

02.10.2023

Курс:

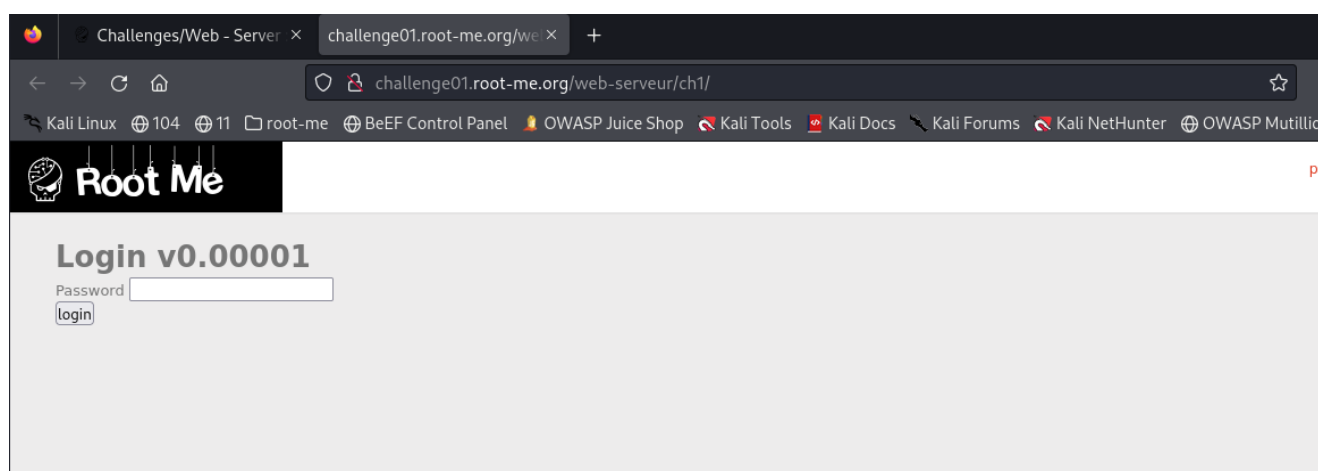
Практическая работа к уроку № Lesson\_5

--

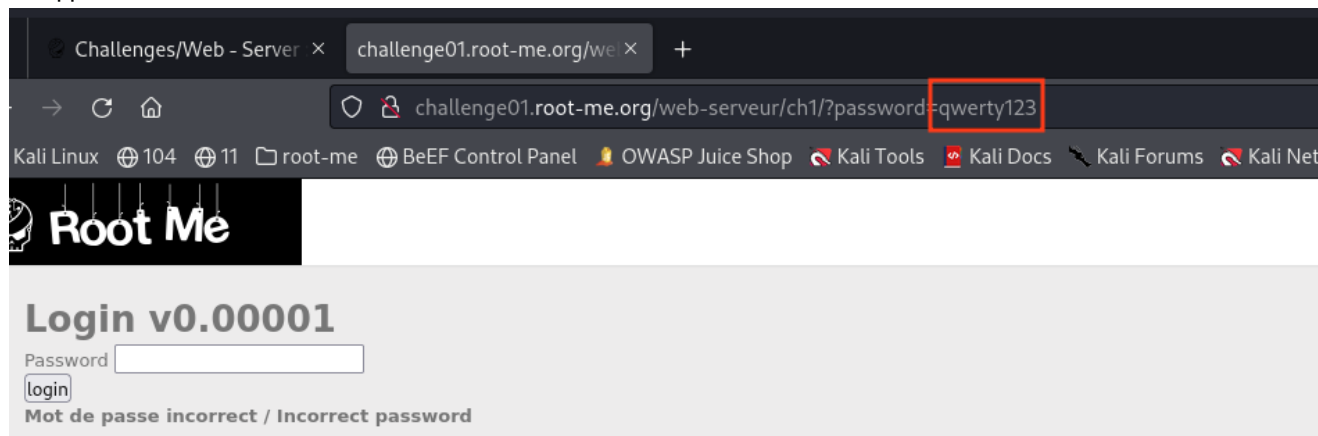
Механизмы аутентификации

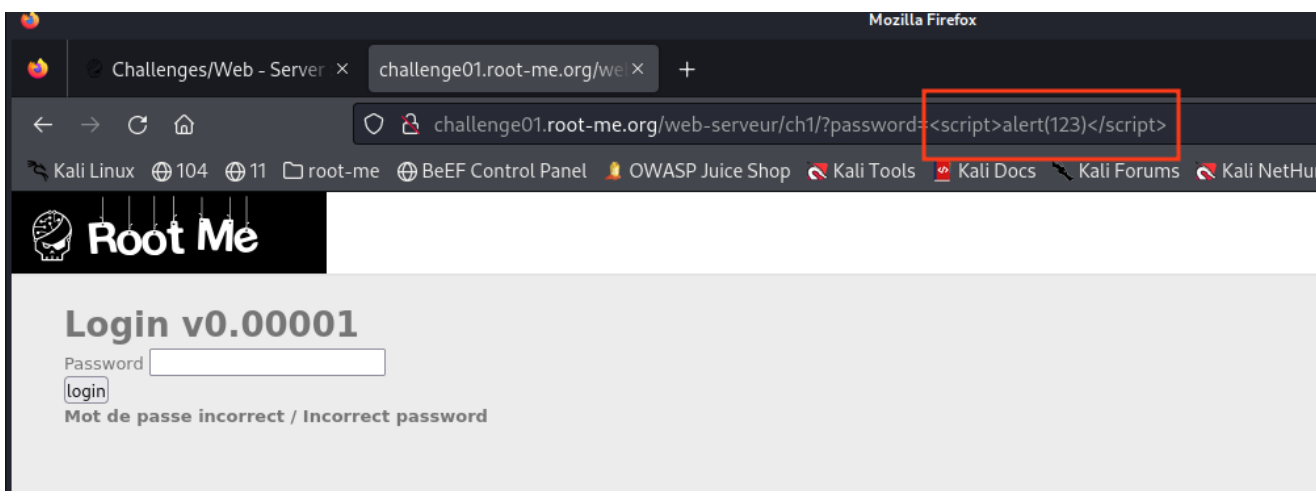
