

Задание выполнил студент группы 2345 Романенко Кирилл

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

Login v0.00001

Password

login

Открыл ссылку, отловил запрос через Burp. В Response был флаг

Response

Pretty

Raw

Hex

Render

\n

≡

```
11 <!--
12
13 Bienvenue sur ce portail,
14 Welcome on this portal,
15
16 J'espère que vous passerez un agréable moment parmi nous, m
17 I hope that you will enjoy your time among us, and above th
18
19 @ très bientôt
20 See ya
21
22 -->
23 <h1>
24     Login v0.00001
25 </h1>
26
27 <form>
28     Password<input type="password" value="" name="passw
29     <br/>
30     <input type="submit" value="login" />
31 </form>
32
33
34 <!--
35 Je crois que c'est vraiment trop simple là !
36 It's really too easy !
37 password : nZ^&@q5&sjJHev0
38
```

Флаг: nZ^&@q5&sjJHev0

Validation

Well done, you won 5 Points

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



tweet it!

2. Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/Weak-password>

challenge01.root-me.org/web-serveur/ch3/

Вход

http://challenge01.root-me.org

Подключение к сайту не защищено

Имя пользователя

Пароль

Вход

Отмена

Введ admin/admin

Bien joué, vous pouvez utiliser ce mot de passe pour valider le challenge

Well done, you can use this password to validate the challenge

Ну ок)

Флаг: admin

Проверка

Молодец, ты выиграл 10 баллов

Не забудьте высказать свое мнение о вызове путем голосования;-)



разместите это в твиттере!

3. Выполните задание <https://www.root-me.org/en/Challenges/Web-Server/User-agent>



Root Me

Wrong user-agent: you are not the "admin" browser!

Отловил запрос через Burp. Отправил в репитер

В Request заменил выделенную строку на admin

```
1 GET /web-serveur/ch2/ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Request

Pretty **Raw** Hex \n ≡

```
1 GET /web-serveur/ch2/ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: admin
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
```

Response

Response

Pretty Raw Hex Render \n ≡

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 10 Nov 2021 14:12:20 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Vary: Accept-Encoding
7 Content-Length: 268
8
9 <html>
  <body>
    <link rel='stylesheet' property='stylesheet' id='s' type='
    <iframe id='iframe' src='https://www.root-me.org/?page=ext
    </iframe>
    <h3>
      Welcome master!<br/>
      Password: rr$Li9%L34qd1AAe27
    </h3>
  </body>
</html>
```

Флаг: rr\$Li9%L34qd1AAe27

Проверка

Молодец, ты набрал 10 баллов

Не забудьте высказать свое мнение о вызове путем голосования;-)



разместите это в твиттере!