

## Задание выполнил студент группы 2345 Романенко К.Д.

1. Имеется логин **admin** и пароль **yo30E#jb**, которые были заданы администратором для входа в систему с использованием веб-формы. Можно ли считать такую комбинацию логина и пароля безопасной для защиты от брутфорса? Ответ обоснуйте.

Я считаю, что данная комбинация небезопасна.

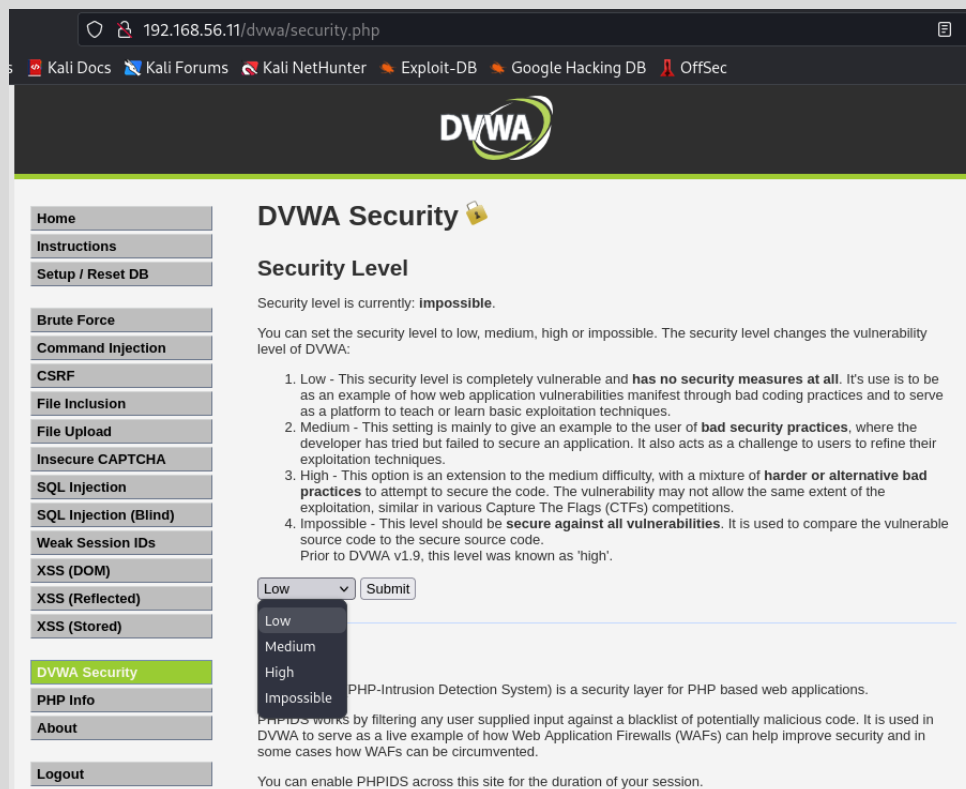
Логин admin – стандартный. В 99% случаев эта учётная запись имеет права sudo. Злоумышленник, на этапе разведки пробежится по словарям и обнаружит, что такой логин есть. Далее брутфорсом подберет пароль.

Да, можно выставить ограничение на 5 попыток входа в течение n-ого времени, но рассуждения на данную тему не входят в тело вопроса.