## Задание\_1:

Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/HTML>



Вводим любые числа и тэги:

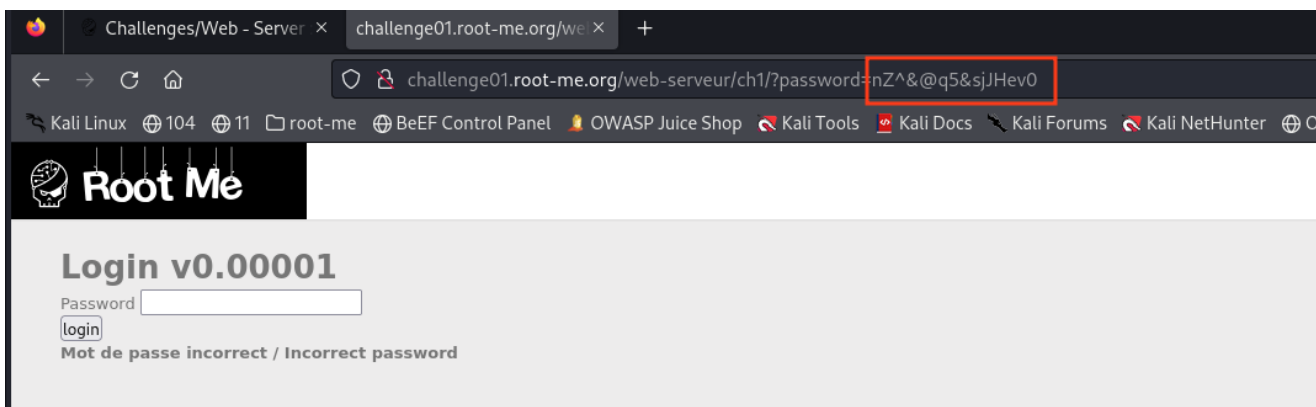




Смотрим исходный код:

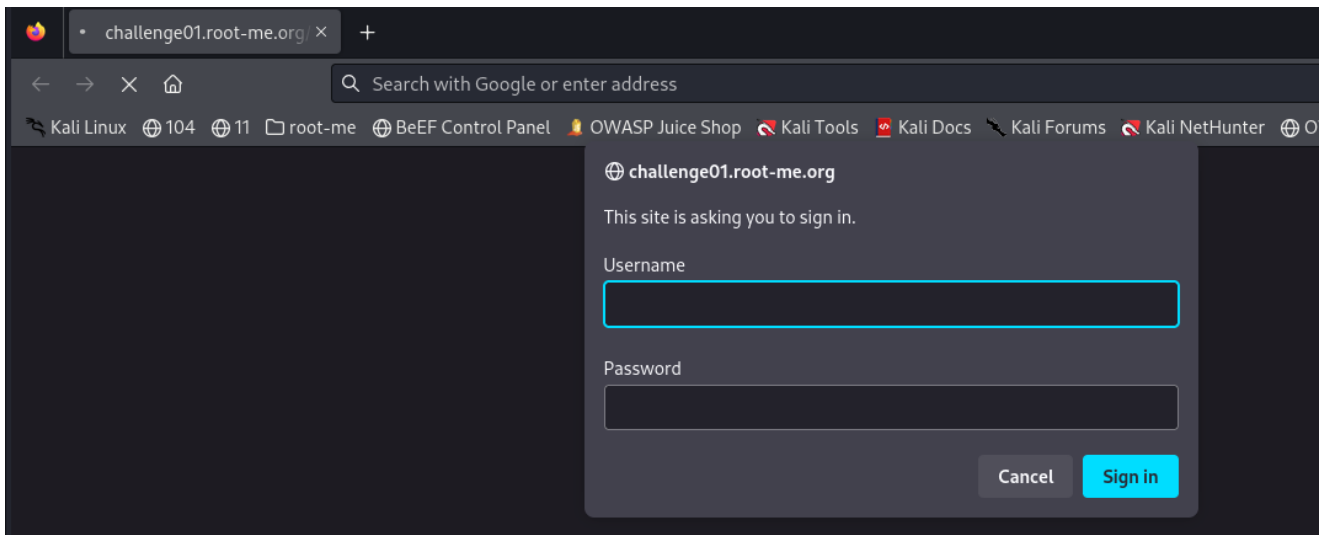
```
<!--  
Je crois que c'est vraiment trop simple là !  
It's really too easy !  
    password : nZ^&@q5&sjJHev0  
-->  
</body></html>
```

Видим пароль `nZ^&@q5&sjJHev0`



## Задание\_2:

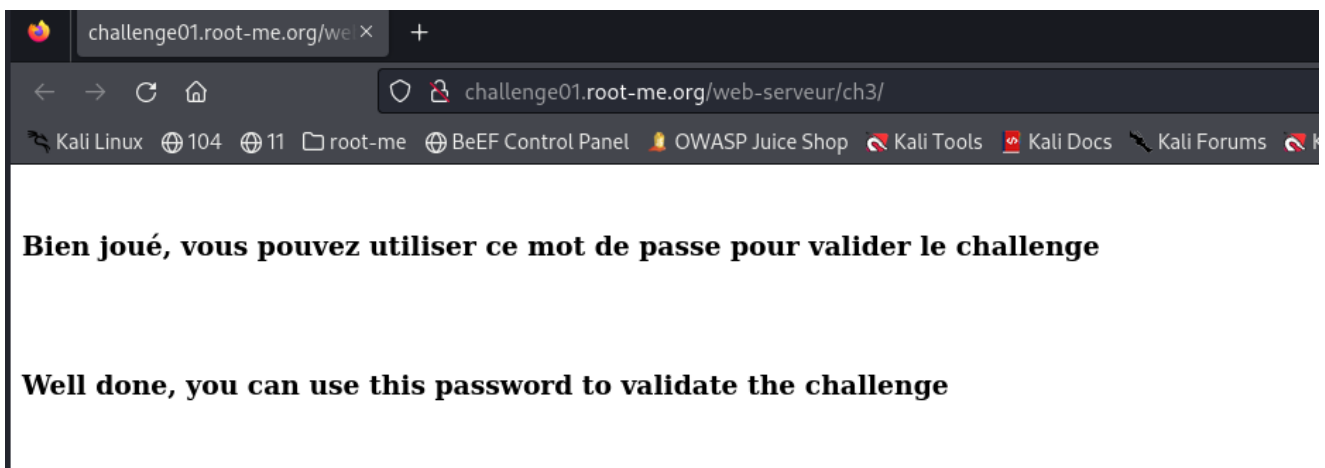
Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/Weak-password>



