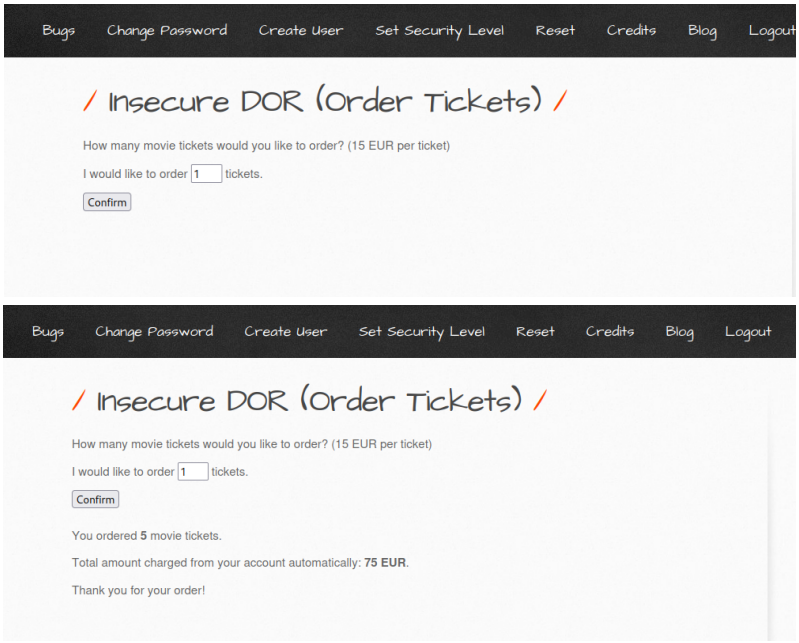
Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

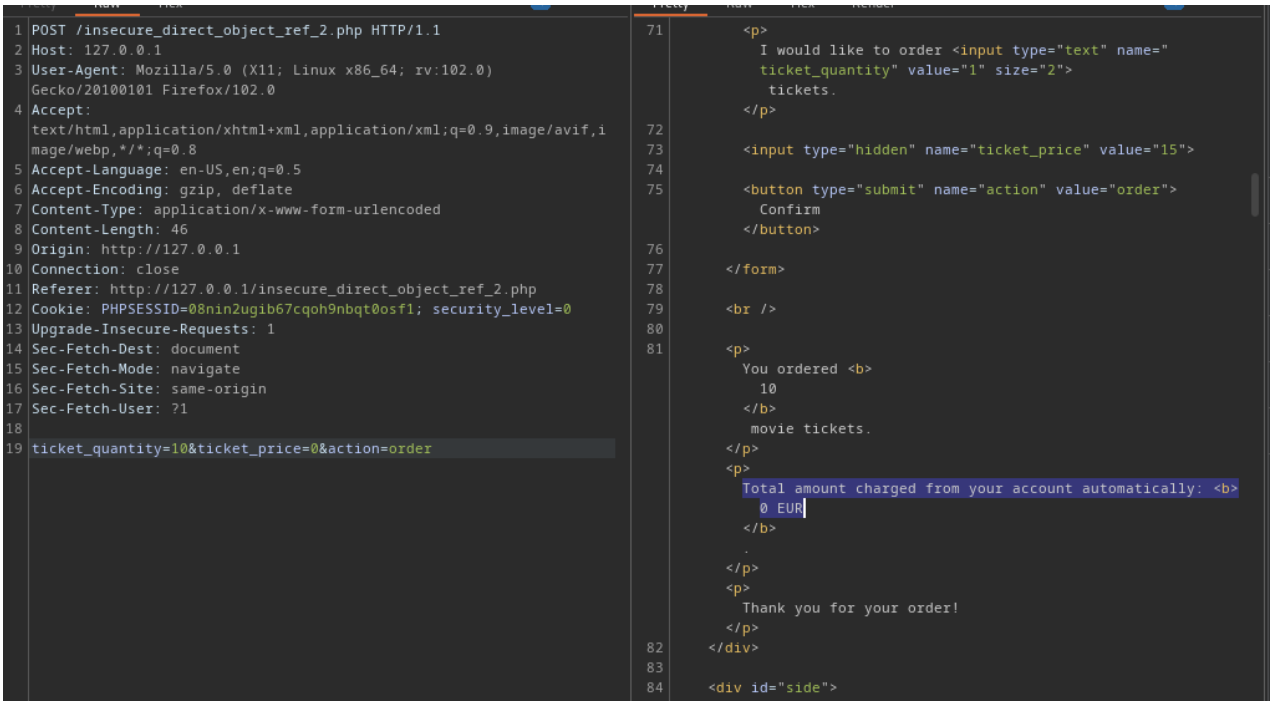
Задание 1: Выполнить задание Insecure DOR (Order Tickets) в bWAPP.

