green, Exact match, Yellow: Partial match, Match, Inc.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to precomputed lookup tables, see our <u>hashing security page</u>.

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup