


## 作业一

(1) 南开大学体育场馆预约网站 <http://tycg.nankai.edu.cn>



南开大学体育场馆在线预订系统

- 23、24日闭馆预告

6月24日校园开放日期间如遇极端天气，体育馆1、2号馆 23日14:00-24日全天,将暂停开放，保障校园开放日活动，如需要暂停开放，我中心将以短信方式通知已预订场地师生，请留意场馆预定平台公告及通知短信。

6月17日至7月15日，因毕业晚会、毕业典礼、场馆座椅维修等活动，体育中心羽毛球场暂停对外开放。

6月22日全天田径场举办2017届毕业嘉年华活动，活动欢迎非毕业班同学参与，活动期间田径场暂停足球运动。

6月24号14:00-18:00 留学生活动，篮球场暂停对外开放。

6月24日体育中心全馆（包括游泳馆）暂停开放。

6月25号12:00-18:00，南开大学、成都电子科技大学、格拉斯哥大学3校联合运动会羽毛球比赛，1号馆闭馆。

6月26号8:00-12:00 南开大学、成都电子科技大学、格拉斯哥3校联合运动会足球赛，

登录该网站时，对网站进行请求，会出现一个数据包

其 url 为

`index.php?s=My/Account/login.html&v=1370796461123973&callback=jsonpReturn&Username=1511366&Pwd=hM3XiD2Eq58I6AAWPKV4aw%3D%3D&mPwd=&login_type=1&remember_me=&button=&_1498183736757`

分析可以看出，是一个 GET 请求密码是在请求时就加密的，没有明文发送

田径场暂停对外开放。

请登陆

1511366	
.....	

- ☒ 信息门户用户登录
- ☐ 非信息门户用户登录

Name	Sta...	Ty...	Initiator	Size	Time	Timeline - Start Time	1.00 s
<input type="checkbox"/> index.php?s=...	200	xhr	jquery,...	593 B	184...		

Name	Sta...	Ty...	Initiator	Size	Time	Timeline – Start Time	1.00 s▲
index.php?s=...	200	xhr	jquery....	593 B	184...		

1 requests | 593 B transferred

× Headers Preview Response Cookies Timing

▼ General

**Request URL:** http://tycg.nankai.edu.cn/nkvenue/index.php?s=My/Account/login.html&v=1370796461123973&callback=jsonpReturn&Username=1511366&Pwd=hM3XiD2Eq58I6AAWPKV4aw%3D%3D&mPwd=&login\_type=1&remember\_me=&button=&\_=1498183736757

**Request Method:** GET

**Status Code:** 200 OK

▼ Response Headers view source

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

(2) 计算机上机课程辅助测评系统 <http://acm.nankai.edu.cn/nkcoj/>  
 登录后，network 中有两个请求，login.php 和 vcode

计算机上机课程辅助测评


首页 课程 题目列表 解题状态

用户登录

用户名或密码错误！

用户ID:

密码:

验证码:  

