02.10.2023

Курс:

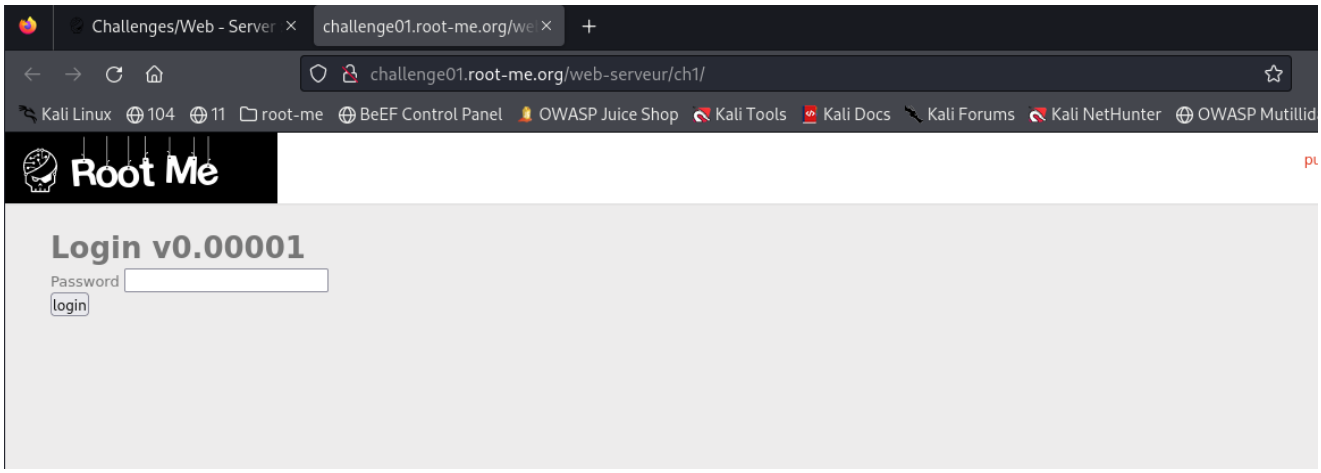
Практическая работа к уроку № Lesson_5

--

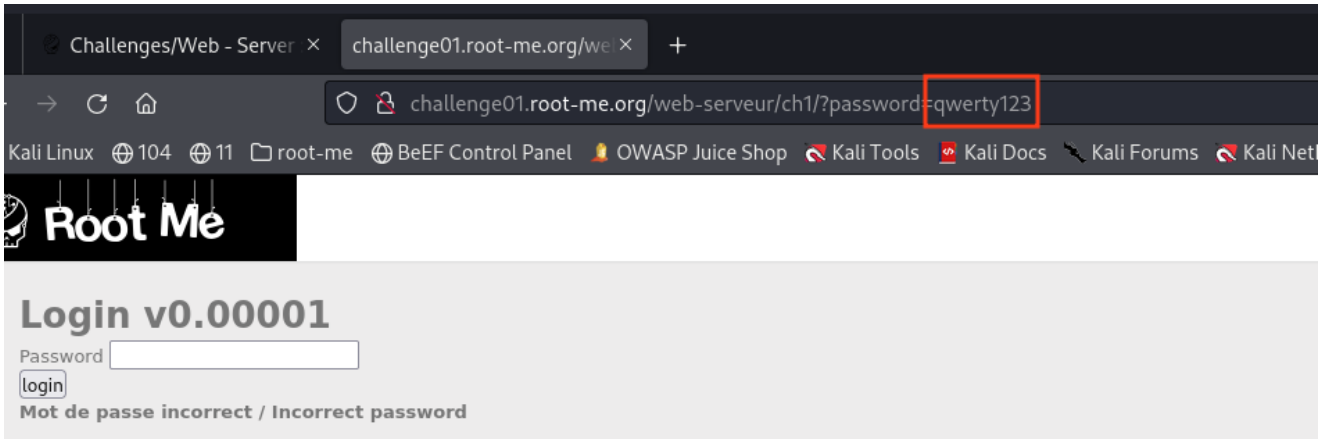
Механизмы аутентификации

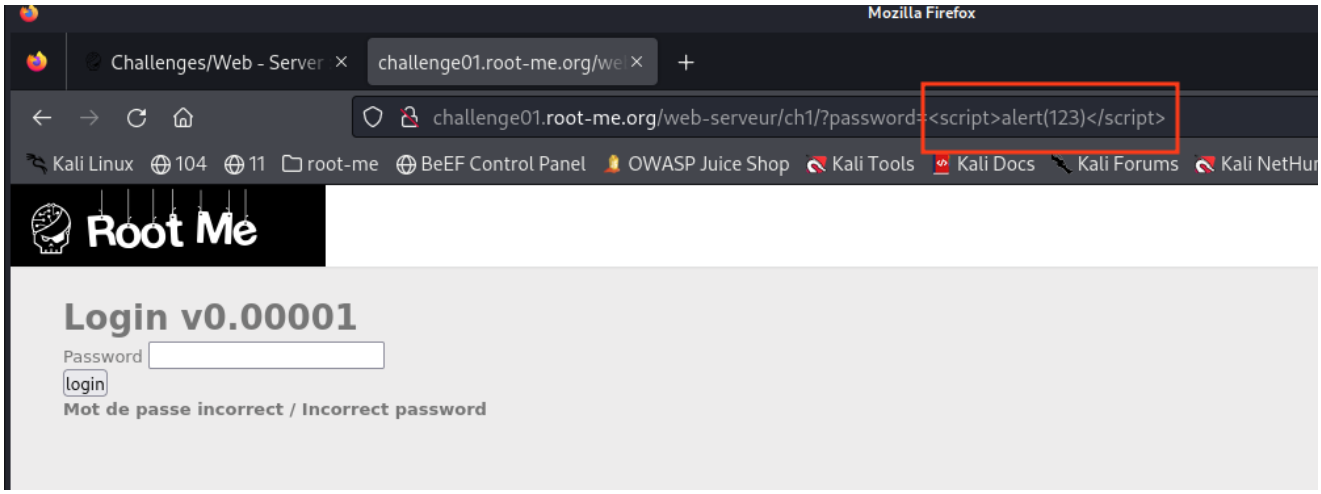
Задание_1:

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



Вводим любые числа и тэги:

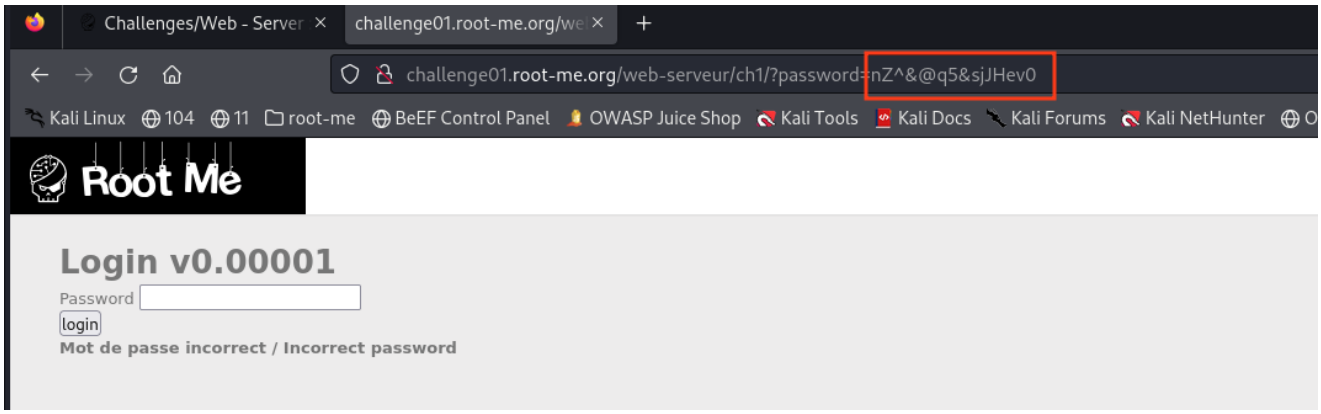




Смотрим исходный код:

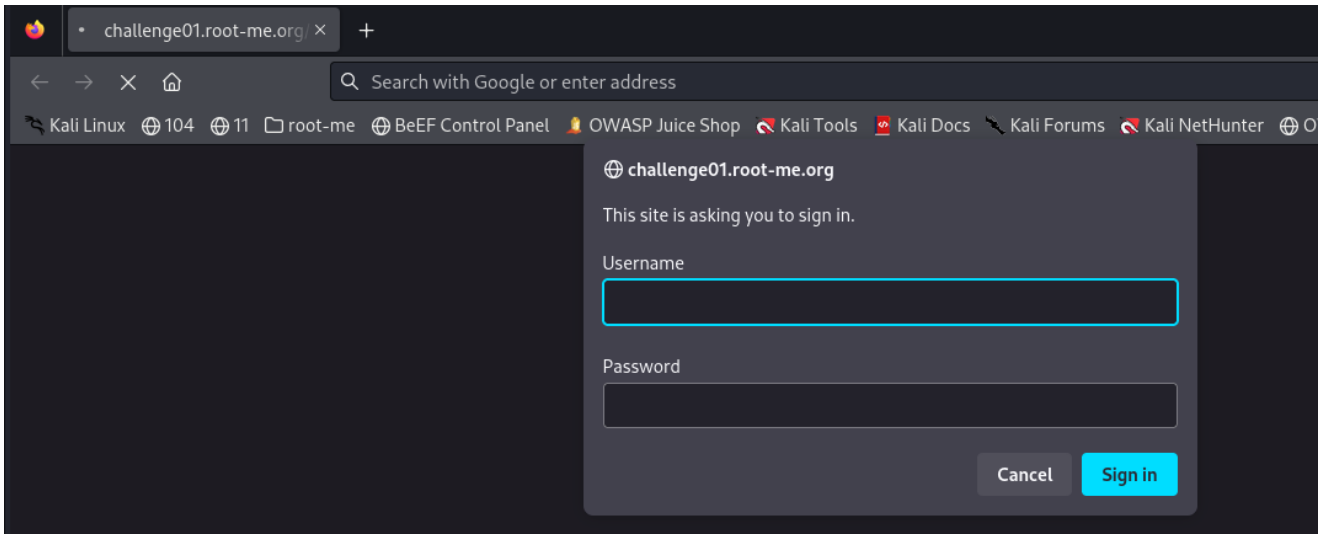
```
<!--
Je crois que c'est vraiment trop simple là !
It's really too easy !
     password : nZ^&@q5&sjJHev0
-->
</body></html>
```

