Crypto CTF

1. find
2. log in
3. AES
4. break

find

- QR code on your badge
  - yes, server change

log in

```
resp = requests.post(
    "http://{0}/api-token".format(SERVER),
    data={"user": "becca", "password": "908ygiw42*ho3iu98
)
```

hint? AES

```
payload = json.dumps({"admin": admin,
"user": user}, sort_keys=True)
# encrypt the payload
return _encrypt(payload)
```

AES is not a AEAD by default

break

- understand the structure
- flip ciphered bits
- change the resulting output

```
data = binascii.unhexlify(token)
mutable_data = bytearray(data)
mutable_data[26] ^= ord("0")
mutable_data[26] ^= ord("1")
admin_token = binascii.hexlify(mutable_data)
```

break :: win

- bc1ad1fd22f8367217ced9673e0a7a16aed97409e13aa8539eb2132a928f43d3b51cd1d819fb86e6df4f5fde06
- bc1ad1fd22f8367217ced9673e0a7a16aed97409e13aa8539eb2122a928f43d3b51cd1d819fb86e6df4f5fde06