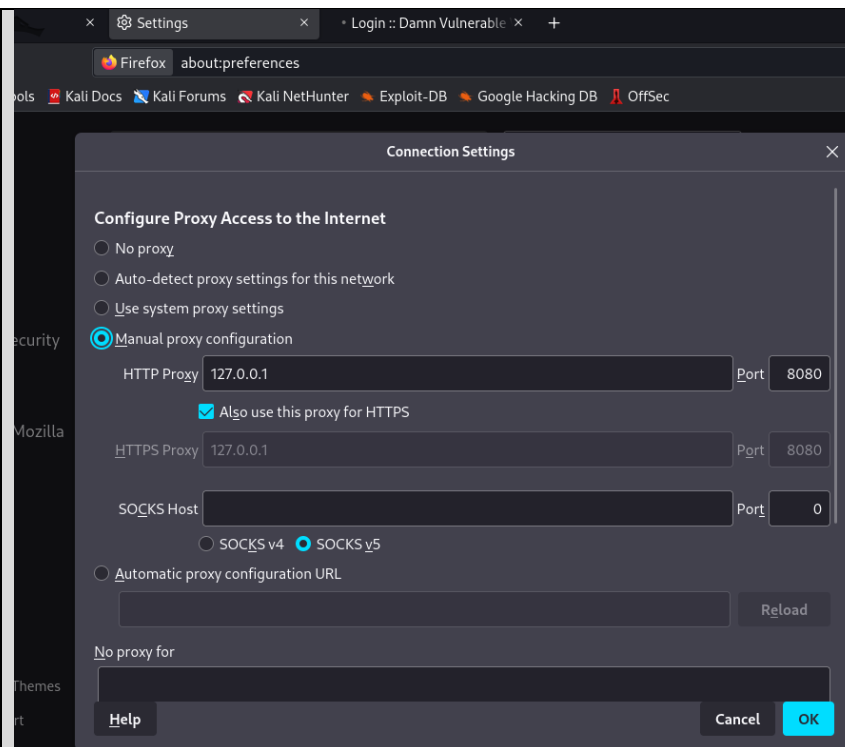
2. Подберите логин и пароль к странице bruteforce-сервиса **dvwa** на уровне сложности LOW. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

Открыл браузер на kali. Подключился к 192.168.56.11. Выбрал DVWA.

