## 一 暴力破解

使用Intruder进行暴力破解，抓包选择password字段，生成字典进行爆破。观察到密码正确时返回文件大小不同。

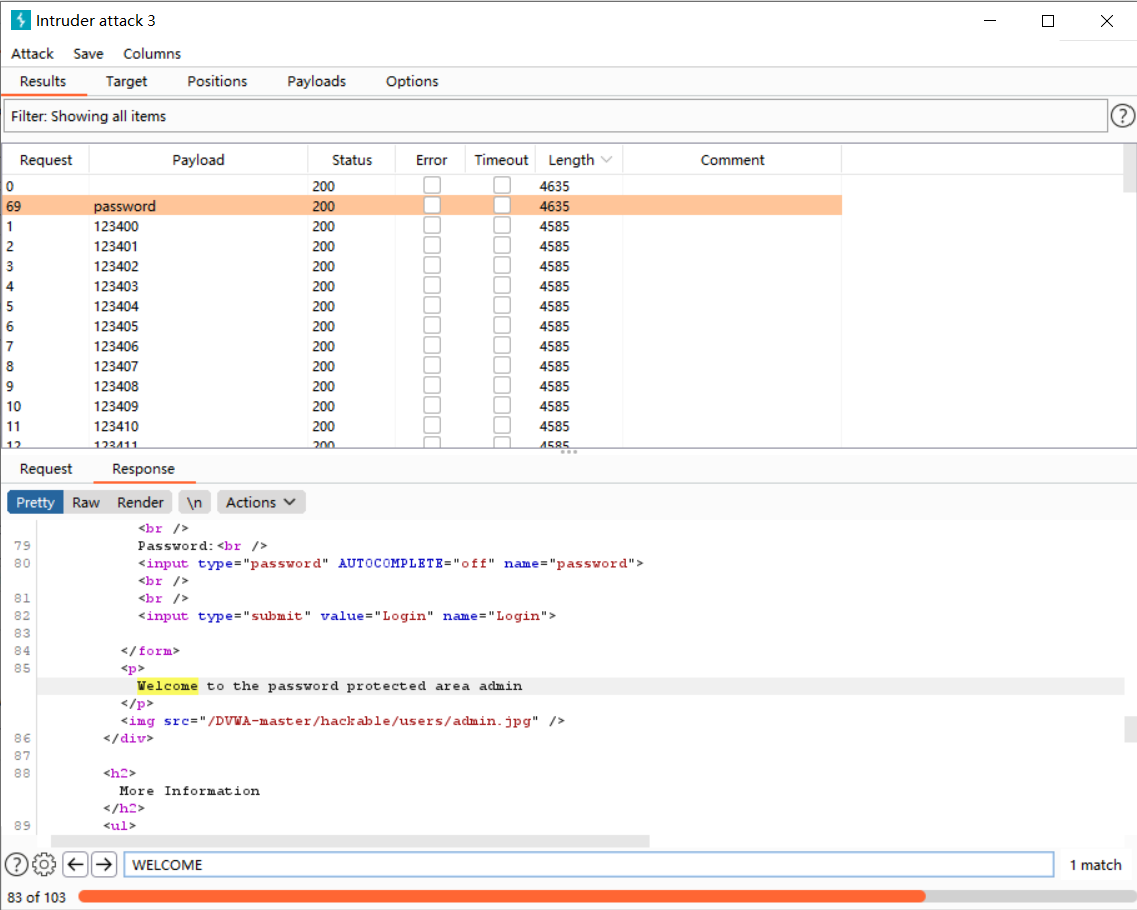


图1 暴力破解

## 二 命令注入

在DVWA的Command Injection界面，在填入IP地址的输入框内输入“127.0.0.1 && ipconfig”，观察到输出了不应输出的信息（ipconfig暴露了主机地址）

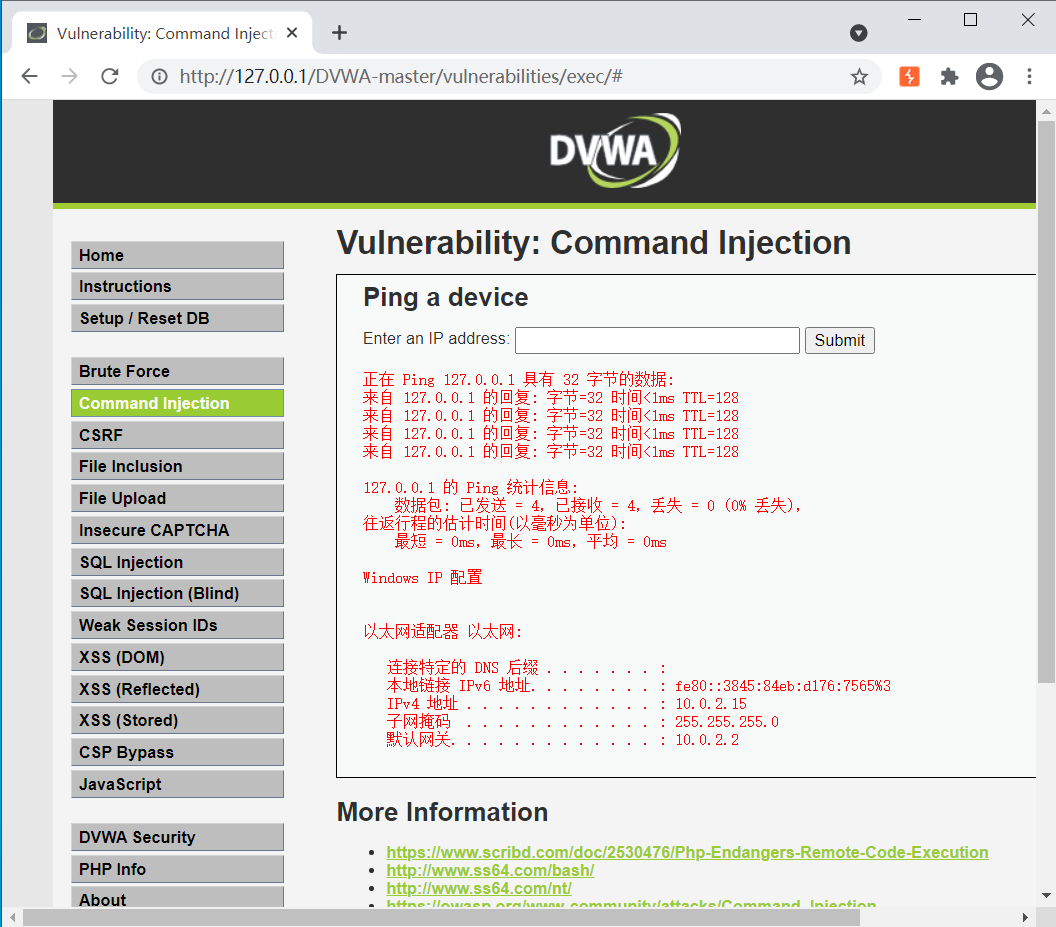


图2 命令注入

## 三 跨站请求伪造

在CSRF界面，填入密码进行修改，发现请求的url中直接暴露了要修改的密码，故构造伪装页面，伪造用户浏览器进行访问。

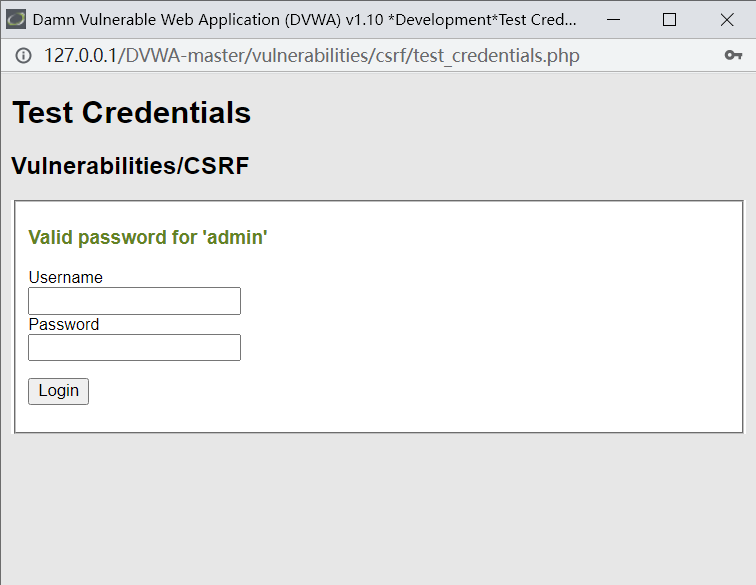


图3 验证密码正确