Пробуем несколько распространённых вариантов:

логин *admin*

пароль *admin* или *password* или *qwerty* или *qwerty123*

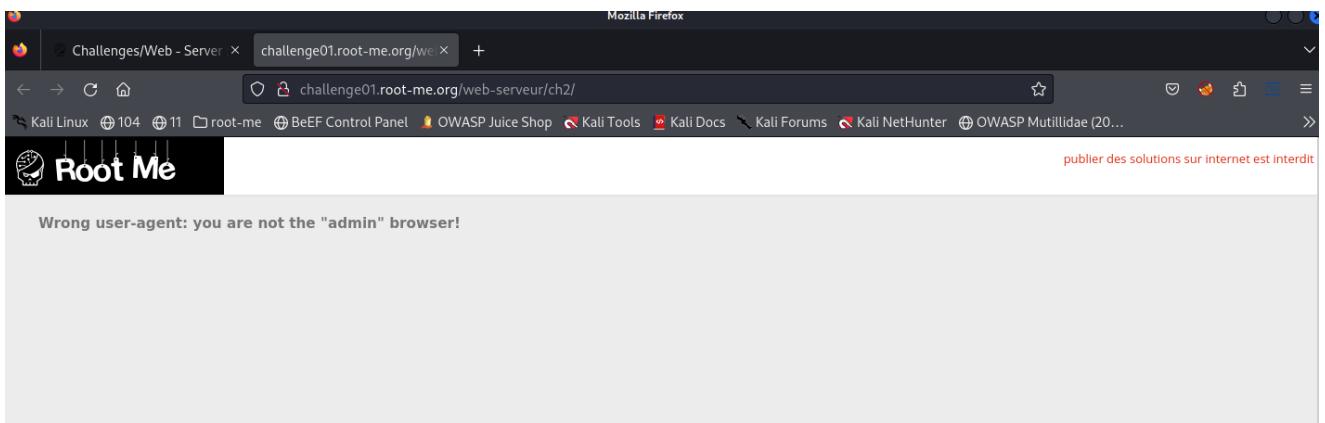


Пароль *admin*

Вывод: пароль не должен быть таким же как логин.

