验证码漏洞

- 缺失验证码导致爆破
  - 邮箱轰炸
  - 短信轰炸
- 前端校验
  - 先输入正确验证码再抓包爆破
  - 禁用js：
    - 用浏览器插件：uBlock Origin
    - F12禁用所有函数
    - F12重写校验函数，置空
- 验证码回传
- 验证码复用
  - 验证码不失效
  - 他人验证码复用（使用其他用户名和其验证码）
- 验证码爆破

任意用户注册

- 无限注册导致垃圾信息
- 用别人邮箱、手机注册
- 注册覆盖已有用户导致密码重置

扩展

存在CSRF token的爆破

现象

爆破时后端服务器会验证自己下发的一次性的token字符串

思路

1. 在尝试新的密码前，先发送一个请求，从该请求的响应中获得token的值
2. 在尝试新密码的时候，用第一步请求获得的token值来替换原有的token值

工具

yakit（用到其中的序列）

步骤

1. 拦截并创建两个请求

   ctrl+r两次

2. 将两个请求加入爆破序列

   鼠标拖动

   点击序列标签，加入第二个请求

3. 在第一个请求中筛选出token的值并存入变量token

   选中第一个请求，发送请求

   创建一个数据提取器，用正则提取，存入token中

   ```
   name="token" value="(.*)"
   ```

   调整成分组1

   创建一个pass的变量，值：{{x(pass_top25)}}

4. 在第二个请求中继承pass和token变量的值

   选中第二个请求

   替换密码和token的值，分别为：

   ```
   {{p(pass)}}
   {{p(token)}}
   ```

5. 直接爆破

注意

1. 变量名选fuzztag类别
2. 两个请求都要删除cookie