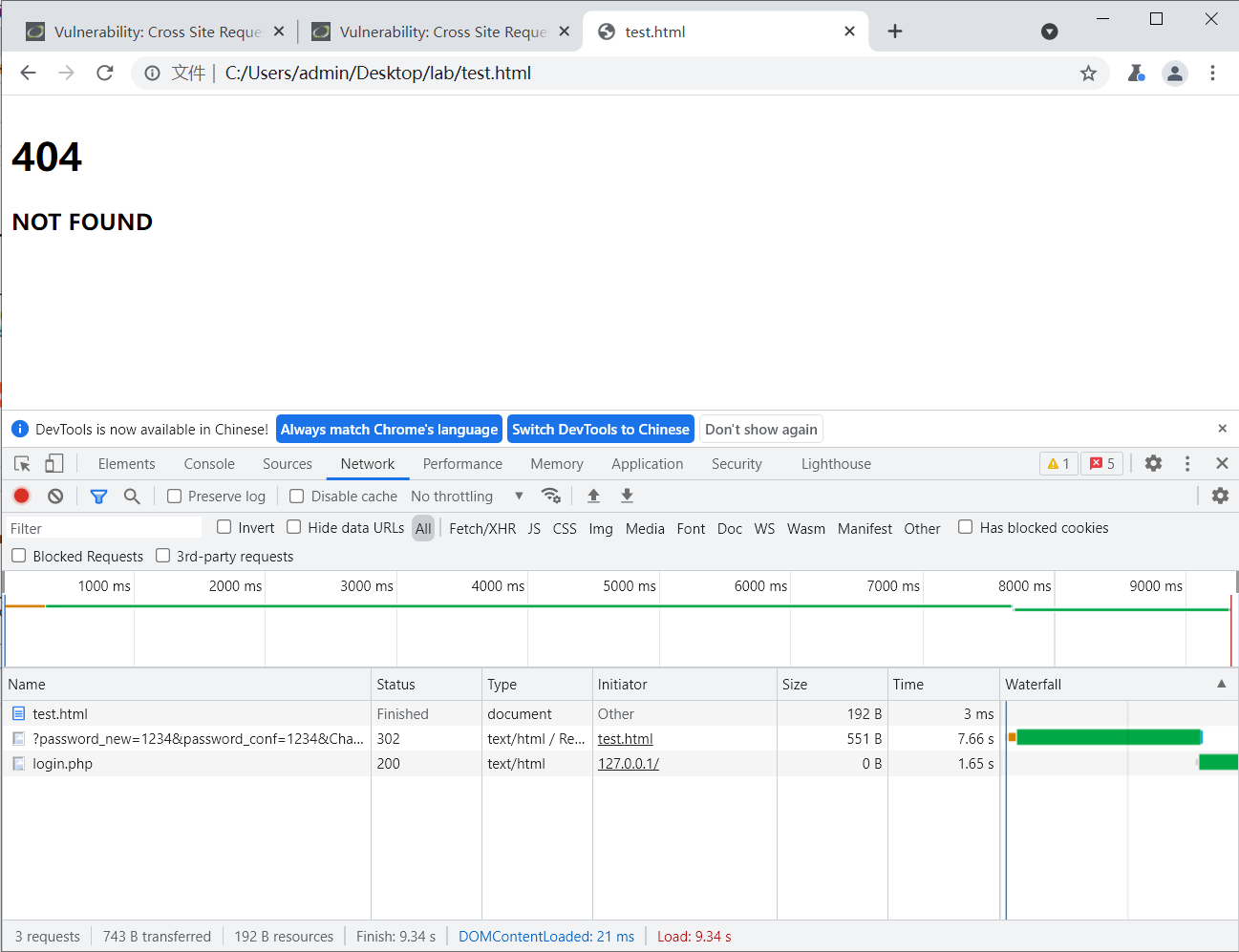


图4 构造的伪造请求界面

## 感想

本次实验主要使用DVWA和burpesuite进行渗透测试。Burpesuite功能全面，比wireshark+手写工具使用效率更高。实践的几个漏洞较为基础，在当代web环境下可能很难发挥作用，但对今后学习更深入的web渗透有一定意义。