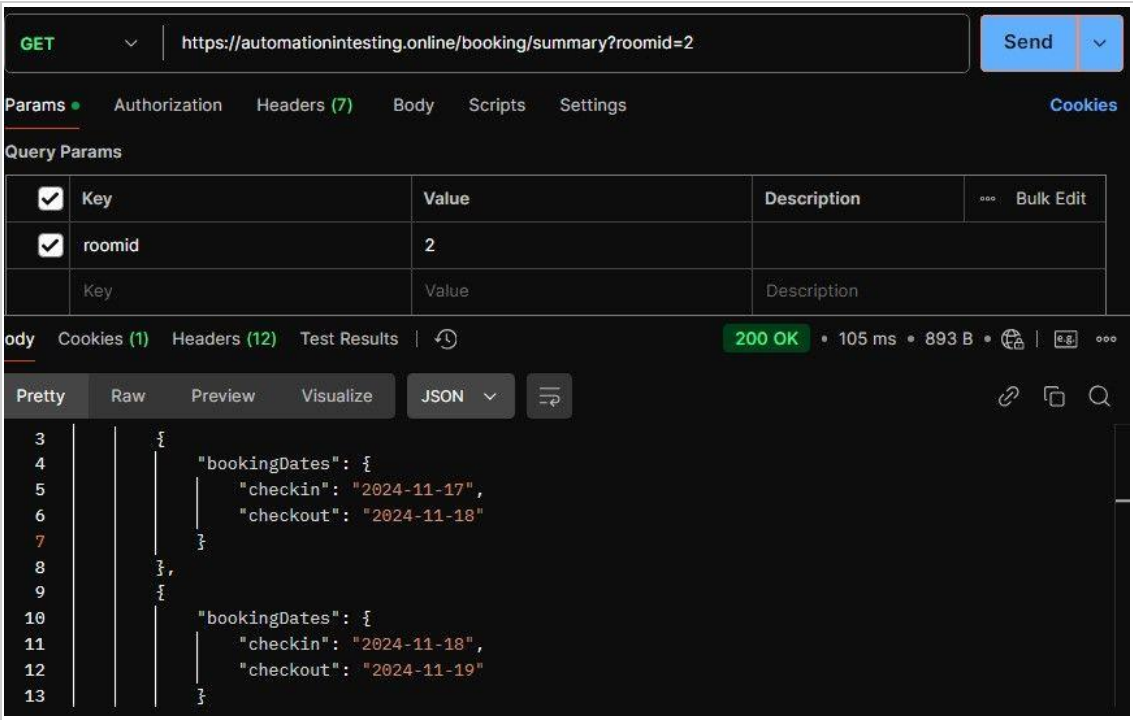
[HBP3-623] Доступ к данным бронирования возможен без авторизации

Created: 11/Nov/24 Updated: 26/Nov/24

Status:	Open
Project:	Hotel Booker Platform - 3
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Bug		
Reporter:	Dzmitry Paulouski	**Assignee:**	Dzmitry Paulouski
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Attachments:



Issue links:

Relates

relates to	HBP3-375	Проверить возможность получить брони ...	New
relates to	~~HBP3-160~~	API | Тестирование API для управления...	Done
relates to	~~HBP3-161~~	Баг-репорты для "User Booking"	Done

Rank:	0|i007u7:
Severity:	High

Description

TEST RUN LINK:

HBP3-TR-308

Используя параметр "roomid" можно получить доступ к данным бронирования из неавторизационной зоны - уязвимость безопасности.

ПРЕДУСЛОВИЯ

Запущен Postman.

Авторизоваться с помощью POST-запроса

адрес запроса: https://automationintesting.online/auth/login

тело запроса:

{ "username": "admin", "password": "password" }

Шаги воспроизведения:

1 Создать с помощью POST-запроса номер

адрес запроса: https://automationintesting.online/room/

тело запроса:

{ "roomid": 0, "roomName":"testRoom", "type": "Single", "accessible": true, "image": "https://avatars.dzeninfra.ru/get-zen_doc/9731390/pub_644a7e154da1351cb7cd9ee3_644a7eb038c3436f14a1b379/scale_2400", "description": "Beautiful room with a view of nature", "features": ["WiFi", "TV", "Refreshments", "Views"], "roomPrice": 777 }

2 С помощью Get-запроса без параметров получить значение параметра “roomid” добавленного номера.

адрес запроса: https://automationintesting.online/room/

3 Создать с помощью POST-запроса бронирование

адрес запроса:

Тело запроса: { "bookingid": 0, "roomid": **(полученного номера из шага 2)**, "firstname": "John", "lastname": "Snow", "depositpaid": false, "email": "example@example.com", "phone": "12345678998", "bookingdates":

{ "checkin": "2024-11-21", "checkout": "2024-11-22" }

4 С помощью Get-запроса без параметров получить значение “bookingid” созданной брони

адрес запроса: https://automationintesting.online/booking/

5 Разлогиниться с помощью POST-запроса

адрес запроса: https://automationintesting.online/auth/logout

Тело запроса:

{ "token": "string"}

6 С помощью Get-запроса вызвать все брони номера

адрес запроса: https://automationintesting.online/booking/summary?roomid=2

{значение параметра “roomid” }

Фактический результат:	**Ожидаемый результат:**
Get-запрос успешно отправлен. Код ответа от сервера 200 ОК. Тело содержит параметр bookingDates. Ответ в формате JSON, содержит данные:	Запрос отправлен. Код Ответа 403 Forbidden


```
{
    "bookings": [
        {
            "bookingDates": {
                "checkin": "2024-11-17",
                "checkout": "2024-11-18"
            }
        },
        {
            "bookingDates": {
                "checkin": "2024-11-18",
                "checkout": "2024-11-19"
            }
        },
        {
            "bookingDates": {
                "checkin": "2024-11-19",
                "checkout": "2024-11-20"
            }
        }
    ]
}
```


Программное окружение: Windows 10, Postman, Chrome.