【实验要求】

脚本攻击是利用网页或者文档中可以动态执行的Javascript、VBscript等脚本语言编写恶意操作的代码，从而实现恶意操作。Office文档的宏病毒、HTML恶意脚本、跨站攻击都属于脚本攻击的范畴。

本次实验将进行XSS跨站脚本攻击。

【实验准备】

提前查阅Javascript、VBscript等脚本语言

提前学习PHP或ASP或JSP快速建站的方法

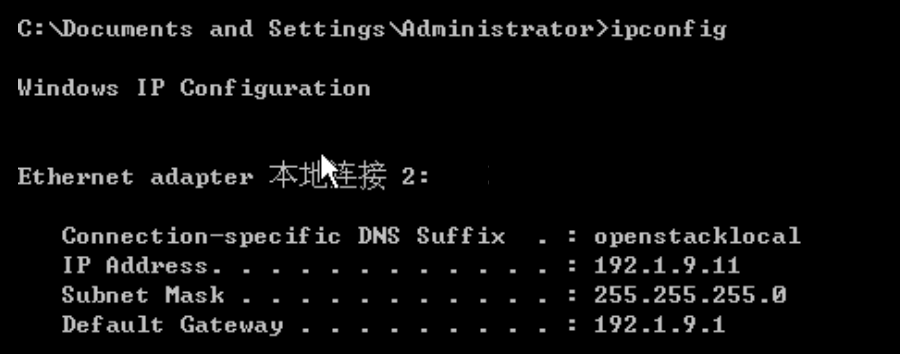
【实验步骤】

1）启动【安全实训平台】（172.19.138.222）——【web漏洞利用】——【动易CMS系统存储型XSS漏洞】，按照实验提示，进入【开始】——【管理工具】——【Internet信息服务管理器】，开启pecms网站服务；

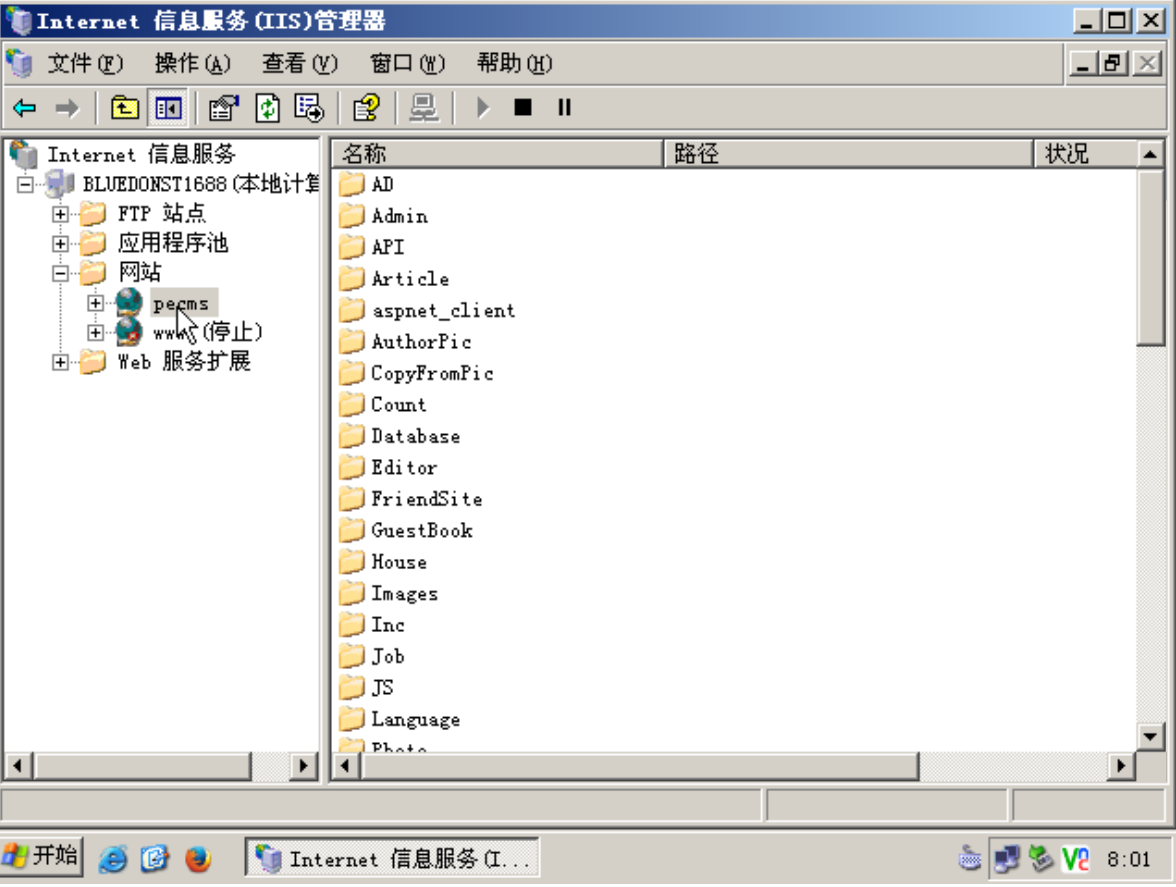
2）使用ipconfig查看本虚拟机IP地址x.x.x.x，使用浏览器打开并访问，即：http://x.x.x.x。注册、登录后，自行查找可以进行xss跨站攻击的目标网页（如短信，留言），并实施脚本攻击测试；