Видим пароль *nZ^&@q5&sjJHev0*

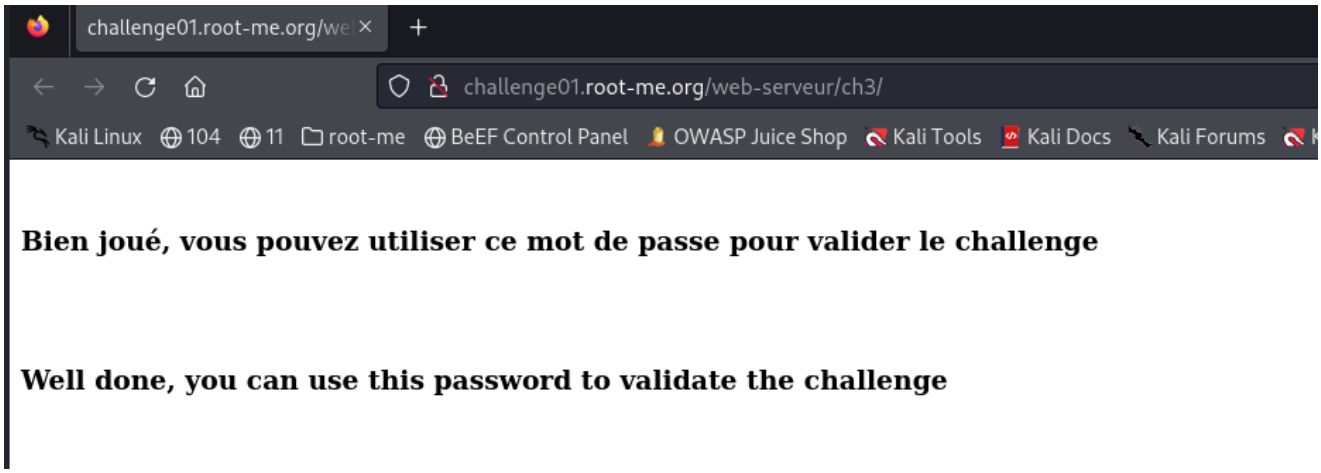


Задание_2:

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*

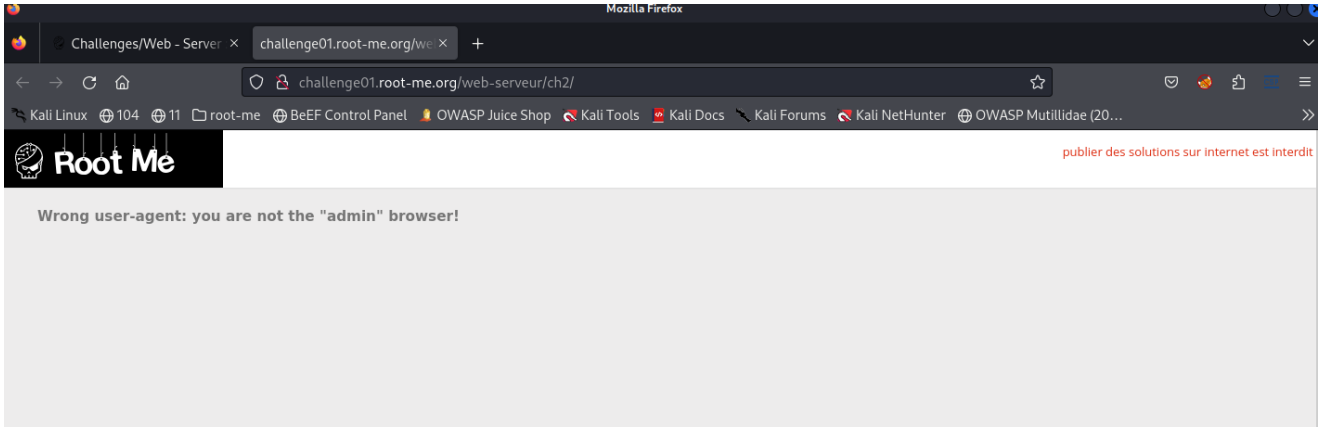


Пароль *admin*

Вывод: пароль не должен быть таким же как логин.

Задание_3:

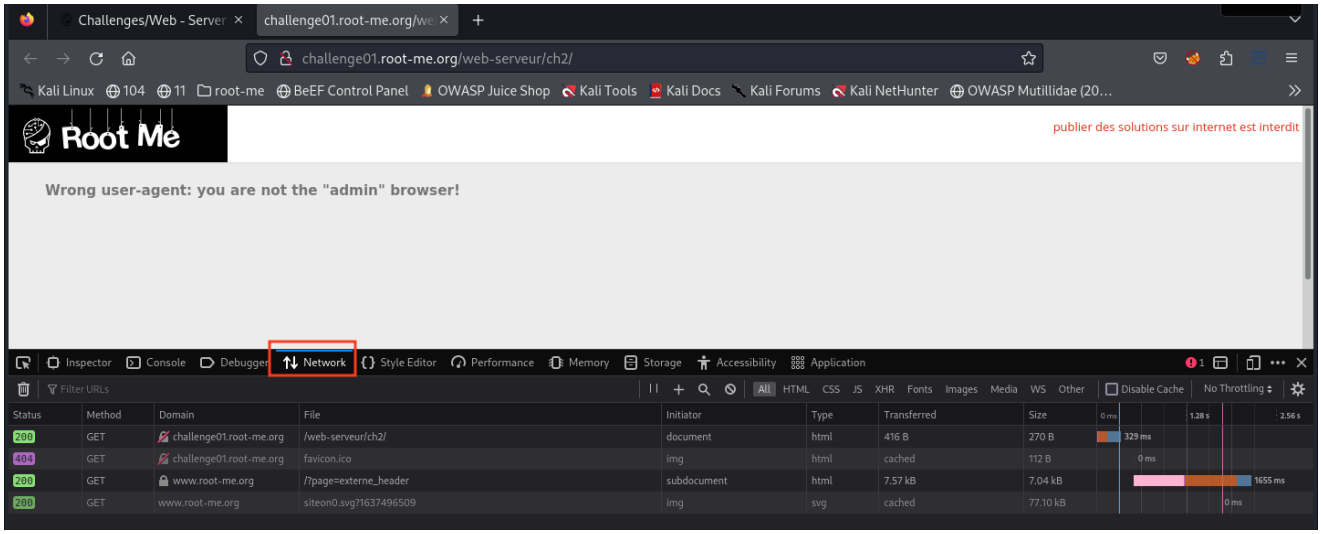
Выполните задание https://www.root-me.org/en/Challenges/Web-Server/User-agent

