02.10.2023

Курс:

Практическая работа к уроку № Lesson_6

--
IDOR и CRLF

Задание_1:

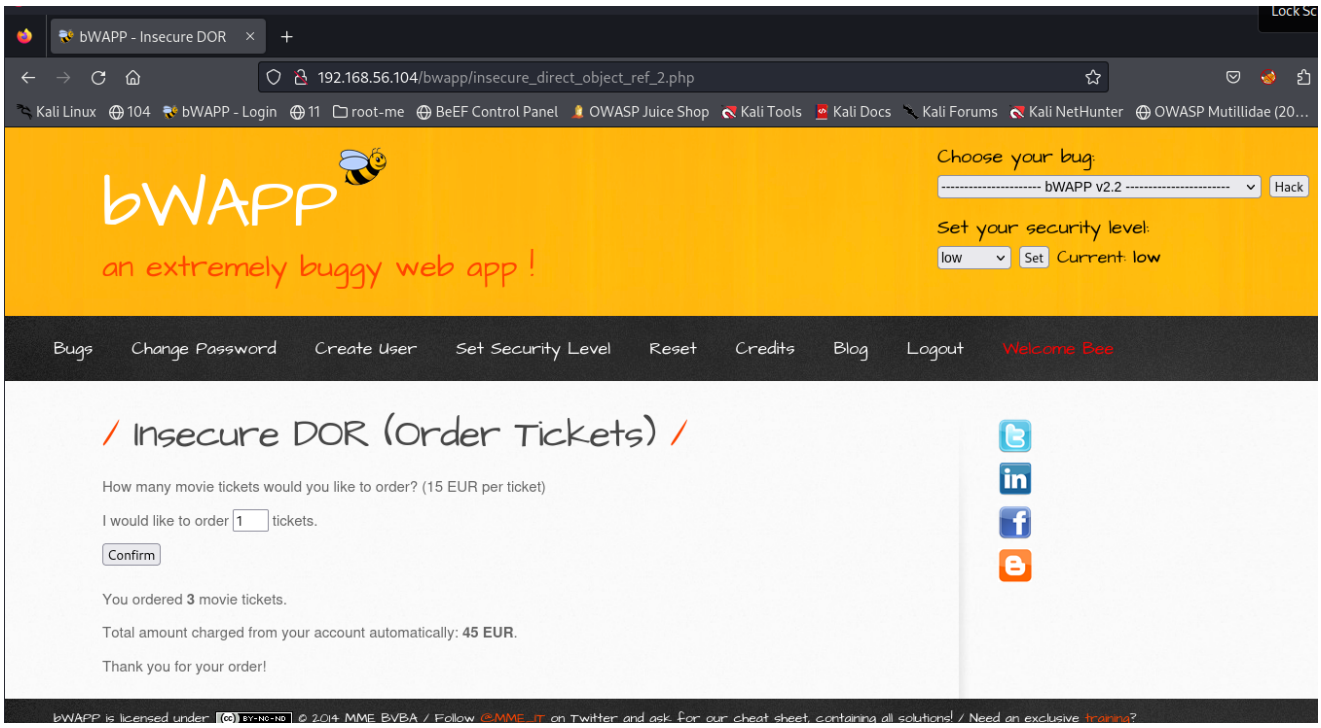
Выполнить задание Insecure DOR (Order Tickets) в bWAPP.

IDOR — это акроним от Insecure Direct Object Reference, «небезопасное прямое обращение к объекту». Мы через пользовательский интерфейс, с Client Side, напрямую меняем значение какой-либо переменной на Server Side или в базе данных.
IDOR может встретиться в любом месте, где для выполнения действия не проверяется авторизация и ID берётся из пользовательского ввода без проверки.