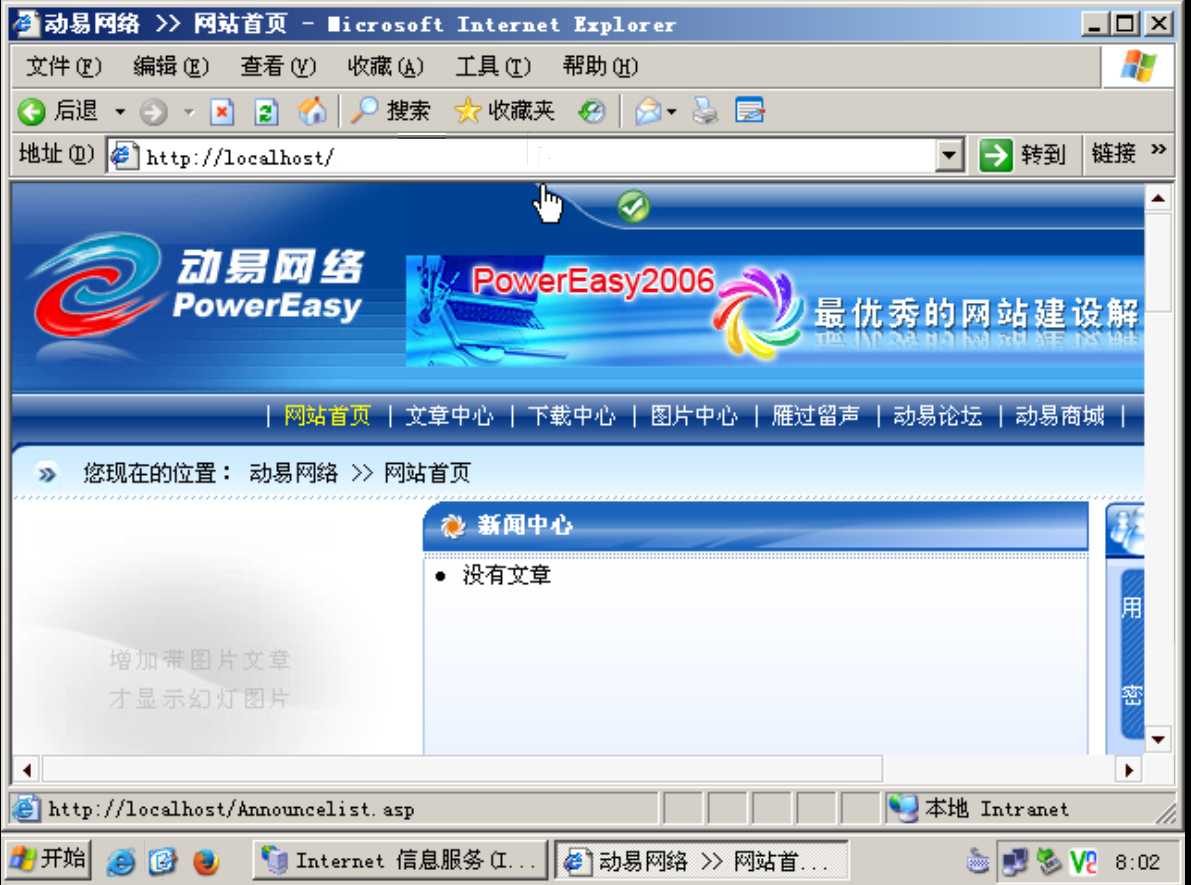
【实验内容】

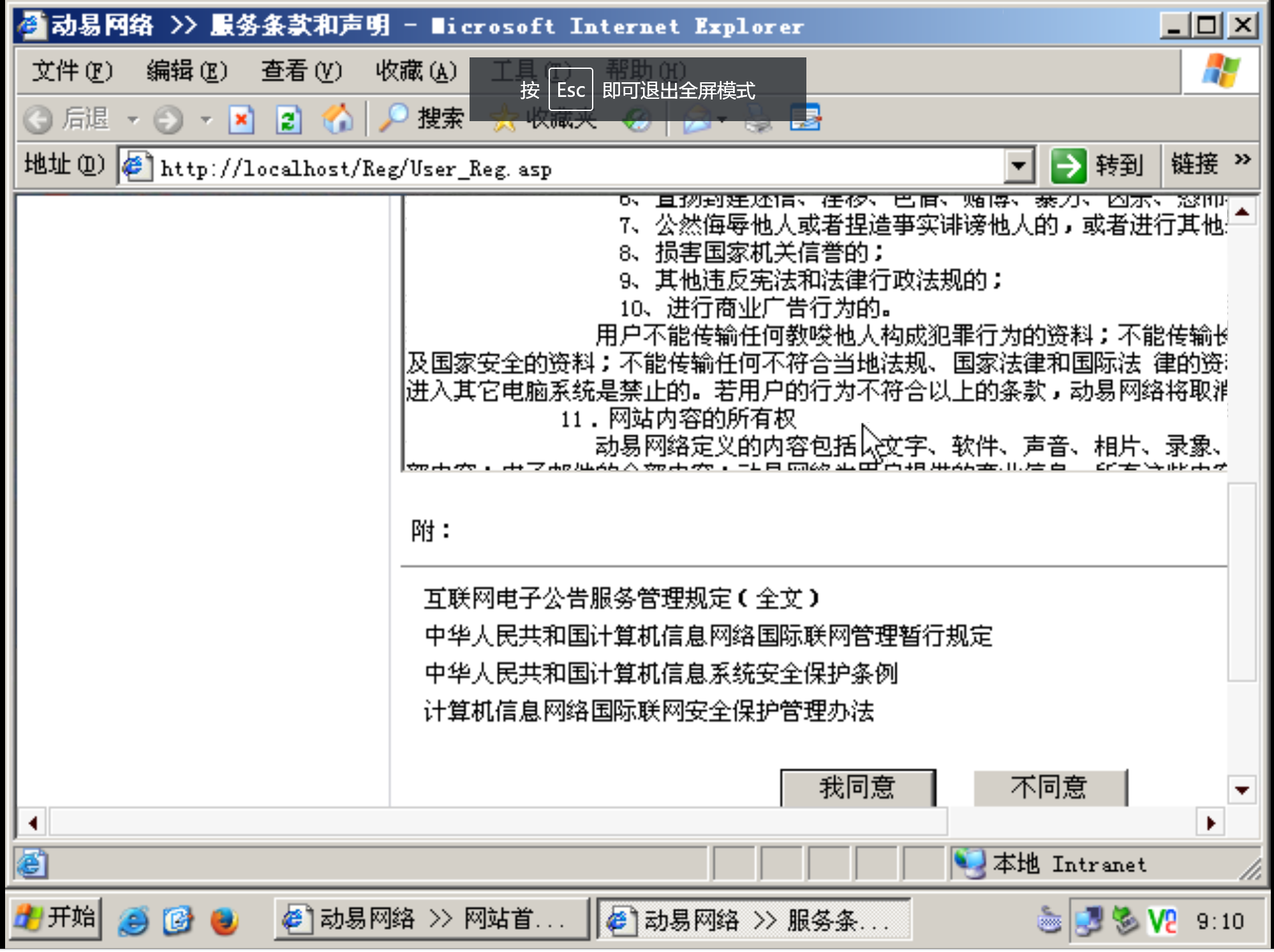