Ввёл логин – пароль: admin – password. Изменил уровень сложности на Low

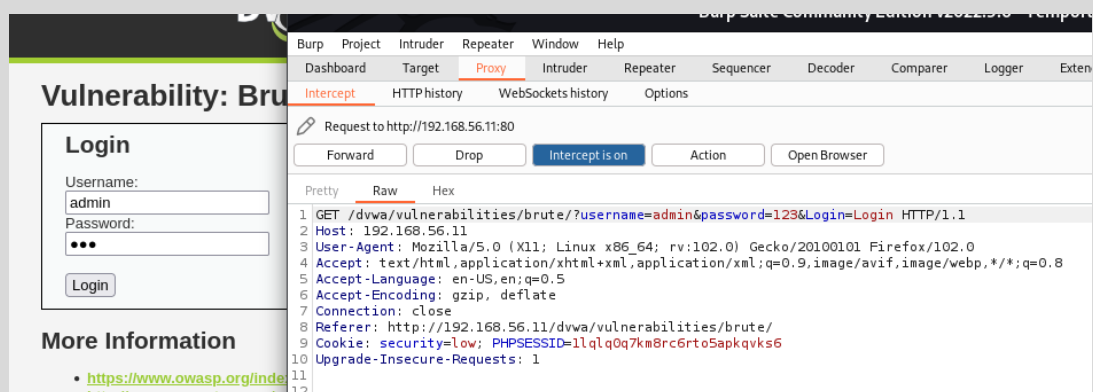


Открыл BurpSuite. Настроил Proxy в браузере

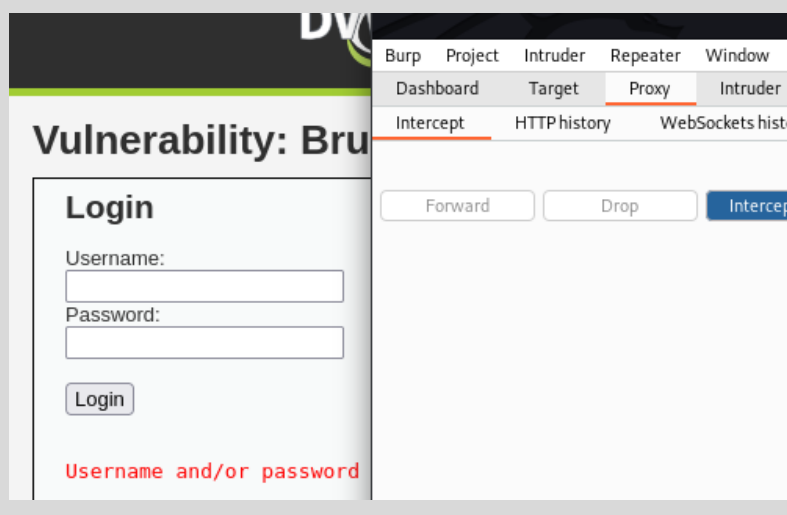


Открыл сайт вкладку Brute Force на сайте DVWA

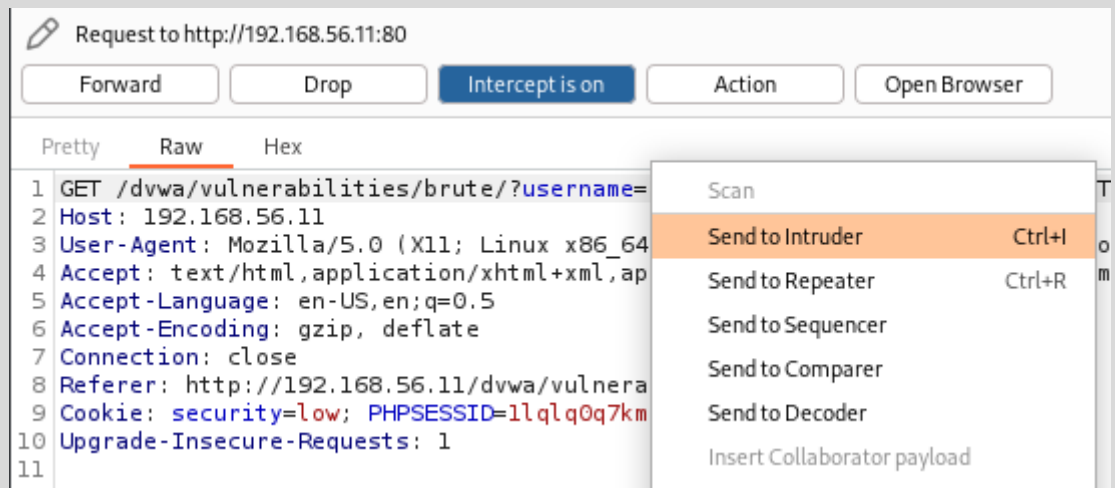
Открыл Burp Suite и запустил проху. В форму на dvwa ввёл логин - пароль: admin - 123.



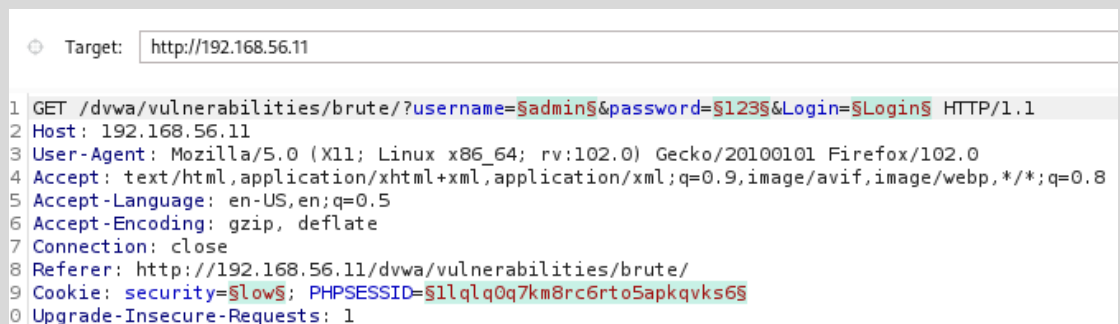
В Burp нажал Forward. Итог: комбинация логин/пароль неверна