## Задание\_3:

Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/User-agent>

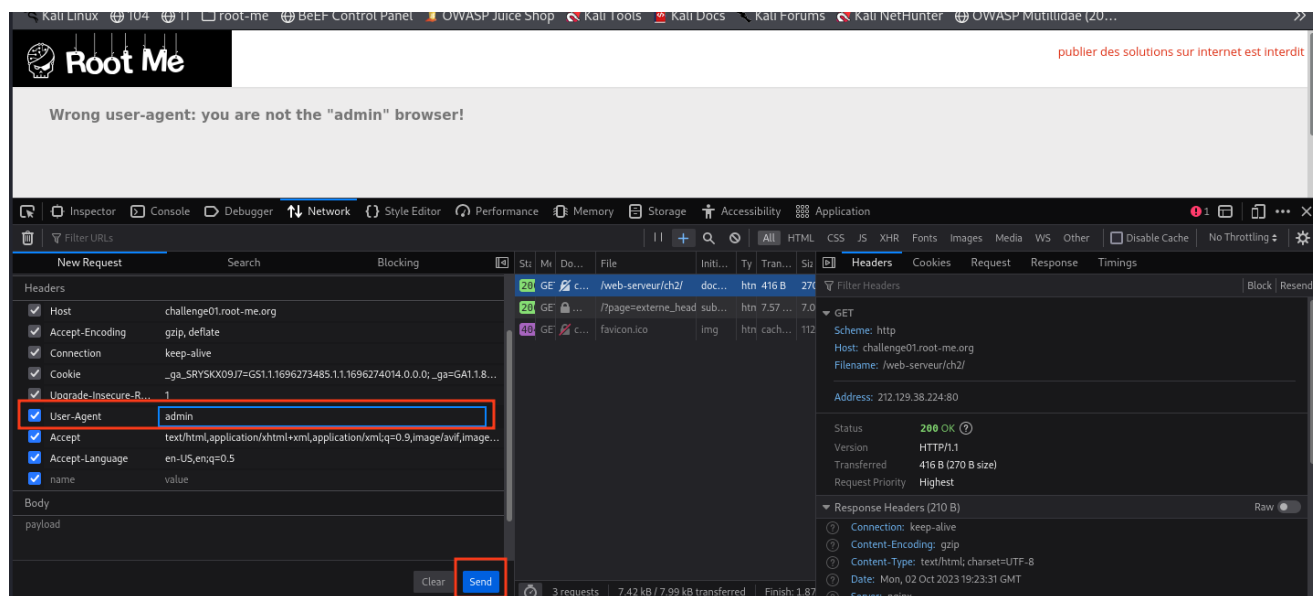
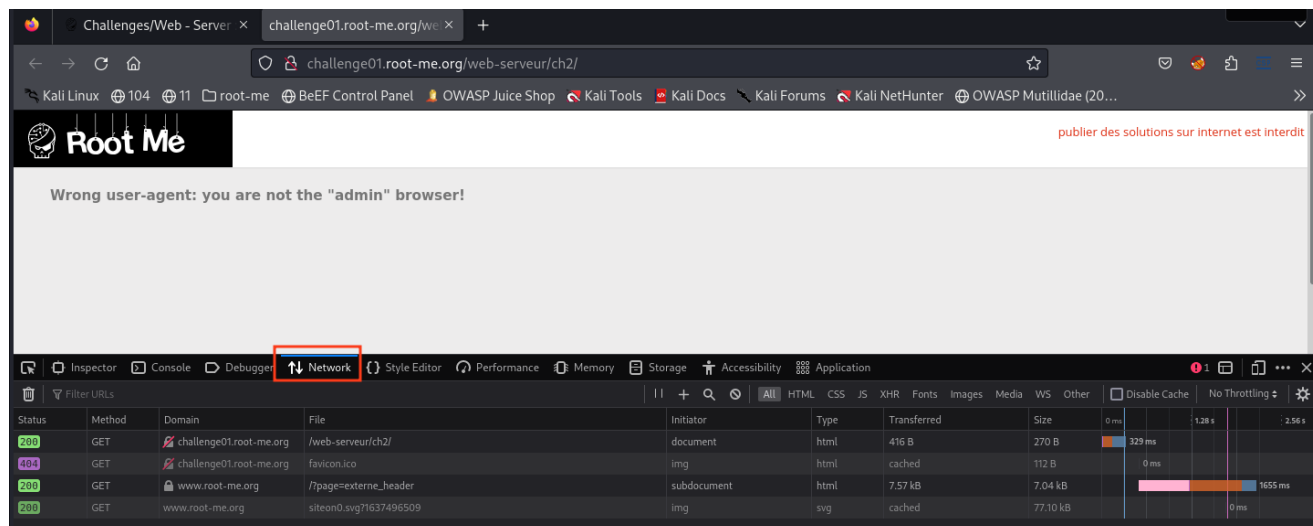


Ответ браузера: у нас не *admin* браузер

При посещении веб-сайта браузер обычно посылает веб-серверу информацию о себе. Это текстовая строка, являющаяся частью HTTP-запроса, начинающаяся с *User-agent* и обычно включающая такую информацию, как название и версию приложения, операционную систему компьютера и язык.