1. Чтение произвольных сообщений, просмотр чужих файлов. Если файлы запрашиваются по ID и этот ID предсказуемый, его можно поменять под своим аккаунтом на ID другого аккаунта.
2. Сброс пароля произвольного пользователя и угон его аккаунта.
3. Изменение стоимости товара.
4. …

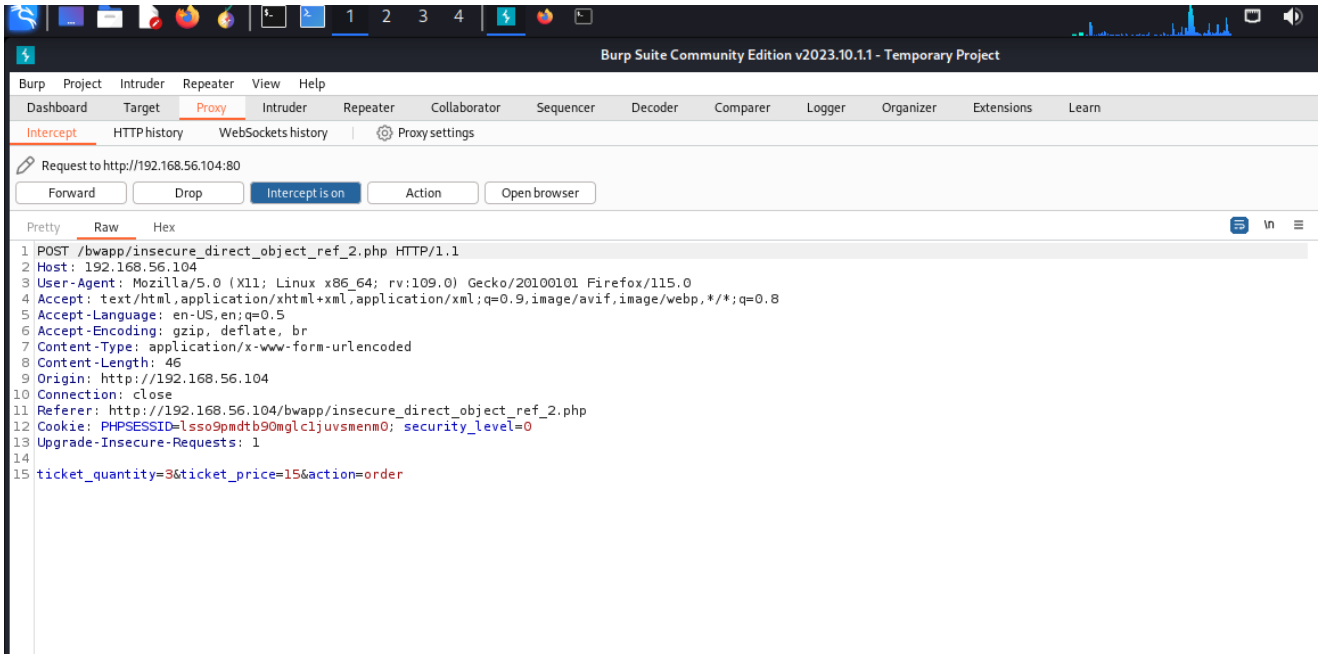
Сбрасываем bWapp *Reset*

Выбираем:

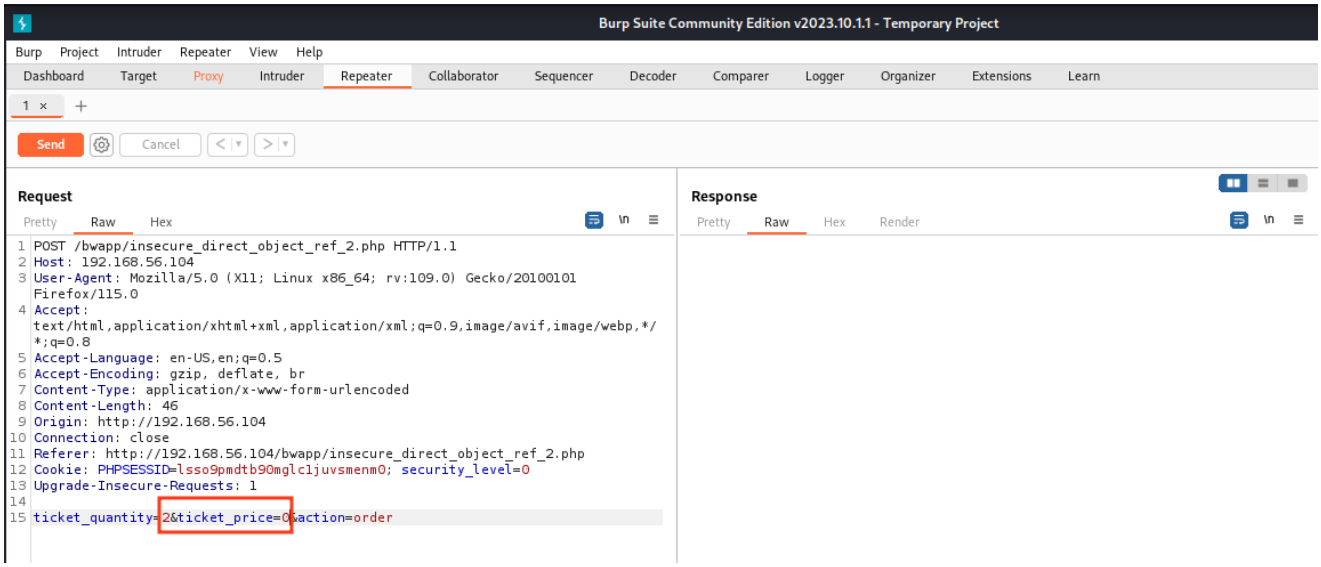


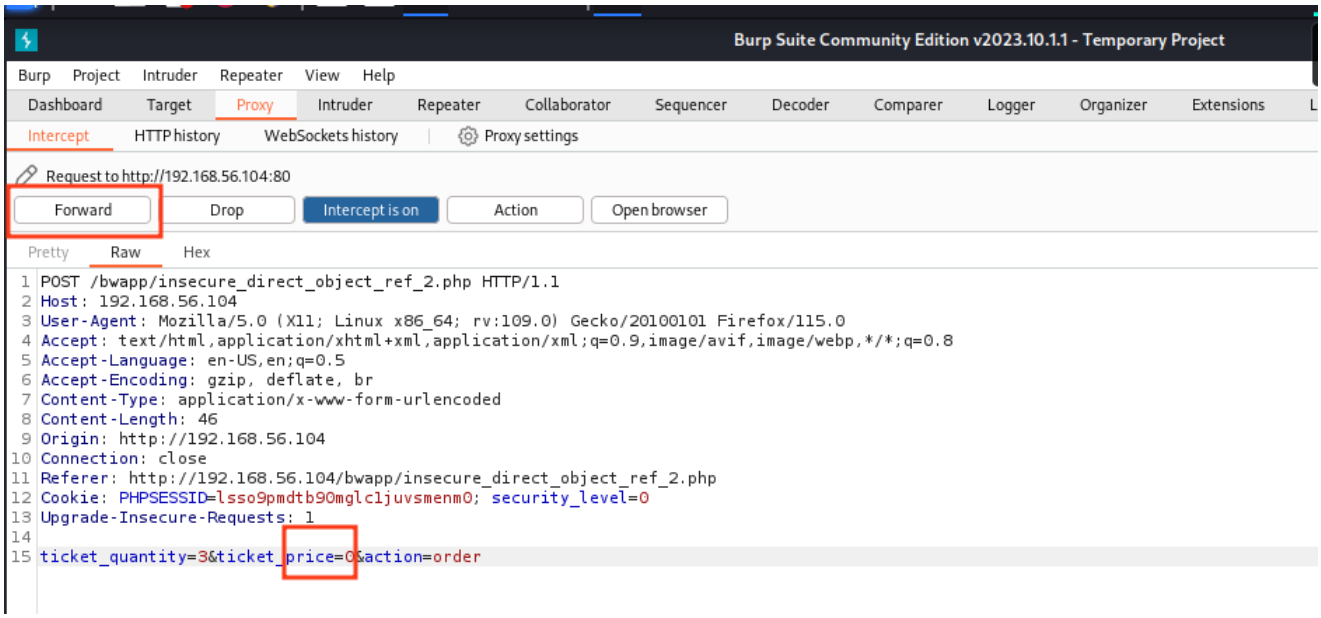
Burp Suite:

3 Ticket

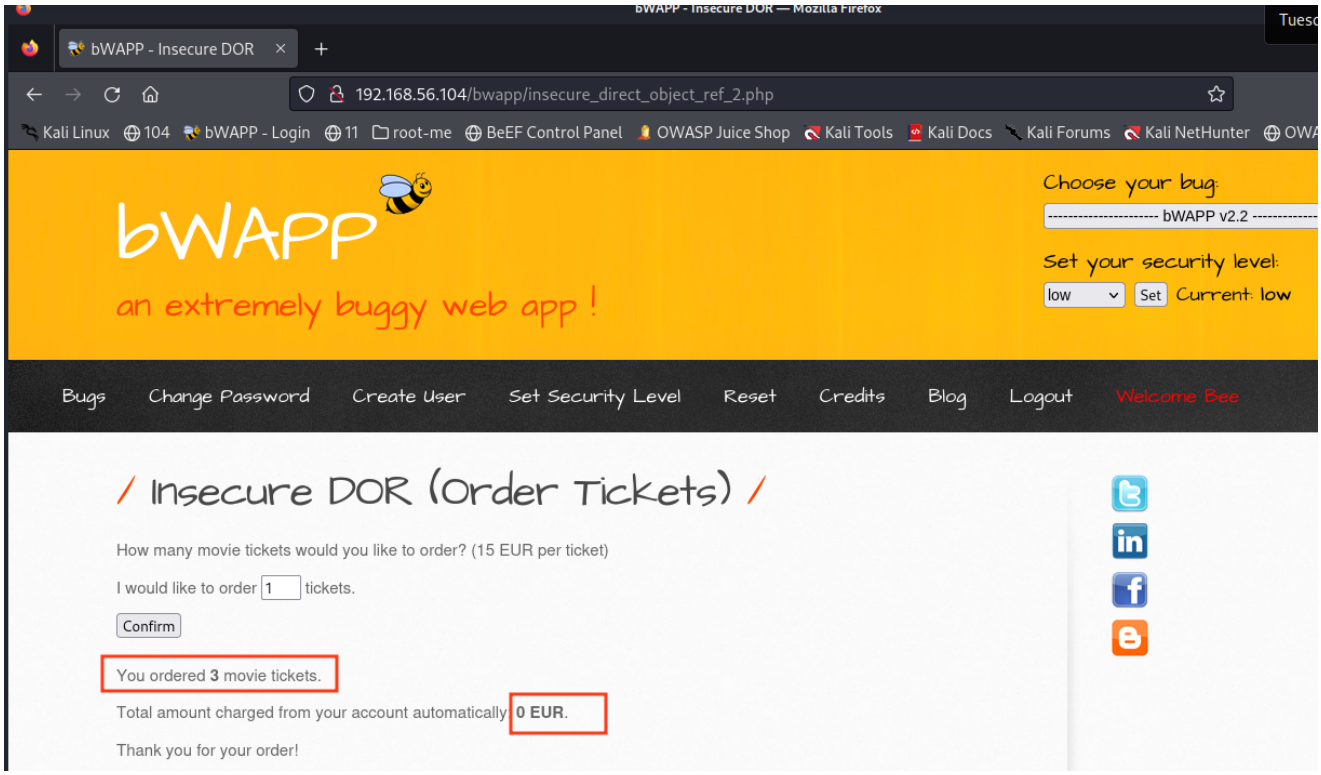


3 Tickets for *0* EUR (change to *0*)





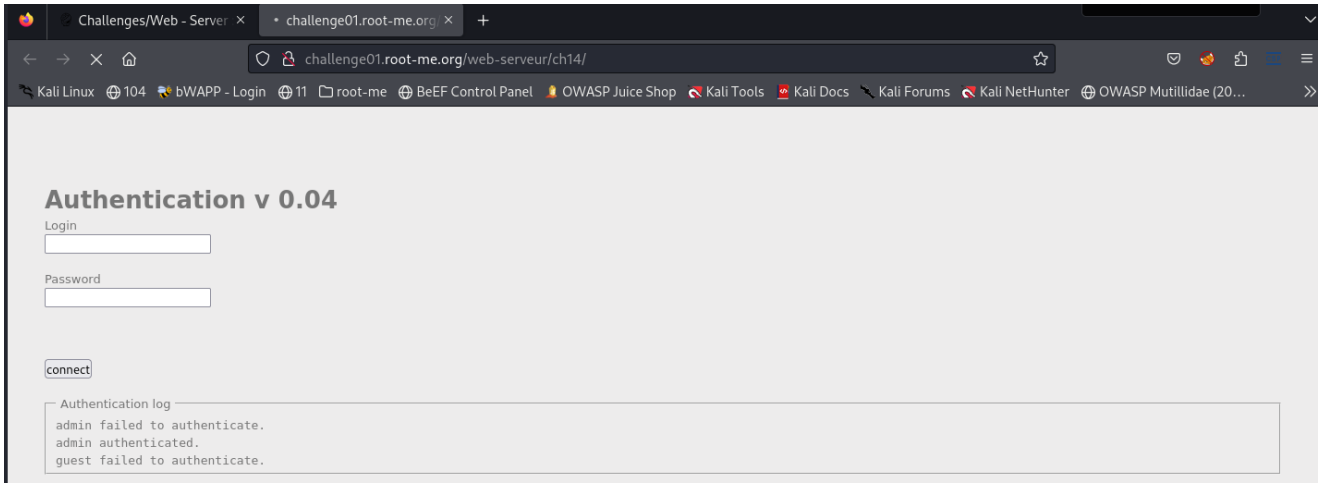
Forward and *Intercept* is OFF



Задание_2:

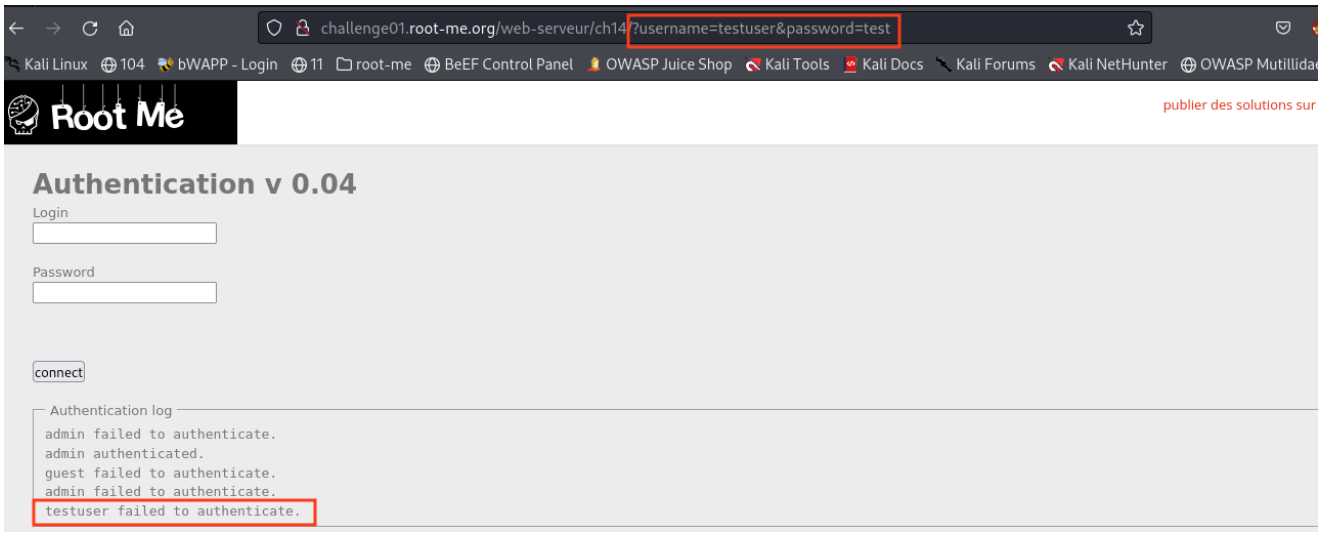
Выполнить задание https://www.root-me.org/en/Challenges/Web-Server/CRLF

Обычно CRLF переносит строку в HTTP-заголовке, например, в заголовке Location, когда мы неправильно достаём символы из URL. В результате происходит перенос строки там, где он не нужен, это приводит к *небезопасным последствиям*.
Первый и самый естественный импакт от CRLF — внедрение произвольных HTTP-заголовков Location, Cookie и любых других. Позже мы покажем, как это происходит. Как правило, CRLF возникает именно в HTTP-заголовках.



