guestbook（hackme web部分writeup）

原创

cggwz 于 2020-10-31 12:16:19 发布 329 收藏

分类专栏： CTF hackme题解 文章标签： hackme ctf sql注入 数据库 union select

题目链接

打开链接可以发现，是一个公告栏，可以自己提交标题和内容，然后会在网页上显示出来。

网页源代码肯定啥也没有，抓包也是没有有用的信息，我们考虑flag在服务器的数据库内，所以我们就想到用sql注入。那么数据库的信息会显示在哪儿呢？那就是我们提交的标题内容显示的地方，我们先随便提交一些数据，比如标题为12，内容为34。提交后，查看信息，我们通过网址来进行注入。

首先我们有用的一个尝试：

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,2,3,4#
```

关于这个语句我们有很多值得注意的点。（方便萌新理解，所以会说得更详细一些）

首先是union select，这个语句是用来合并两个搜索，即将两个select的结果放在同一个表内。这就有一个要求，两个结果的列数要是相同，如果不相同会报错。

第二点，#是什么？这是mysql的单行注释，把后面的语句注释掉，消除后面语句的影响。

第三点，我们知道select后面一般加列名，表示我们需要哪一列的信息，那么这里的1234是什么？这就是select的一个特殊用法，这样返回的是一个如下的表：

1	2	3	4
1	2	3	4

列名是1234，内容也是对应的数字。

那么我们这里最大的用处就是试探前面一个select的列数以及回显的位置。

什么意思？

正如前述，如果前后的结果列数不同，是会出错的。所以我们这里并不是直接就写1，2，3，4，其实是尝试1、1，2、1，2，3后得到的结果，所以我之前也是说这是一个有用的尝试，就是示意我略过了这个过程。

那么确定回显的位置又是什么意思？

因为我们要想获取flag，必须要让flag显示在客户端，那么我们就得知道1，2，3，4分别会显示在页面的那个位置，或者说哪个位置会显示。

而这也蕴含第四点，为什么id=-1？因为id=-1时，前面的结果肯定是空，因为id通常是大于0，所以这样我们返回的结果就是如下的结果：

1	2	3	4
1	2	3	4

这样就可以确保网页上显示我们的数字。
关于这一点我们就说这么多，如果有不理解的可以继续向下看。
我们得到的结果可以发现，1不显示，2是标题，3是内容，4是时间。也就是说我们可以利用2，3，4去回显信息。我们以2为例。
输入如下的url：

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,database(),3,4#
```

我们这里用database（）代替了2，database()是用来显示数据库名称的函数，代替了2以后，该url返回的结果中，标题的位置，即原来2的位置，会显示数据库名称，我们看到是g8.
接下来就用类似的方法依次查询我们需要的信息：

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,(select table_name from information_schema.tables wher
e table_schema=database() limit 0,1),3,4#
```

这个语句是查询表的名字，可以得到是flag。
值得解释的是这里的limit，这也只是一个尝试，limit后的第二个数字表示要返回几个数据，而第一个数字是偏移量，表示要从第几行开始查找，这也是需要尝试，只不过这里凑巧，第一个就是我们需要的。
接下来就不一样了，一个有用的尝试：

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,(select column_name from information_schema.columns wh
ere table_name='flag' limit 1,1),3,4#
```

此处我们就是偏移量为1时才是我们需要的列，名字是flag
最后查询flag即可：

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,(select flag from flag limit 1,1),3,4#
```

这样我们就可以获取flag了。
一个类似的练习题：
Login as admin 0.1
这一题是获取数据库里的flag，方法类似。该题的题解会写得简略一些。