还没有账户？快来注册一个吧

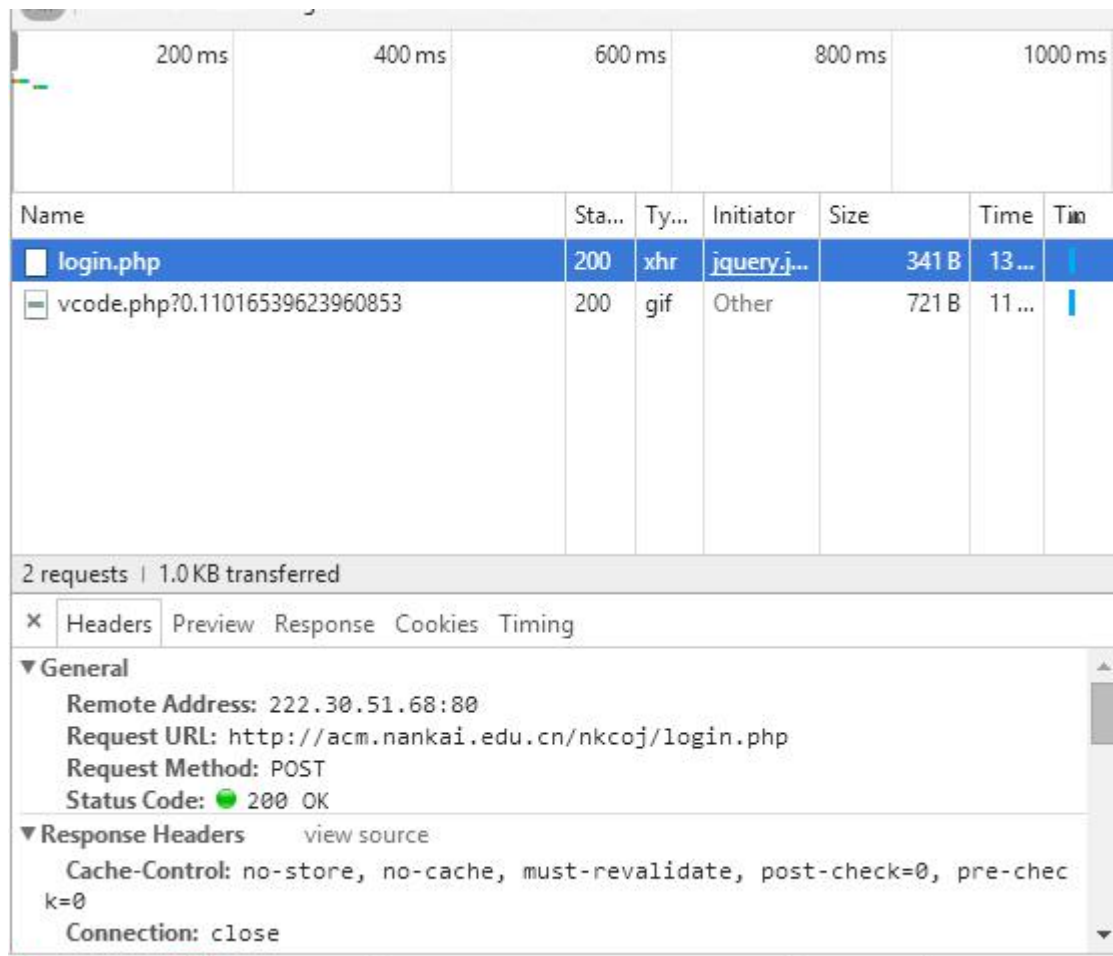
Network

Filter: XHR JS CSS Img Media Font Doc WS Other

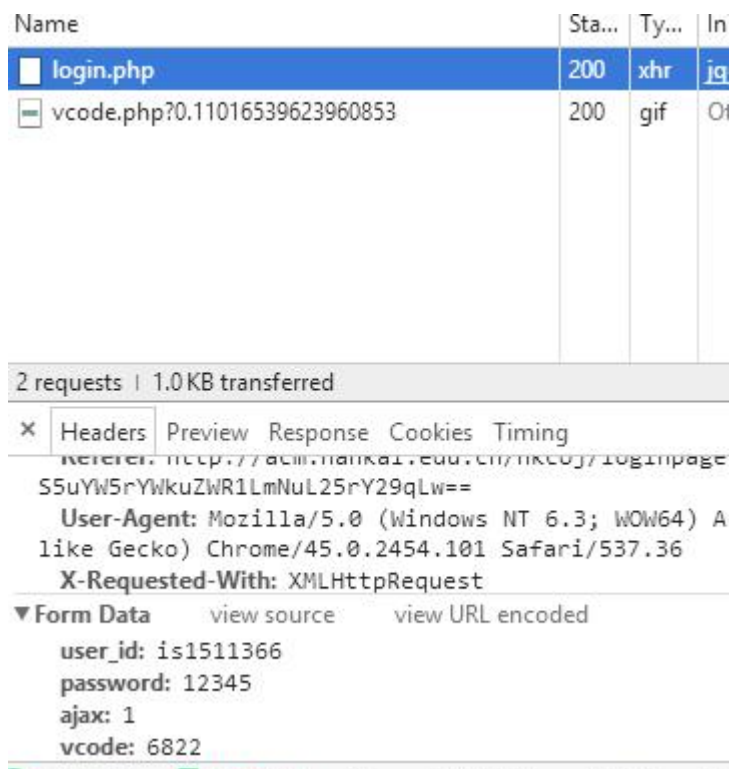
200 ms 400 ms 600 ms 800 ms

Name	Sta...	Ty...	Initiator	Size	T
login.php	200	xhr	jquery-j...	341 B	
vcode.php?0.11016539623960853	200	gif	Other	721 B	