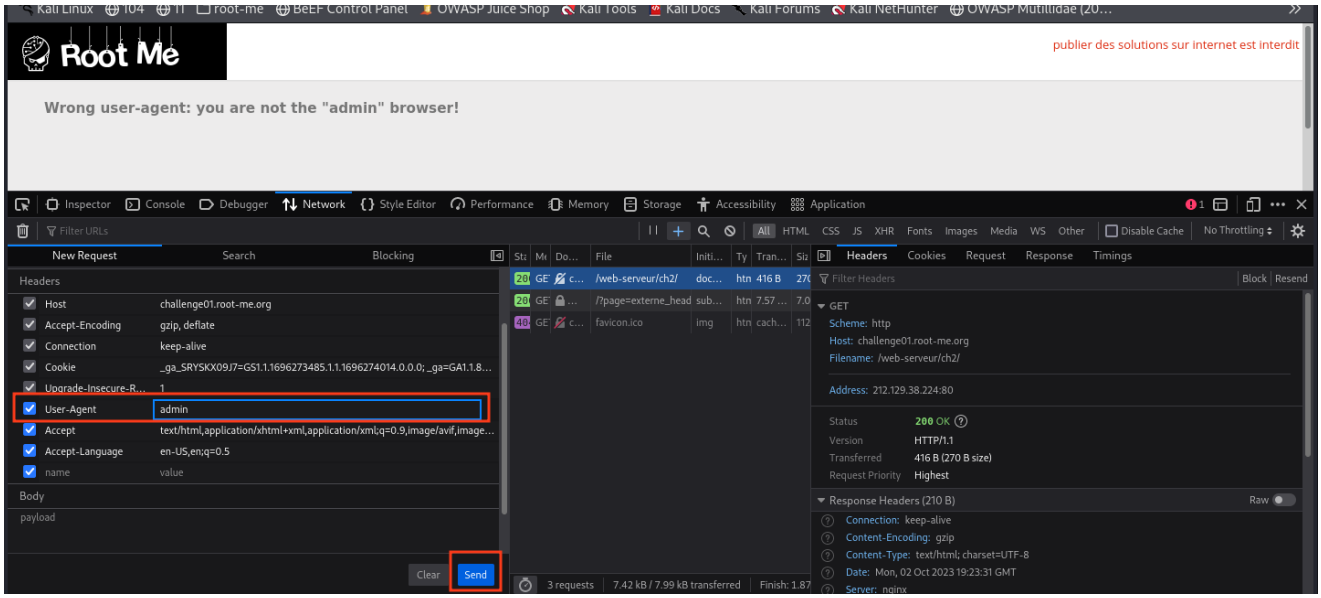


Ответ браузера: у нас не *admin* браузер

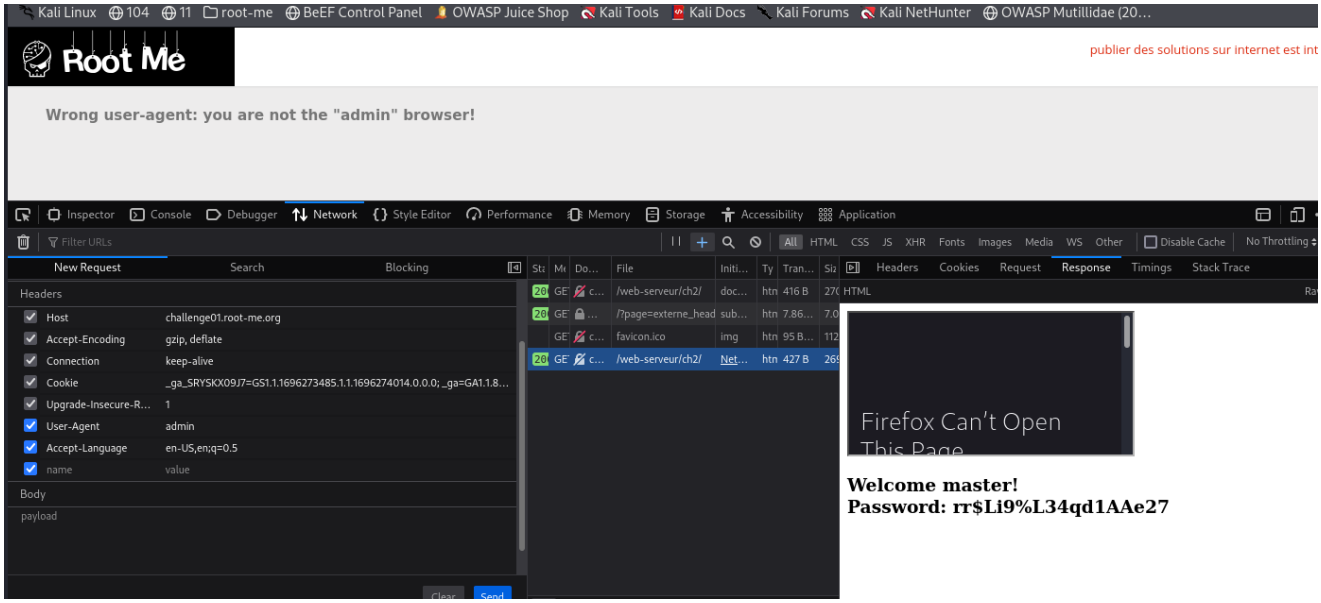
При посещении веб-сайта браузер обычно посылает веб-серверу информацию о себе. Это текстовая строка, являющаяся частью HTTP-запроса, начинающаяся с User-agent и обычно включающая такую информацию, как название и версию приложения, операционную систему компьютера и язык.
User agent — это полностью подконтрольный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

