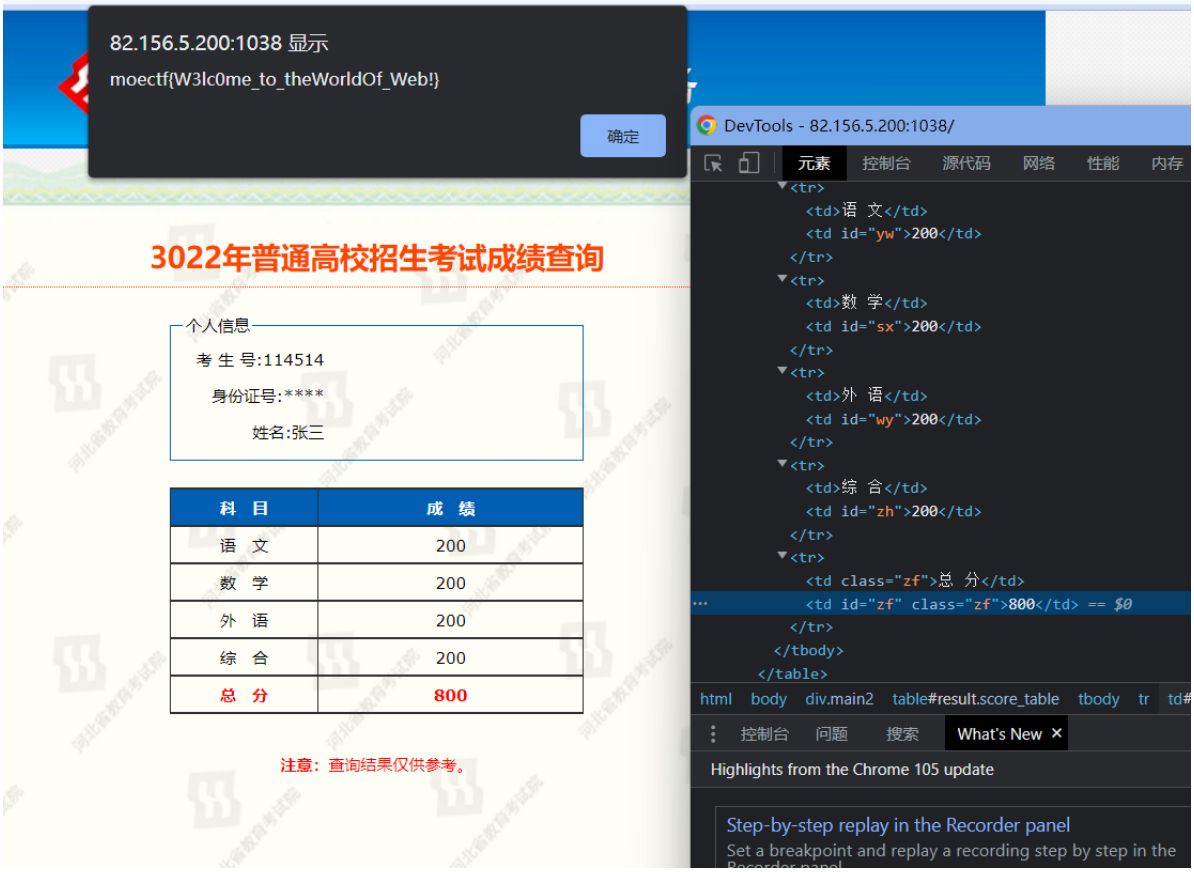
web

ezhtml

F12修改html即可（四科之和等于总分，大于600）

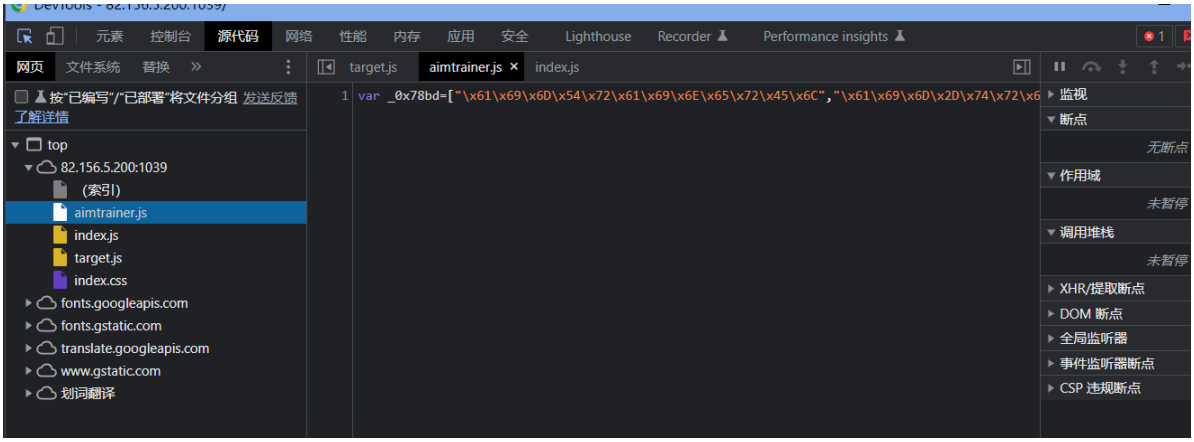


web安全之入门指北

God_of_Aim

打通第一部分，给一半flag，第二部分不可能用手打过吧

在网页源代码里面看了下，看到aimtrainer.js似乎是混淆过的



找找反混淆工具，得到

```
60      checkflag1() {
61          if (this.score == this.aimscore) {
62              this.stop();
63              alert("moectf{Oh_you_can_a1m_");
64              alert("你已经学会瞄准了\uFF01试试看:");
65              this.start2();
66          }
67      }
68      checkflag2() {
69          if (this.score == this.aimscore) {
70              this.stop();
71              alert("and_H4ck_Javascript}");
72          }
```

inclusion

这个题和搜索到的几乎一模一样，都是文件包含

```php
if(isset($_GET['file'])){
    $file = $_GET['file'];
    include($file);
}else{
    highlight_file(__FILE__);
}
```

首先这是一个file关键字的get参数传递，`php://`是一种协议名称，`php://filter/`是一种访问本地文件的协议，`/read=convert.base64-encode/`表示读取的方式是base64编码后，`resource=index.php`表示目标文件为index.php。

通过传递这个参数可以得到index.php的源码，下面说说为什么，看到源码中的`include()`函数，这个表示从外部引入php文件并执行，如果执行不成功，就返回文件的源码。

而include的内容是由用户控制的，所以通过我们传递的`file`参数，是`include()`函数引入了index.php的base64编码格式，因为是`base64`编码格式，所以执行不成功，返回源码，所以我们得到了源码的base64格式，解码即可。

构造成 http://82.156.5.200:1041/?file=php://filter/convert.base64-encode/resource=flag.php

得到flag的base64，解码得到一个ikun

```
<?php
Hey hey, reach the highest city in the world! Actually I am ikun!!;

moectf{Y0u_are_t00_baby_la};

?>
```