Hgame week1 write up

very easy web

```php
<?php
error_reporting(0);
include("flag.php");

if(strpos("vidar",$_GET['id'])!==FALSE)
  die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
  echo $flag;
}
highlight_file(__FILE__);
?>
```

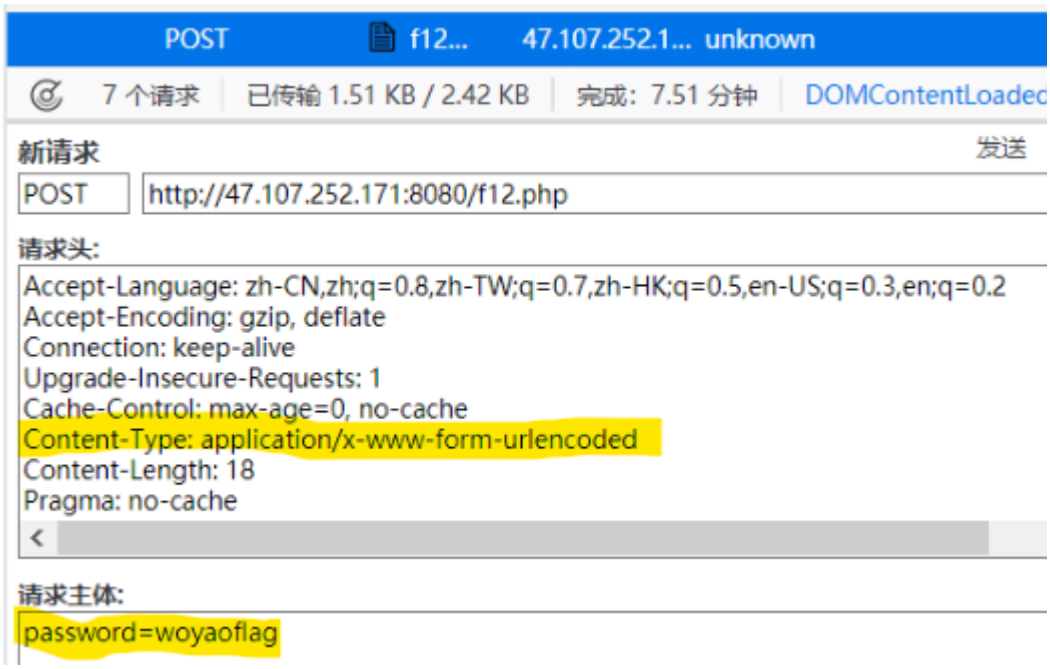
通过代码可知，通过`GET`方法传输数据，并将`id`的值在字符串`vidar`中查找，如果返回值非`false`则直接输出退出脚本，输出`干巴爹`。

又因为下面进行了`urldecode($_GET['id'])`,所以要在`urldecode`前不等于`vidar`，解码后等于`vidar`，因此将`vidar`编码，所以查找ascii码，得到字符串`%76%69%64%61%72`，又因为在地址栏直接传值的时候会自动进行一次urldecode，所以对`%76%69%64%61%72`再进行一次urlencode，得到字符串`%2576%2569%2564%2561%2572`，传值进入后得到flag

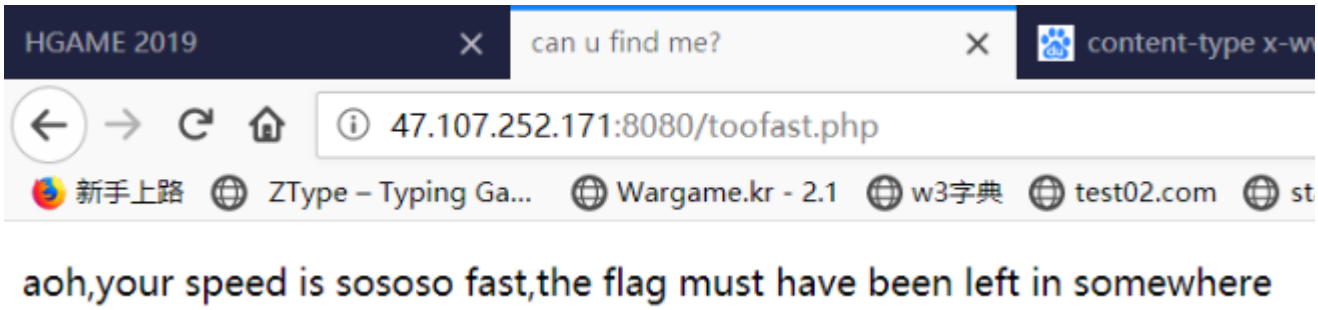
hgame{urlDecode_Is_GoOd} <?php
error_reporting(0);

can you find me?

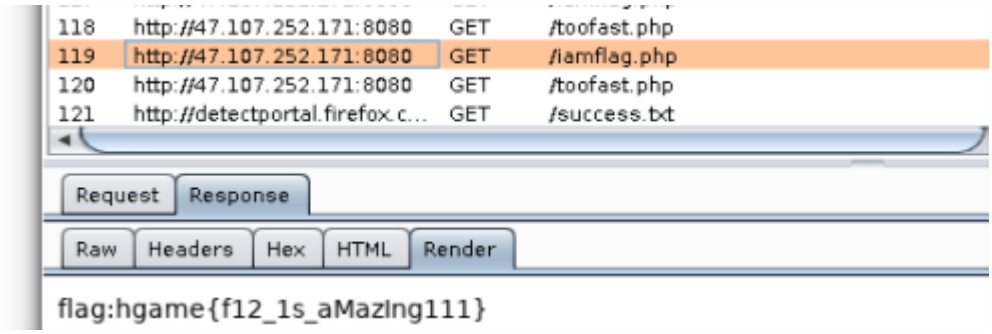
进去直接开f12，找到`f12.php`，通过页面知道要通过`POST`方法传入密码，继续开f12，找到密码是`woyaoflag`，用`burp suite`或者火狐浏览器可以直接改包，将方法更改为`POST`，在报文主体添加`password=woyaoflag`，并在首部添加`content-type: application/x-www-form-urlencoded`。



根据响应的页面已知，flag应该在`iamflag.php`页面，然而访问过去后进入了`toofast.php`页面，提示说我速度太快？？？？



继续f12，看到302跳转，这个地方因为响应头部有location，所以直接进行了跳转，因此看不到响应实体，换`burp suite`，



拿到flag