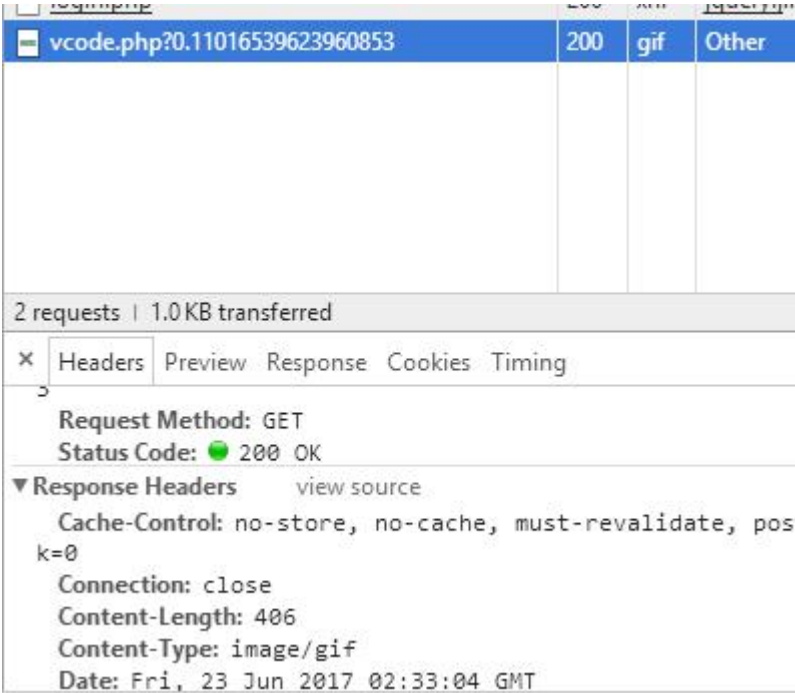
Login.php 是响应登录的请求，是 post 方式的，密码没有加密但是在 post 方式下打包进行传输。



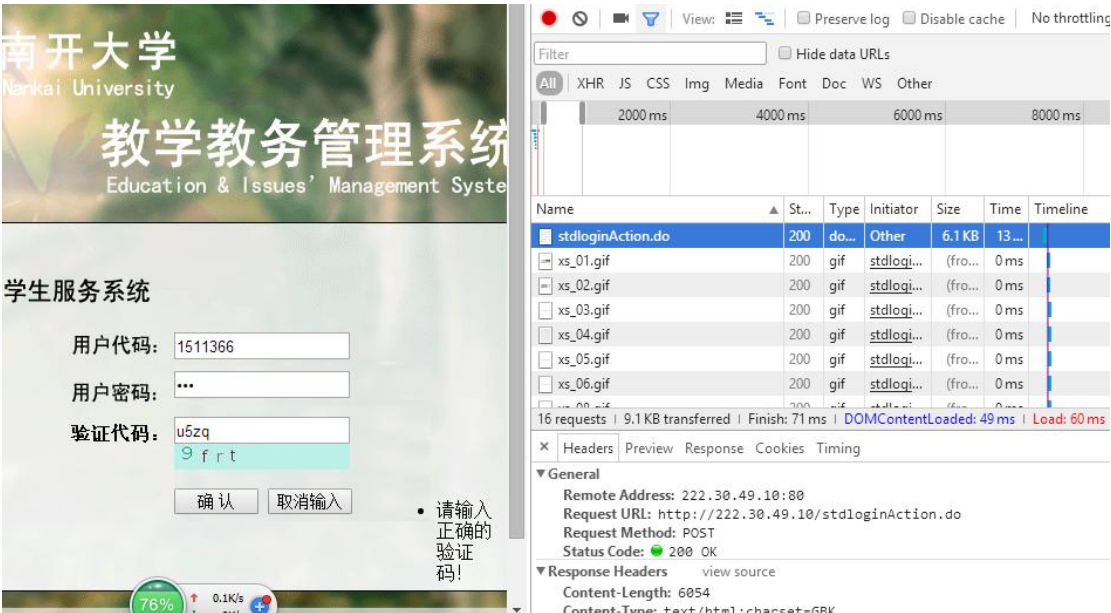
下图可以看出用户名，密码，验证码



另一个请求时 `vcode`，是 `gif` 文件，应该是一个验证码的图片，当登陆失败后，请求一张新的验证码图片，传输方式为 `get`，连接类型为 `image/gif`