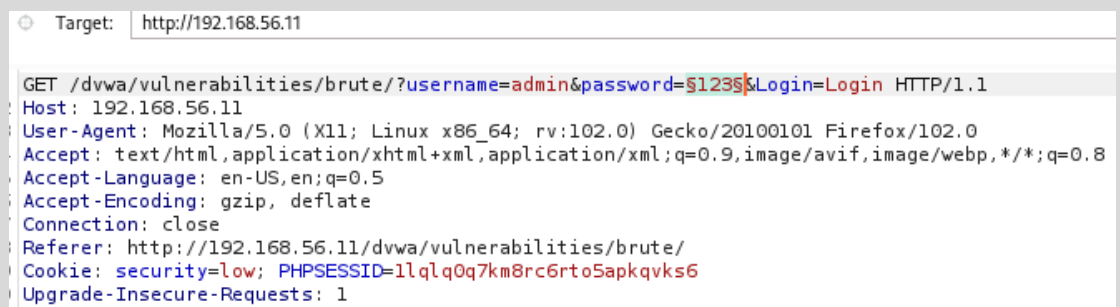
## ПКМ в burp и Send to Intruder



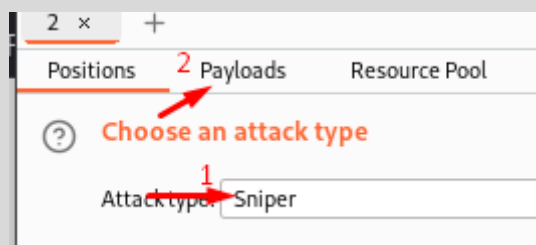
## Вывод Intruder'a:



Очистил выделение переменных с помощью Clear. Выделил значение password и нажал Add



Выбрал тип атаки Sniper, открыл вкладку Payloads



Задал payload set (1 переменная, Simple list) Наполнил payload options данными, т.е. паролями, которые надо подставить методом bruteforce

**?** **Payload Options [Simple list]**

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

Paste	password
Load ...	admin
Remove	12345
Clear	12345678
Deduplicate	1111
	qwerty

**Add**

Add from list ... [Pro version only] ▼

Вкладка Options. Пункт Grep-Match

Здесь ввёл все варианты вывода ответа, которые нужно отсеять из результатов. Сначала очистил фильтр

**?** **Grep - Match**

**↶** These settings can be used to flag result items containing specified expressions.

☐ Flag result items with responses matching these expressions:

Paste	error
Load ...	exception
Remove	illegal
<b>1 Clear</b>	invalid
	fail
	stack
	access
	directory
	file
	not found

**2 Add**

Match type: ☒ Simple string ☐ Regex

>>> Start Attack <<<

## Результат:

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Passwor...	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
1	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5524		
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
3	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
4	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
5	1111	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
6	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	

Из всего списка выбивается password с Length = 5524

Request ^	Payload	Status	Error	Timeout	Length	Passwor...	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
1	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5524		
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
3	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
4	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
5	1111	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	
6	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1	

Request Response

Pretty Raw Hex

```
1 GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 192.168.56.11
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 Referer: http://192.168.56.11/dvwa/vulnerabilities/brute/
9 Cookie: security=low; PHPSESSID=1lqlq0q7km8rc6rto5apkvks6
10 Upgrade-Insecure-Requests: 1
```

Нажал Response -> Render

Request ^	Payload	Status	Error	Timeout	Length	Passwor...
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
1	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
3	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
4	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
5	1111	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
6	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1

Request

Response

Pretty

Raw

Hex

Render

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

## Login

Username:

Password:

Login

Welcome to the password protected area admin

Готово. Сочетание admin – password рабочее.

Для самопроверки чекнул другое сочетание с Length = 5486

Request ^	Payload	Status	Error	Timeout	Length	Passwor...
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
1	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5524	
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
3	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
4	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
5	1111	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1
6	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	5486	1

Request

Response

Pretty

Raw

Hex

Render

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

## Vulnerability: Brute Force

### Login

Username:

Password:

Login

Username and/or password incorrect.

- Подберите логин и пароль к странице Broken Auth. - Weak Passwords сервиса bwapp на уровне сложности LOW. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

Открыл bwapp. Ввёл логин/пароль – bee/bug. В правом верхнем углу выбрал нужный пункт и уровень сложности

Choose your bug:

Broken Authentication - Weak Passwords

Hack

Set your security level:

low

Set

Current: low

Результат подготовки:

## / Broken A

Enter your credentials.

Login:

Password:

Login

Попробовал различные варианты логин-пароль, ответ один:

Login

Invalid credentials!