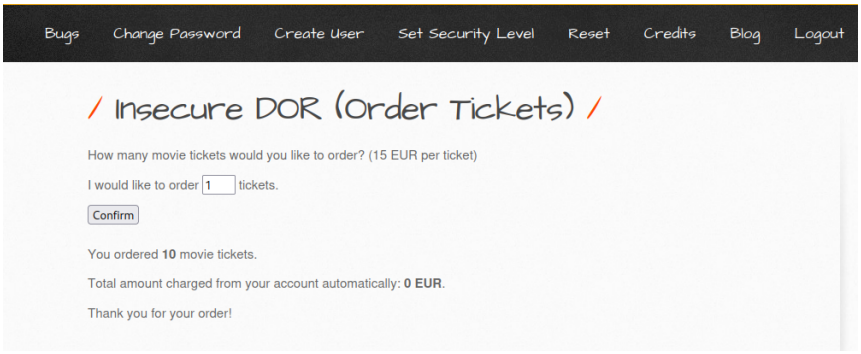
На данном ресурсе существует возможность заказа билетов с автоматическим списанием средств со счёта за покупку.

Изначально попробую "заказать" несколько билетов.



Видно, что за 5 билетов списывается сумма в "75эвра". Рассмотрю перехваченные запросы в BurpSuite. В данной "лабораторной машине" есть не безопасная отправка запроса. Меняю её на "более интересную", и для закрепления результата смотрю через "ответ в браузере".





В результате получаю 10 билетов с автоматическим списанием средств равным "0эвра". Считаю, что на данном этапе "лабораторная машина" выполнена.

Задание 2: Выполнить задание https://www.root-me.org/en/Challenges/Web-Server/CRLF

На данном ресурсе снова представлена форма аутентификации. Из описания задания известно, что данный ресурс связан с уязвимостью CRLF. Далее необходим поиск для раскручивания данной уязвимости.

https://owasp.org/www-community/vulnerabilities/CRLF_Injection

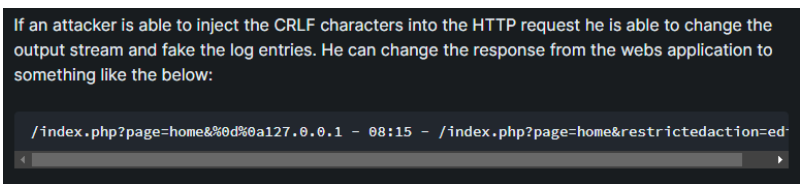
Description

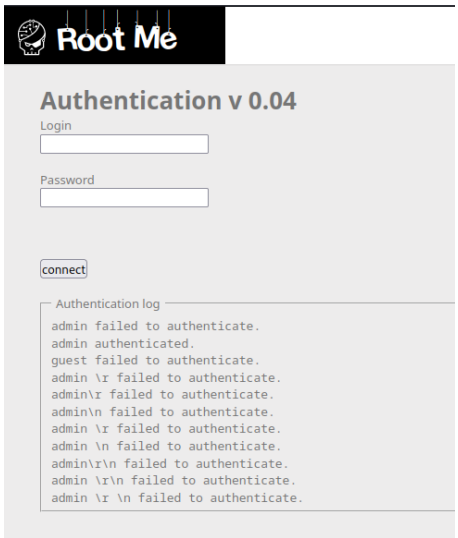
The term CRLF refers to **C**arriage **R**eturn (ASCII 13, \r) **L**ine **F**eed (ASCII 10, \n). They're used to note the termination of a line, however, dealt with differently in today's popular Operating Systems. For example: in Windows both a CR and LF are required to note the end of a line, whereas in Linux/UNIX a LF is only required. In the HTTP protocol, the CR-LF sequence is always used to terminate a line.