1. 使用ipconfig，查看本实训使用的虚拟机IP地址，并截图

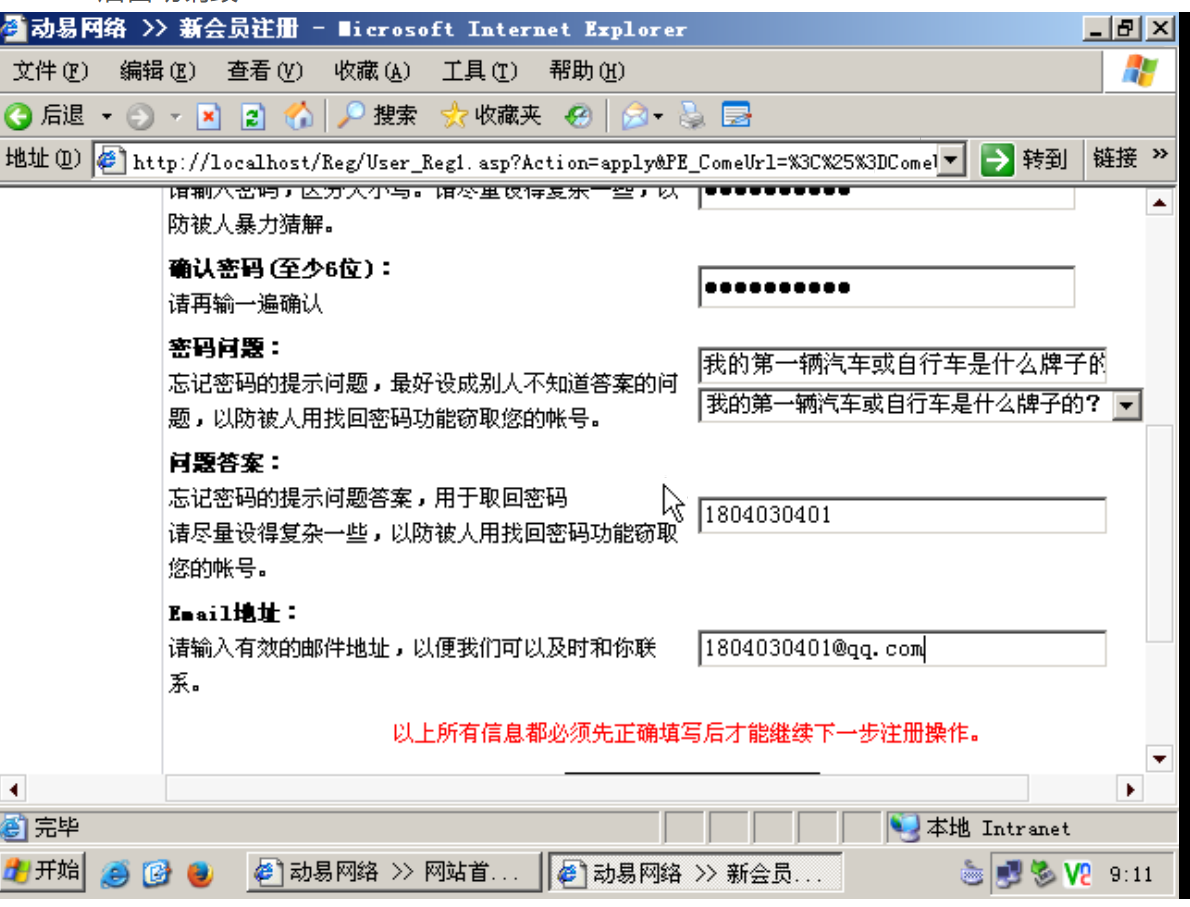


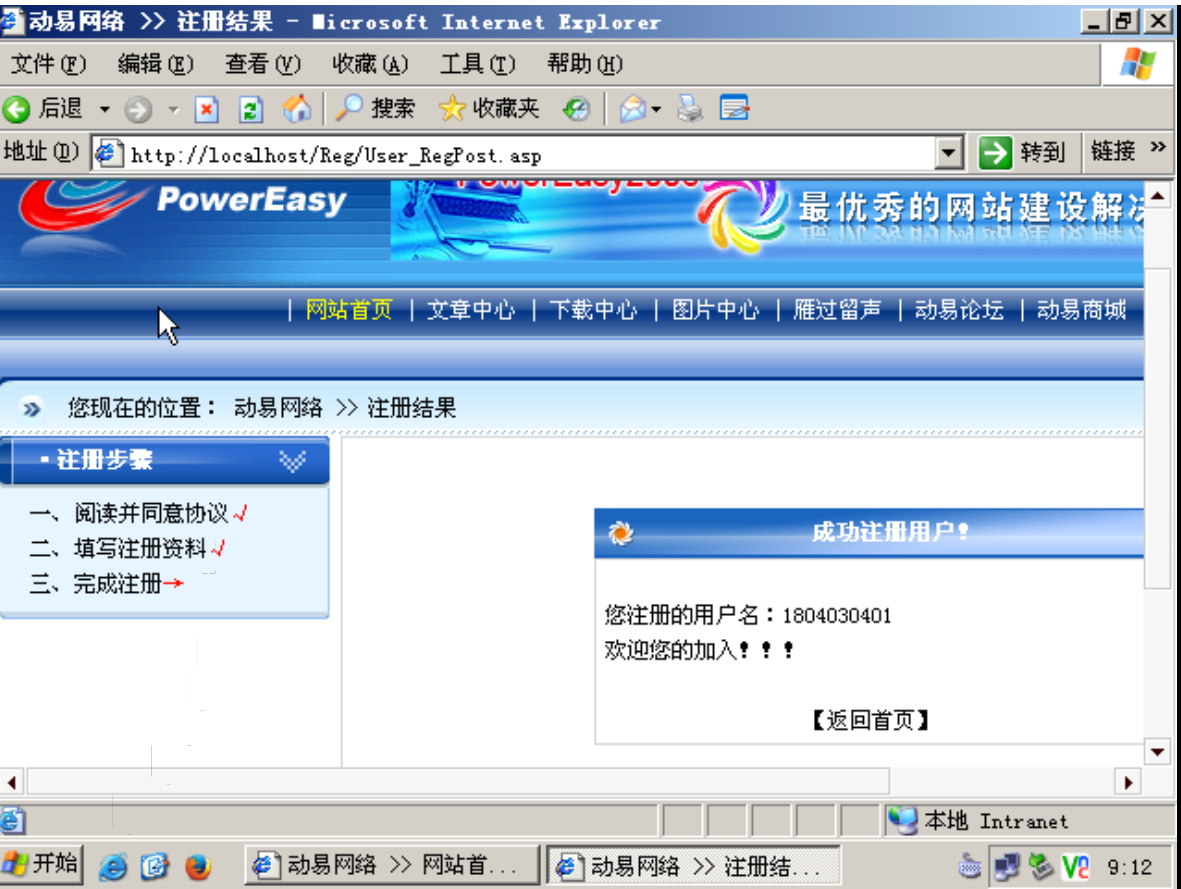
1. 启动pecms动易cms，以你的学号或姓名为账号注册系统，发表留言或短信，并弹出你的姓名，学号的弹窗，弹出cookie，并截图；