*User agent* — это полностью подконтрольный пользователю параметр.

В браузере запускаем инспектор, сеть, в поле *User agent* выставим значение *admin*.



Получаем ответ:

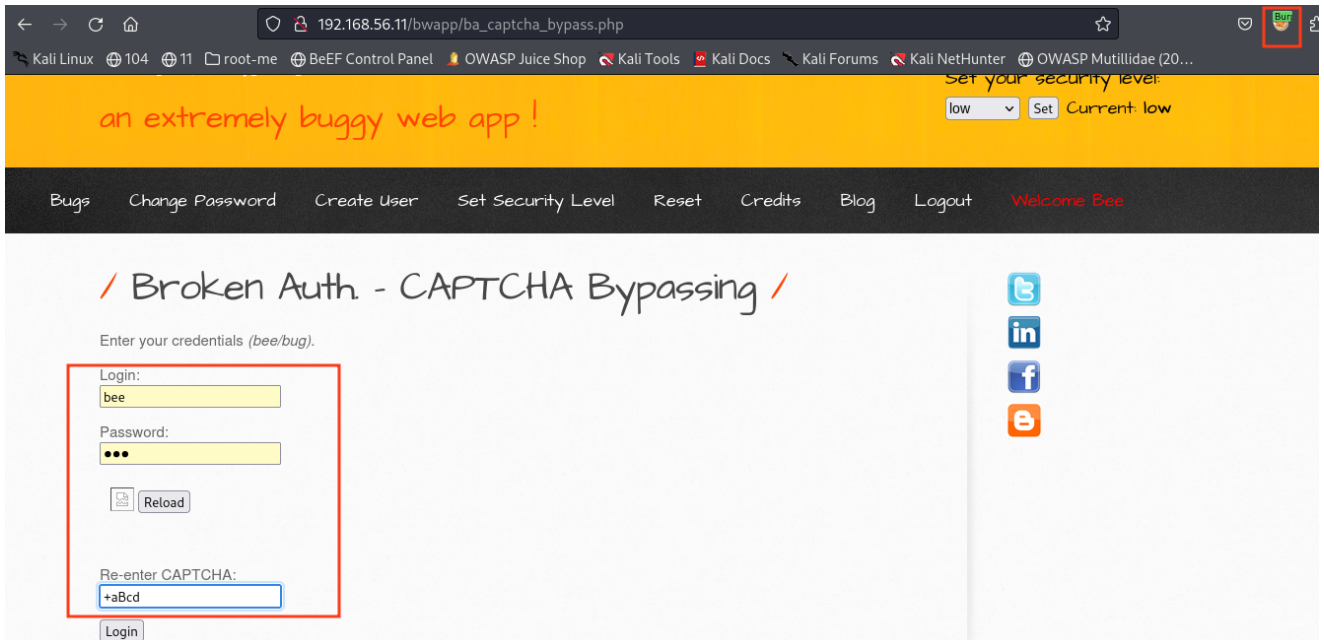
The screenshot shows a web browser window with the address bar displaying 'root-me'. The page content shows a message: 'Wrong user-agent: you are not the "admin" browser!'. Below this, a network inspector is open, showing a list of requests. The selected request is a GET request to '/web-seur/ch2/' with a status of 200. The response body is visible, showing a message: 'Welcome master! Password: rr\$Li9%L34qd1AAe27'. A Firefox error message is also visible: 'Firefox Can't Open This Page'.

Welcome master!  
Password: rr\$Li9%L34qd1AAe27

## Задание\_4:

(\*) Выполните задание CAPTCHA Bypassing из раздела Broken Authentication & Session Management в bWAPP.