admin/admin (login/password) *failed*

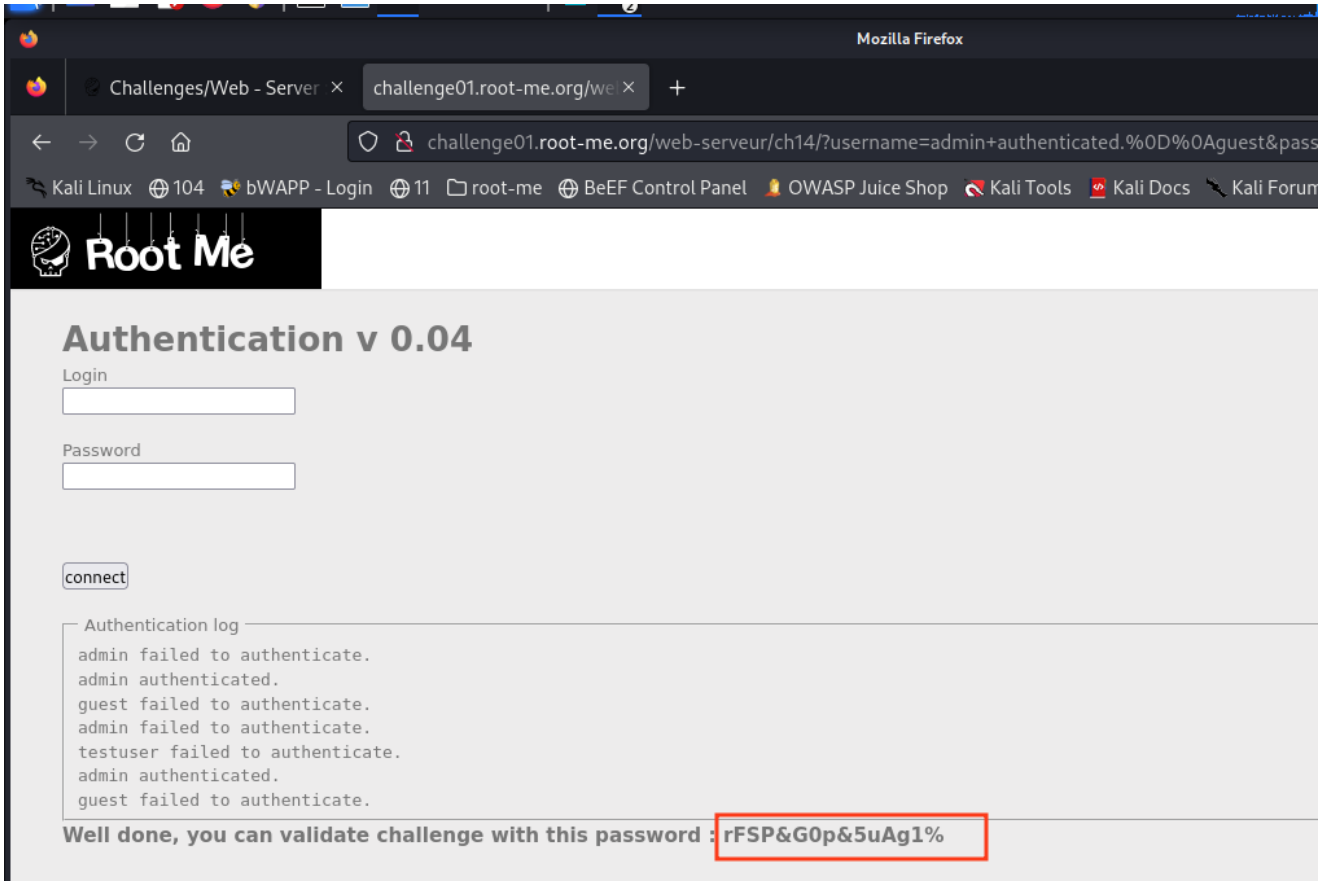
Пробуем зайти под *testuser* пароль *test*
Появилась запись.



Пробуем подставить лог в строку браузера:

```
admin+authenticated.%0D%0Aguest&password=password
```

где *%0* - это перенос строки.



Задание_3:

(*) Если у вас есть желание еще больше потренироваться в данном типе уязвимостей, можете решить эти задания

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