(3) 旧选课系统 `http://222.30.49.10/`  
登陆后会出现一系列的请求数据包，大部分是图片数据，为 `get` 方式，有一个登录请求为 `post` 方式



还有一个数据包是 html 类型，猜测是登陆失败后自动刷新页面，为 get 方式

The screenshot shows the login page of Nankai University's Education & Issues' Management System. The page has a green header with the university's name and logo. Below the header, there's a section for '学生服务系统' (Student Service System) with input fields for '用户代码' (User Code), '用户密码' (User Password), and '验证码' (Verification Code). The '验证码' field contains the text 'u5zq' and a small image of a verification code. There are buttons for '确认' (Confirm) and '取消输入' (Cancel Input). A message on the right says '请输入正确的验证码!' (Please enter the correct verification code!).

The network traffic analysis in Chrome DevTools shows a list of requests. The selected request is 'favicon.ico' with a status of 500 (Internal Server Error). The request details show: Remote Address: 222.30.49.10:80, Request URL: http://222.30.49.10/favicon.ico, Request Method: GET, Status Code: 500 Internal Server Error.

Name	St...	Type	Initiator	Size	Time	Timeline
ValidateCode	200	jpeg	stdlogi...	1.2 KB	9 ms	
favicon.ico	500	text/html	Other	1.8 KB	6 ms	
fgf.gif	200	gif	stdlogi...	(fro...	0 ms	
security.js	200	script	stdlogi...	(fro...	0 ms	
stdloginAction.do	200	document	Other	6.1 KB	13 ...	
xs_01.gif	200	gif	stdlogi...	(fro...	0 ms	
xs_02.gif	200	gif	stdlogi...	(fro...	0 ms	



(4) 四六级报名网站 <http://cet.etest.net.cn/>

点击验证码图片后，会出现两个数据包，一个是图片数据，一个是加载图片，为 post 方式


The screenshot shows the login page of the CET-4/6 registration website. The page has a purple header with the text '考生登录' (Candidate Login) and 'LOGIN'. Below the header, there's a section for '考生登录' with input fields for '账号' (Account), '密码' (Password), and '验证码' (Verification Code). The '验证码' field contains the text 'drlf' and a small image of a verification code. There are buttons for '找回账号?' (Find Account?) and '找回密码?' (Find Password?). A message at the bottom says '没有通行证? 点击注册' (No pass? Click Register).

The network traffic analysis in Chrome DevTools shows a list of requests. The selected request is 'LoadCheckImage' with a status of 200 and type 'xhr'. The request details show: Remote Address: 222.30.49.10:80, Request URL: http://222.30.49.10/LoadCheckImage, Request Method: POST, Status Code: 200 OK.

Name	St...	Type	Initiator	Size
LoadCheckImage	200	xhr	jquery-...	383 B
1B69EDC0D88D7BD615960A14108...	200	jpeg	Other	1.8 KB

Name	St...	Type	Initiator
 LoadCheckImage	200	xhr	jquery-
 1B69EDC0D88D7BD615960A14108...	200	jpeg	Other

2 requests   2.2 KB transferred			
×	Headers	Preview	Response
<div> <div>▼ General</div> <div> Remote Address: 211.151.240.47:443  Request URL: https://passport.etest.net.cn/CheckImag  Request Method: POST  Status Code:  200 OK </div> </div> <div> <div>▼ Response Headers</div> <div> Cache-Control: private  Connection: keep-alive </div> </div>			

## Jquery 调试 1



隐藏了 span 的内容（南开大学体育场馆在先预订系统）





## Jquery 调试 2

通过 click，关闭了网页上的一个广告



## Jquery 调试 3

通过函数，用 val 和 alert 功能，在点击登录时显示账号密码，但是可惜密码是被加密的，但有一次尝试时，密码没有被加密就显示了出来，碰碰运气或许能得到真实密码。

```
$("[type='submit']").click(function(){alert("密码: " + $("#password").val());})
```