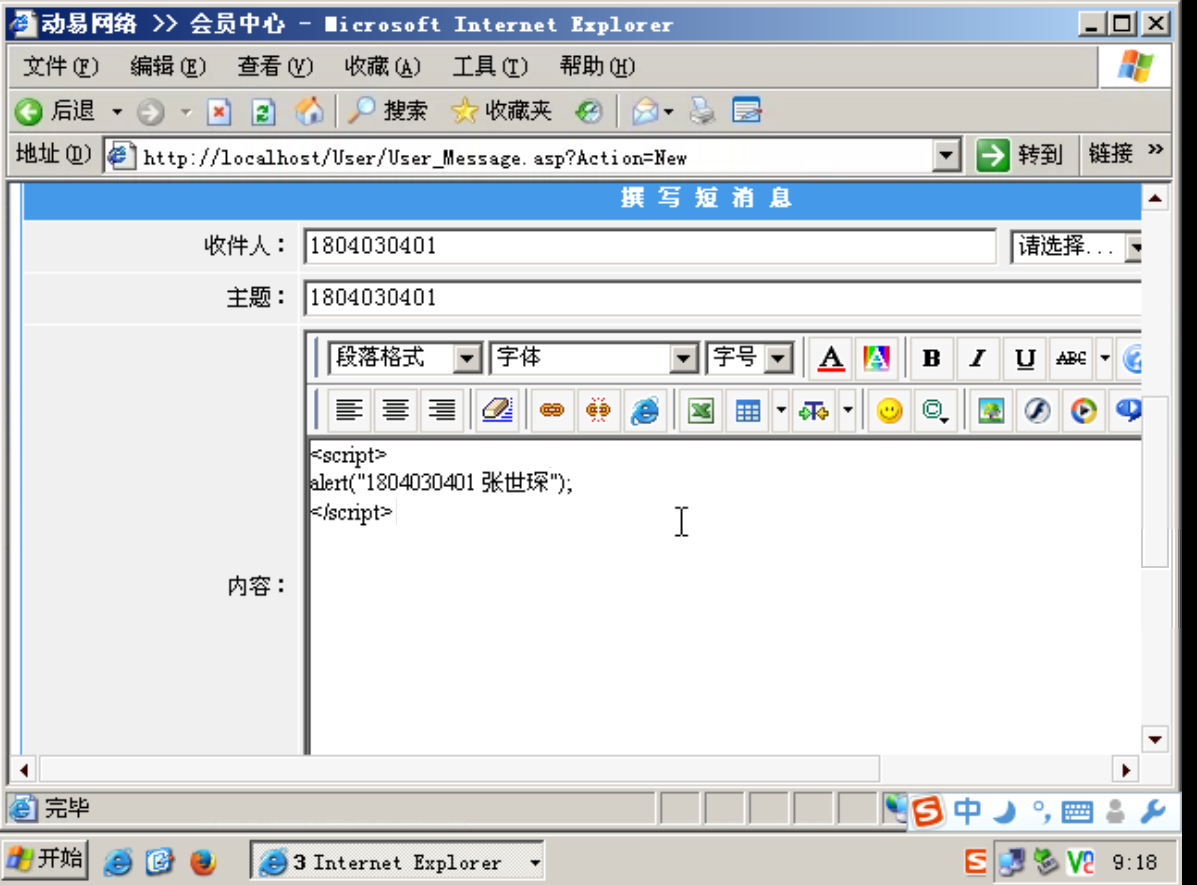


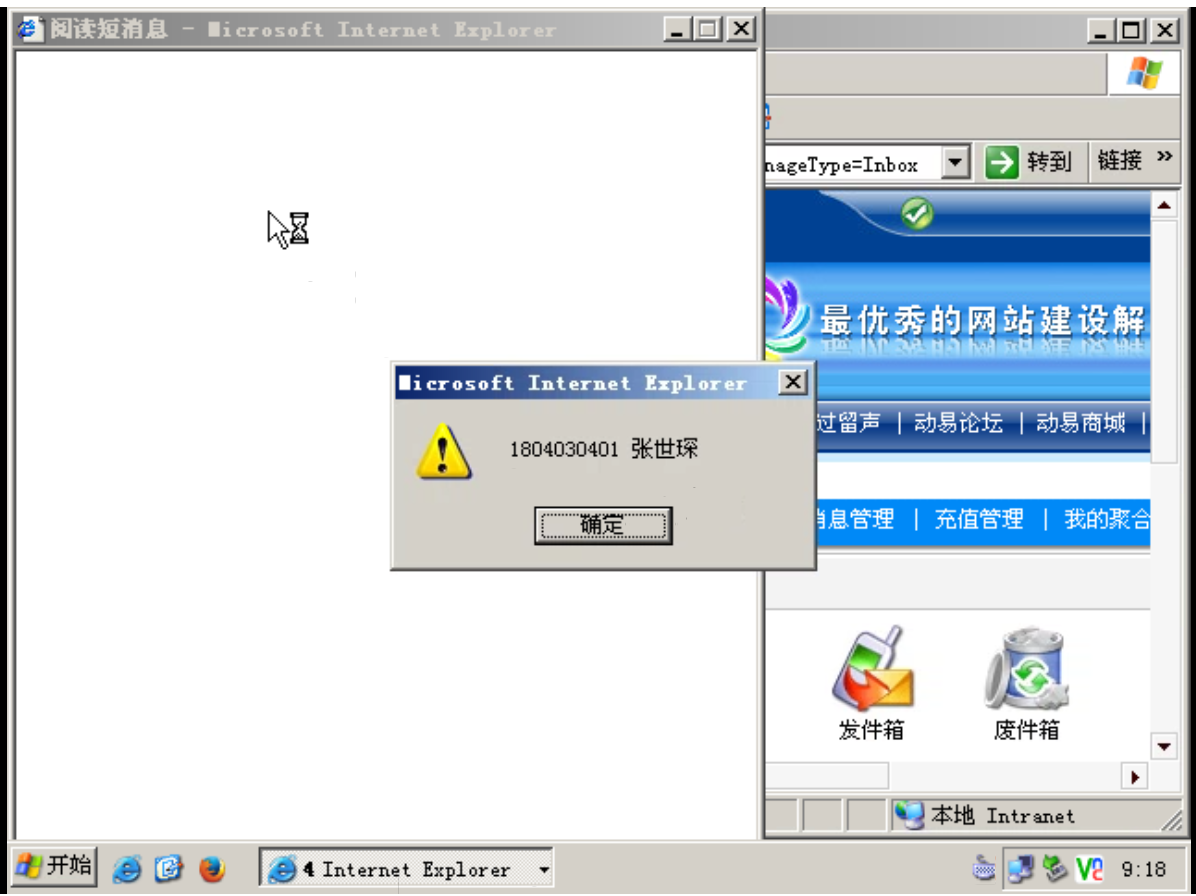