The screenshot shows the bWAPP - Portal web application. The page has a yellow header with the text 'an extremely buggy web app!'. Below the header, there is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. The main content area has a title '/ Portal /' and a description of bWAPP. It mentions that bWAPP is a free and open source deliberately insecure web application, designed to help security enthusiasts, developers, and students discover and prevent web vulnerabilities. It covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project. It is for security-testing and educational purposes only. Below the description, there is a section titled 'Which bug do you want to hack today? :)' with a list of vulnerabilities. The selected vulnerability is 'Broken Authentication - CAPTCHA Bypassing'. Other vulnerabilities listed include XML/XPath Injection (Login Form), XML/XPath Injection (Search), Broken Authentication - Forgotten Function, Broken Authentication - Insecure Login Forms, Broken Authentication - Logout Management, and Broken Authentication - Password Attacks. There is a 'Hack' button at the bottom of the list. On the right side of the page, there are social media icons for Twitter, LinkedIn, Facebook, and Email. At the bottom right, there is a logo for the National Center for Missing & Exploited Children.

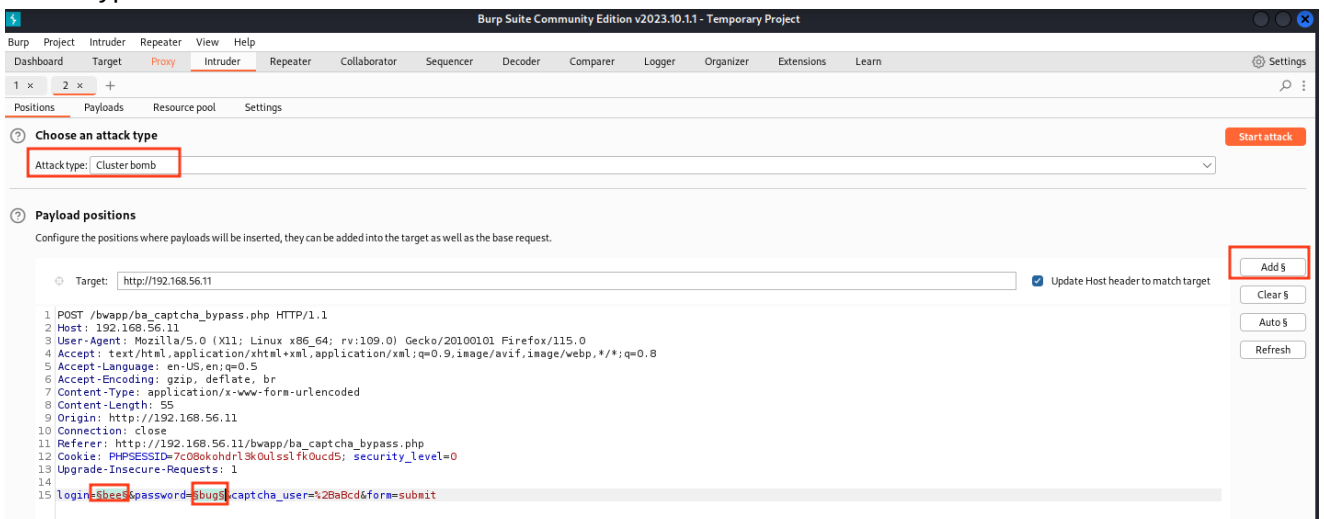


## Burp Suite:



## Send to Intruder:

### Attack type *Cluster bomb*



## Составим словари в *Payloads*

1 x 2 x +

Dashboard Target **Proxy** Intruder Repeater Collaborator

Positions Payloads Resource pool Settings

### ? Payload sets

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

Payload set: 1 Payload count: 6

Payload type: Simple list Request count: 0

---

### ? Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

bee

admin

password

pa\$\$word

test

bug

Add

1 x 2 x +

Dashboard Target **Proxy** Intruder Repeater Collaborator Se

Positions Payloads Resource pool Settings

### ? Payload sets

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

Payload set: 2 Payload count: 6

Payload type: Simple list Request count: 36

---

### ? Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

bee

bug

test

password

pa\$\$word

admin

Add

Add from list ... [Pro version only]





## 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