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





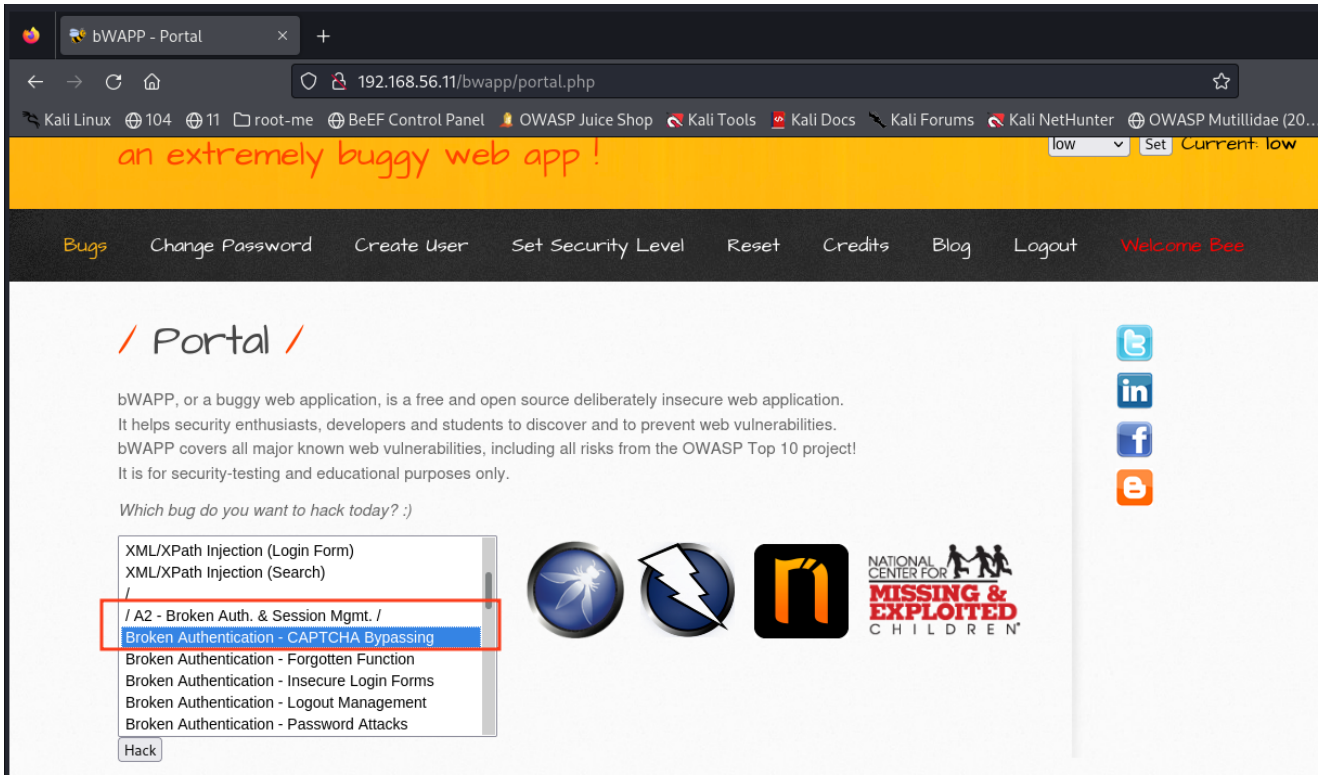
Получаем ответ:

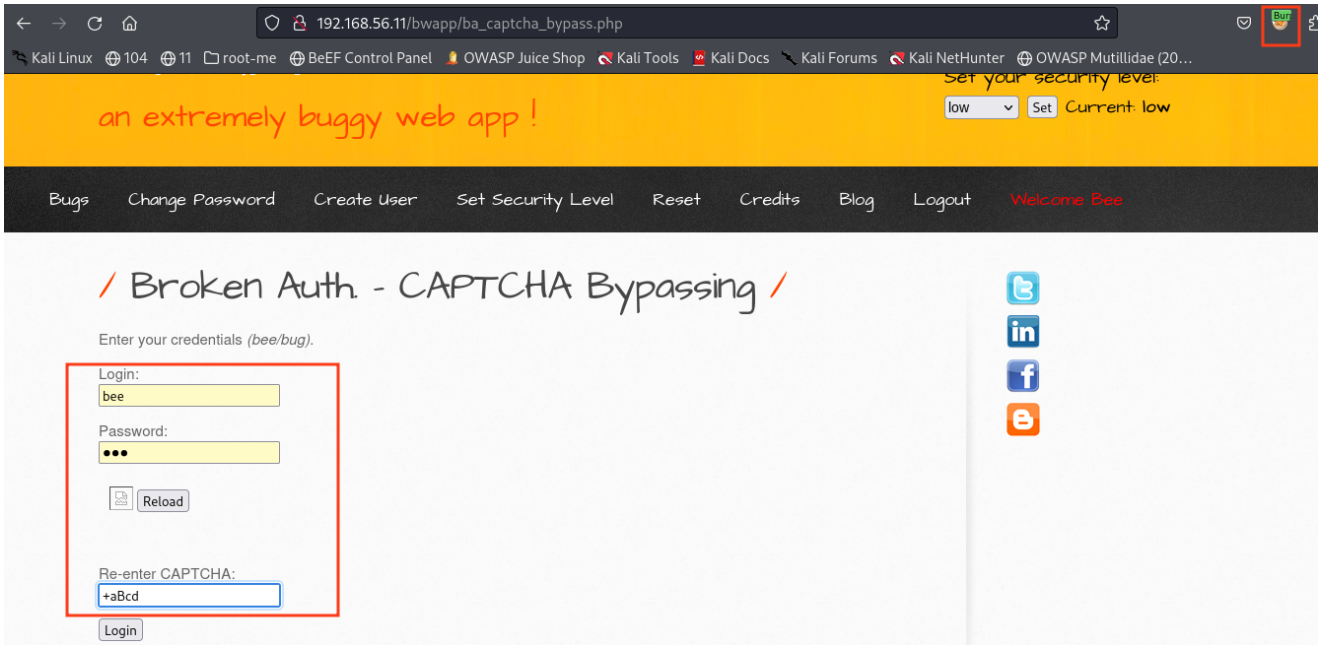



```
Welcome master!
Password: rr$Li9%L34qd1AAe27
```

