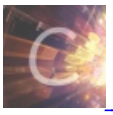
网络安全实验室CTF—注入关 writeup

原创

Senimo_ 于 2019-08-02 20:58:01 发布 1372 收藏 5

分类专栏： 网络安全实验室CTF writeup 文章标签： 网络安全实验室 CTF writeup 注入关

本文链接：https://blog.csdn.net/weixin_44037296/article/details/98239027



网络安全实验室CTF writeup 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

网络安全实验室CTF—注入关 writeup

网络安全实验室CTF链接

最简单的SQL注入

分值: 100

Tips题目里有简单提示

通关地址

进入页面后为登陆模式，查看网页源码：

```
value="重置">
        </form><!-- Tips login as admin-->
    </body>
```

提示以`admin`身份登陆，尝试万能密码：

```
admin' or 1=1 #
```

登录成功！我的座右铭(flag)是 iamflagsafsfskdf11223

成功得到`flag`

最简单的SQL注入（熟悉注入环境）

分值: 100

最简单的SQL注入

通关地址

防注入

到底能不能回显

分值: 350

小明经过学习，终于对SQL注入有了理解，她知道原来sql注入的发生根本原因还是数据和语句不能正确分离的原因，导致数据作为sql语句执行；但是是不是只要能够控制sql语句的一部分就能够来利用获取数据呢？小明经过思考知道，where条件可控的情况下，实在是太容易了，但是如果是在limit条件呢？

通关地址

Today

I meet a girl

看到地址栏通过`GET`方式传参：

```
/index.php?start=0&num=1
```

通过修改参数`start`的值，页面回显不同，通过`'`判断闭合方式：

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' at line 1
Warning: mysql_fetch_row() expects parameter 1 to be resource, boolean given in **sqli5_5ba0bba6a6d1b30b956843f757889552/index.php** on line **52**

根据报错可知，后台对`'`做了转译

邂逅

ErrorBased

盲注

SQL注入通用防护

据说哈希后的密码是不能产生注入的