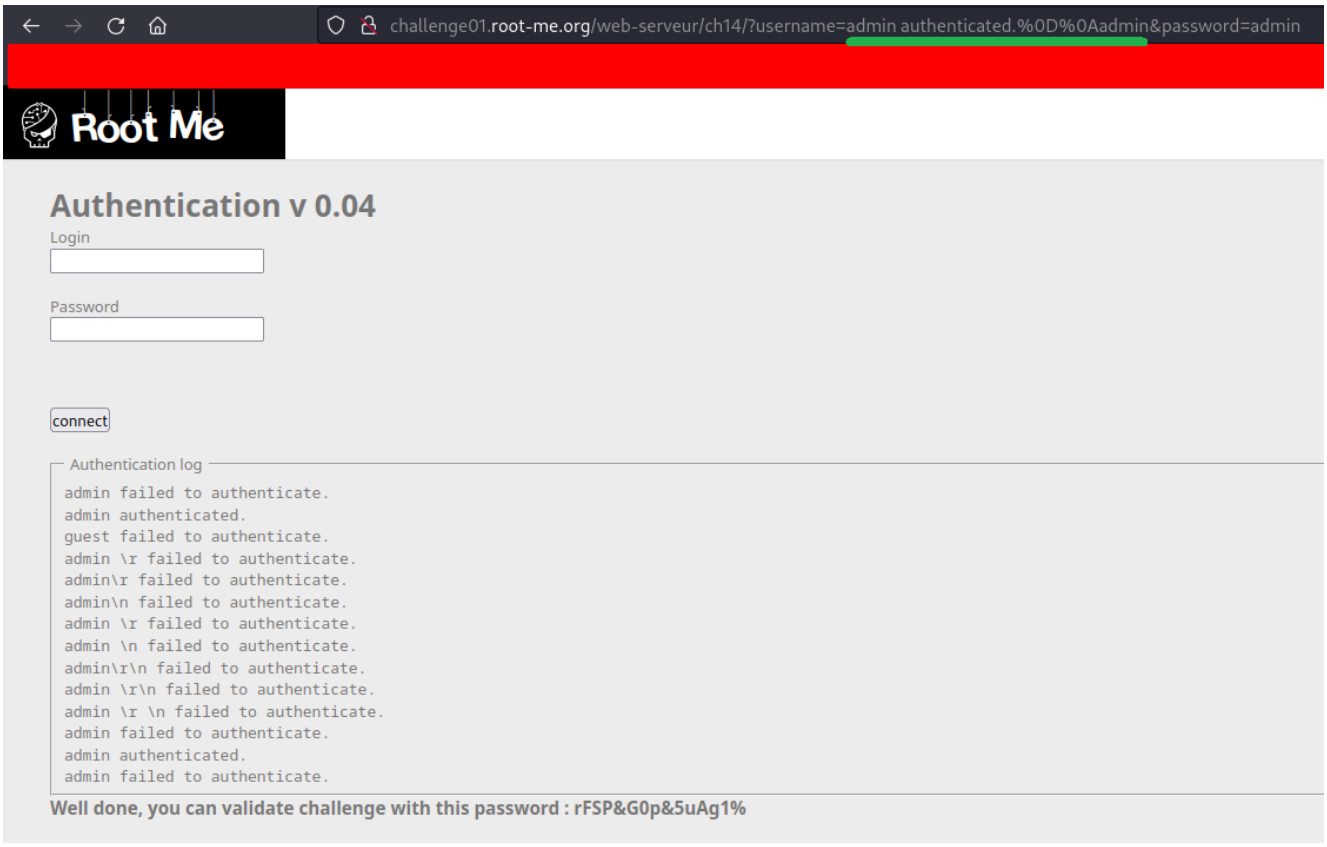
Использование подобных нагрузок при вводе пары для аутентификации - не дало результатов. Продолжив поиски обнаружилась информация

https://book.hacktricks.xyz/pentesting-web/crlf-0d-0a

где уже более интересное объяснение нагрузок и их применение.







Используя полученную информацию снова пытаюсь авторизироваться через пару admin:admin. После чего подставляя в нагрузку authenticated.%0D%0A обрамляя логин admin получается авторизироваться под данной парой. Получаю необходимый пароль для сдачи лабораторной машины.