Значит надо подбирать обе переменные. Поехали

Включил Proxy в Burp Suite

Request to http://192.168.56.11:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /bwapp/ba_weak_pwd.php HTTP/1.1
2 Host: 192.168.56.11
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://192.168.56.11
10 Connection: close
11 Referer: http://192.168.56.11/bwapp/ba_weak_pwd.php
12 Cookie: PHPSESSID=eicu9ni8n9jc7nm7987iv7tn07; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 login=admin&password=123&form=submit
```

Залил в Intruder. Задал переменные для брут форса

Target: http://192.168.56.11

```
1 POST /bwapp/ba_weak_pwd.php HTTP/1.1
2 Host: 192.168.56.11
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://192.168.56.11
10 Connection: close
11 Referer: http://192.168.56.11/bwapp/ba_weak_pwd.php
12 Cookie: PHPSESSID=eicu9ni8n9jc7nm7987iv7tn07; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 login=$admin$&password=$123$&form=submit
```

Тип атаки Sniper



В Kali есть заготовленные словари в директории /usr/share/wordlists

```
File Actions Edit View Help
└─$ cd /usr/share/wordlists

(kali@kali)-[/usr/share/wordlists]
└─$ ls -al
total 52124
drwxr-xr-x  2 root root   4096 Feb 11 2022 .
drwxr-xr-x 320 root root 12288 Apr 12 12:54 ..
lrwxrwxrwx  1 root root    25 Feb 11 2022 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx  1 root root    30 Feb 11 2022 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx  1 root root    41 Feb 11 2022 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx  1 root root    41 Feb 11 2022 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx  1 root root    46 Feb 11 2022 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx  1 root root    41 Feb 11 2022 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r--  1 root root 53357329 Jul 17 2019 rockyou.txt.gz
lrwxrwxrwx  1 root root    25 Feb 11 2022 wfuzz → /usr/share/wfuzz/wordlist
```

Выбрал словарь nmap

Также есть большой словарь **fuzzdb** на гитхабе

Выбрал Payload Set = 1, Simple list

Подставил словарь в Payload Options через Load

**Payload Options [Simple list]**

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

Paste Load ... Remove Clear Deduplicate Add

654321

654321  
michael  
jessica  
111111  
ashley  
000000  
iloveu

Add from list ... [Pro version only]

Вкладка Options. Пункт Grep-Match

Оставил со значениями по умолчанию. Среди них есть invalid.

Для Payload Set = 2 сделал аналогично

**Payload Sets**

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

Payload set: 1 Payload count: 5,007  
Payload type: Simple list Request count: 25,070,049

**Payload Sets**

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

Payload set: 2 Payload count: 5,007  
Payload type: Simple list Request count: 25,070,049

25 млн комбинаций

>>> Start Attack <<<

Старт 02.03.23 в 12:06

## 24 990 001 комбинация

11. Intruder attack of http://192.168.56.11 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
1503	cassidy	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
0							
1	123456	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
2	12345	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
3	123456789	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
4	password	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
5	iloveyou	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
6	princess	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
7	12345678	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
8	1234567	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
9	abc123	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
10	nicole	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
11	daniel	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
12	monkey	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	
13	babunil	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	13710	

Request

Pretty Raw Hex

```
1 POST /bwapp/ba_weak_pwd.php HTTP/1.1
2 Host: 192.168.56.11
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://192.168.56.11
10 Connection: close
11 Referer: http://192.168.56.11/bwapp/ba_weak_pwd.php
12 Cookie: PHPSESSID=eicu9ni8n9jc7nm7987iv7tn07; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 login=esperanza&password=123456&form=submit
```

1502 of 24990001

Очень низкая скорость перебора. 300 комбинаций/час

Ждать, пока он все подберет, времени нет. Оставлю так

*Есть возможность ускорить процесс брут форса?*

- Через консольные утилиты быстрее, GET быстрее POST
- Вообще, конечно, такой брут не делают обычно, это слишком заметно. Делают ну 500 максимум

4. \* Протестируйте пример 3 на практике. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

5. \* Решите задание <http://challenge01.root-me.org/web-serveur/ch3/> методом брутфорса. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