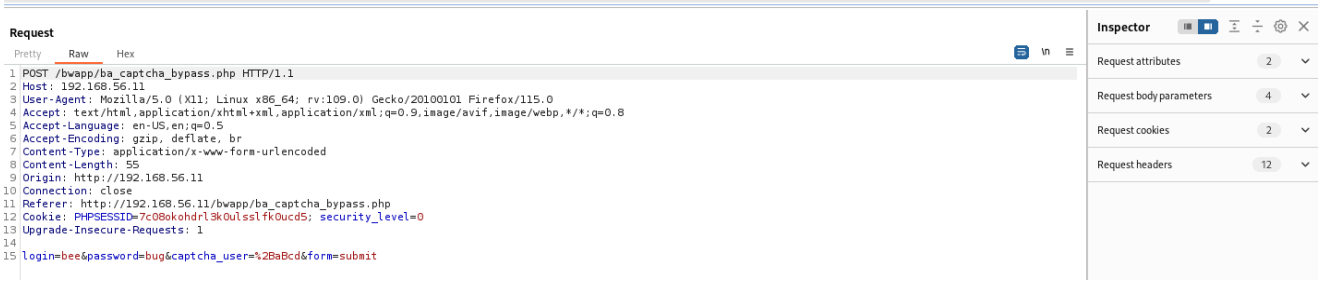
Задание_4:

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



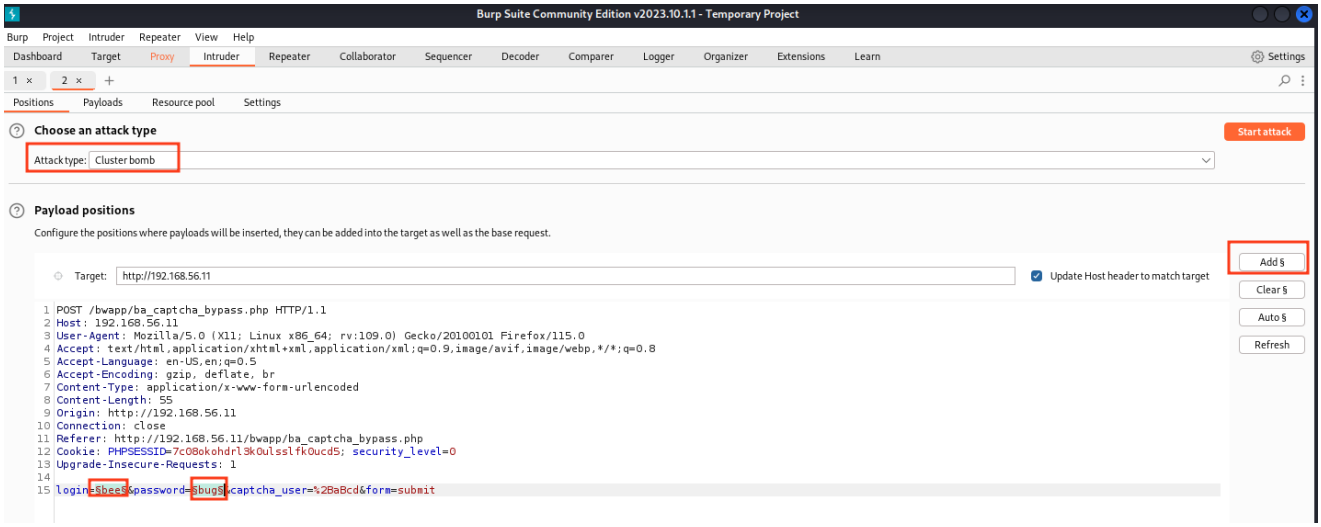


Burp Suite:

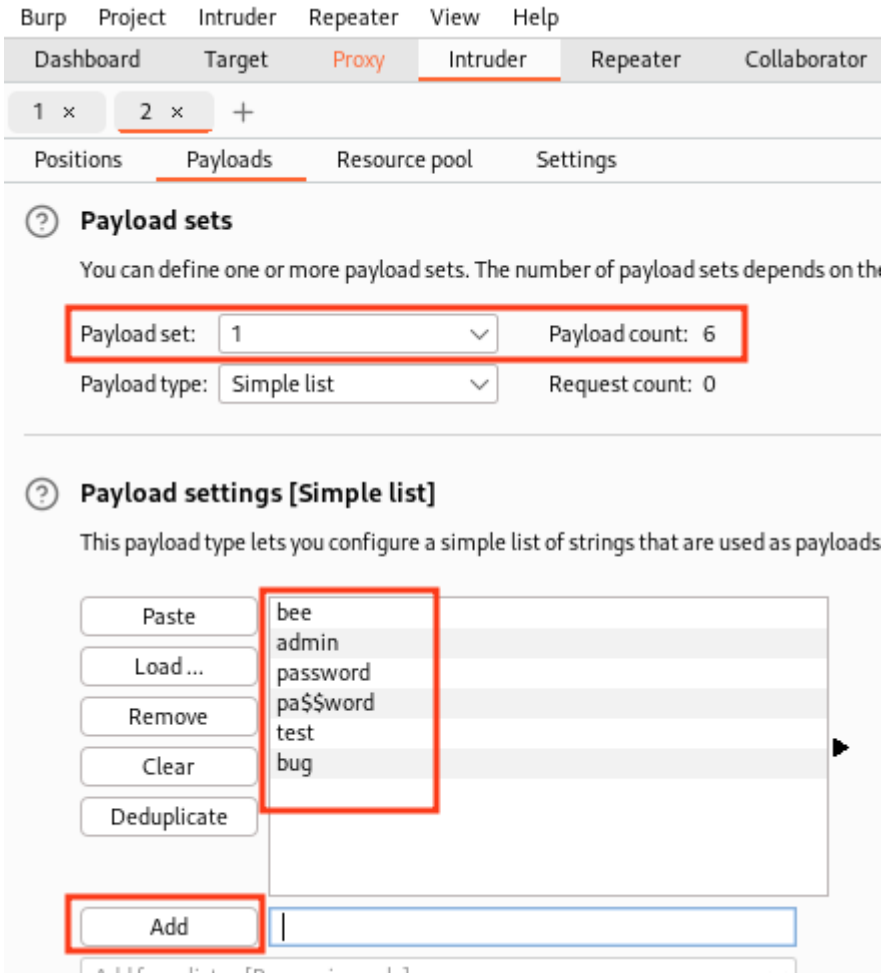


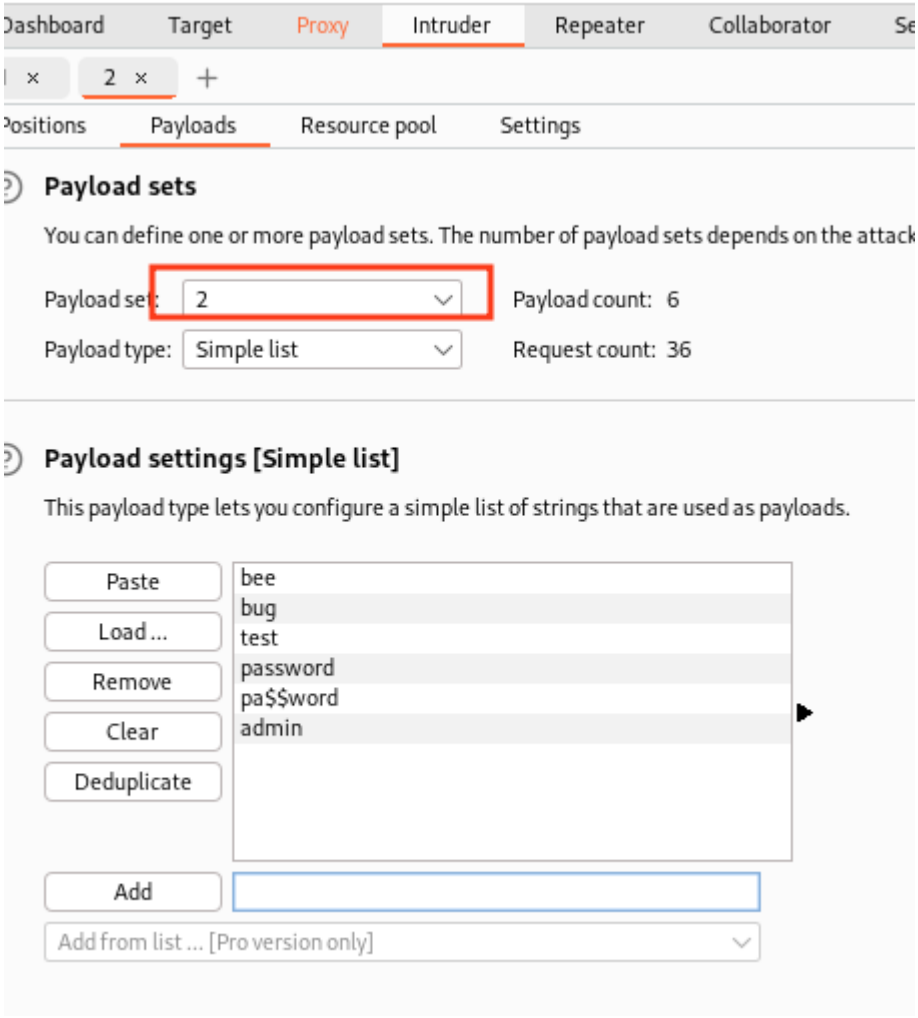
Send to Intruder:

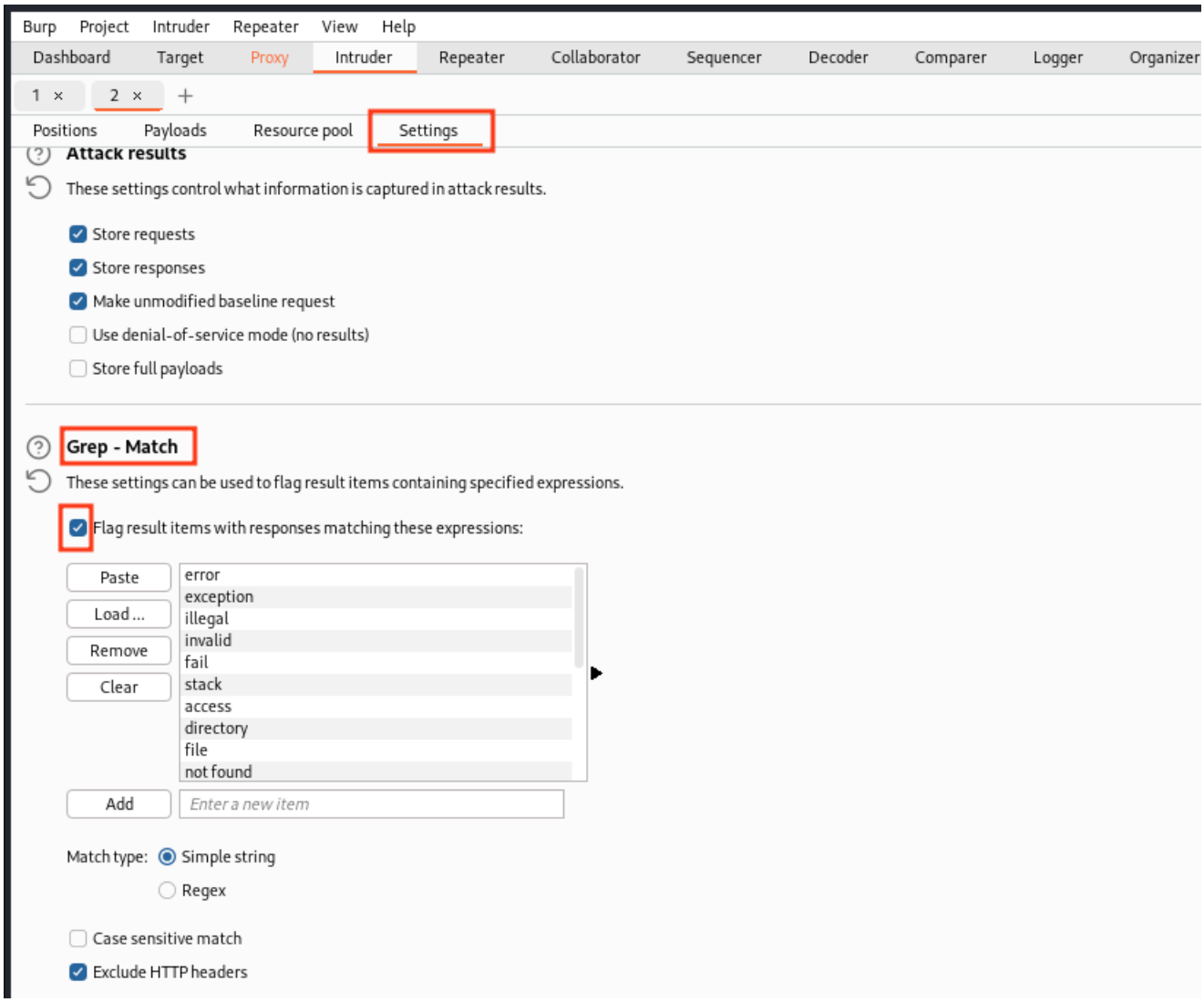
Attack type *Cluster bomb*

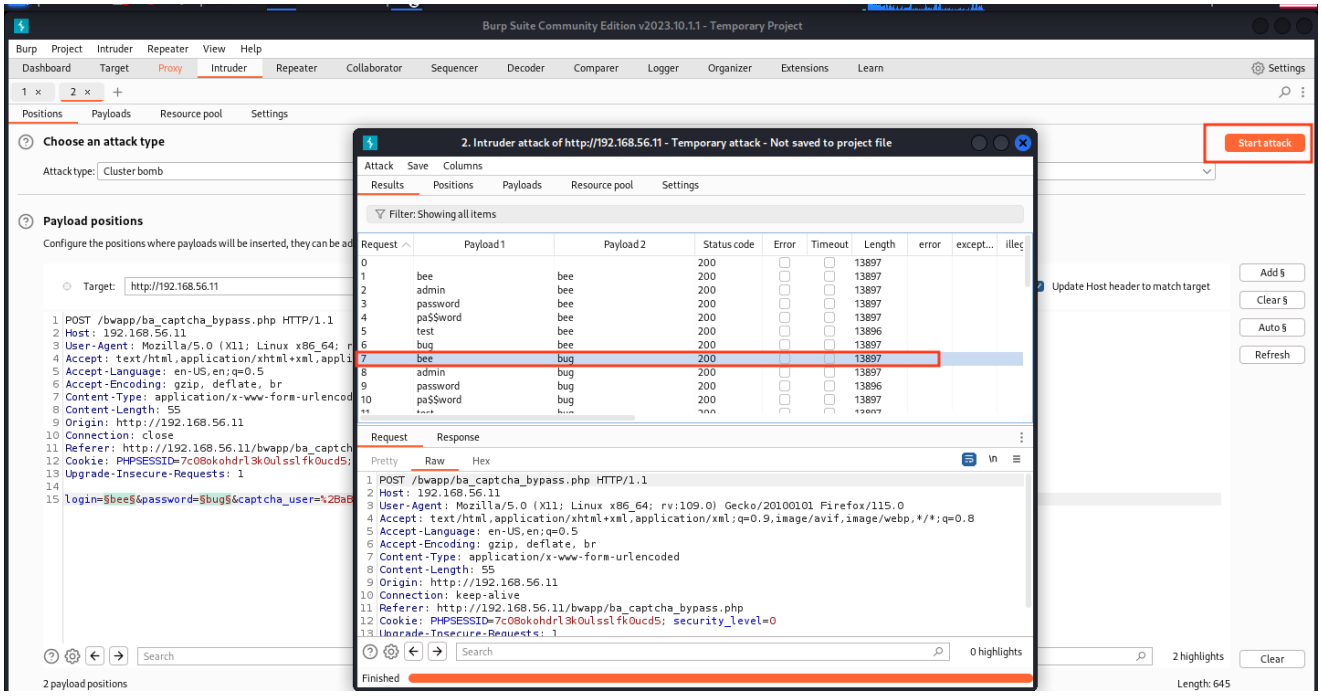


Составим словари в *Payloads*






Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
1 × 2 ×
Positions Payloads Resource pool Settings
Attack results
These settings control what information is captured in attack results.
Store requests
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
error
exception
illegal
invalid
fail
stack
access
directory
file
not found
Add
Enter a new item
Match type:
Simple string
Regex
Case sensitive match
Exclude HTTP headers


Burp Suite Community Edition v2023.10.1.1 - Temporary Project
2. Intruder attack of http://192.168.56.11 - Temporary attack - Not saved to project file
Start attack
Choose an attack type
Payload positions
Request
Response
Finished


Re-enter CAPTCHA:
Login
Successful login!

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