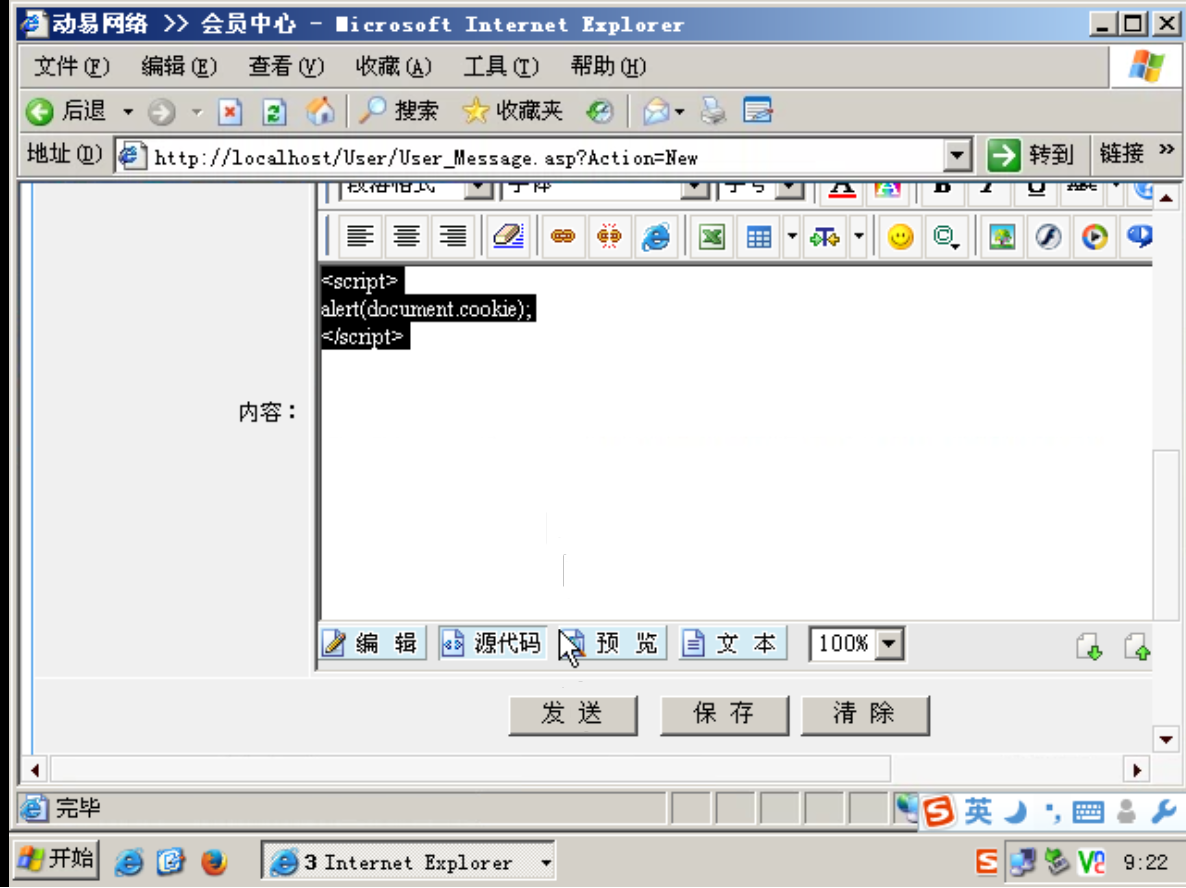


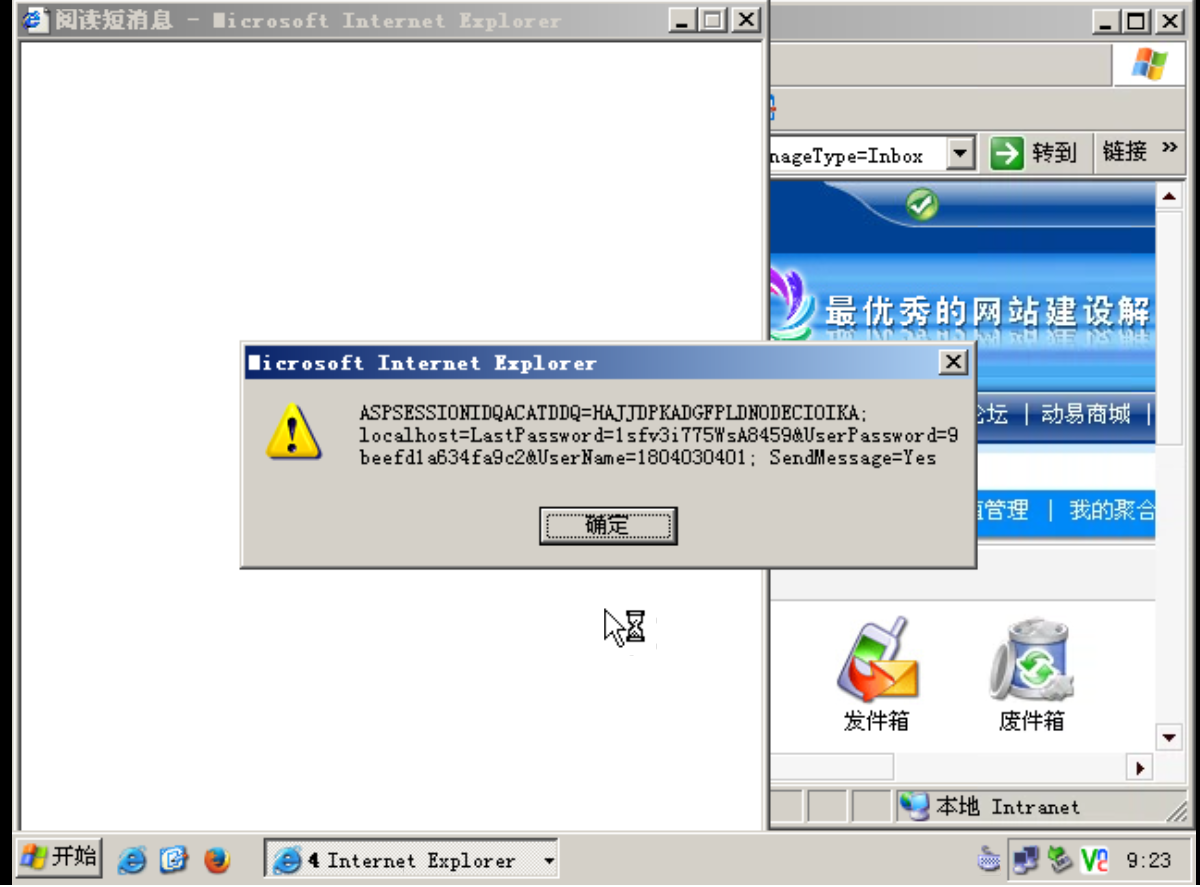












[3.选做] 在实训虚拟机上录入能够盗取cookie的脚本，并作为参数发送到已经搭建好环境的另一台实训虚拟机上 （本虚拟实验环境为asp.net环境），结果截图。