

# CookieEdit插件安装与应用

## 实验目的

通过本实验理解Cookie在浏览器客户端访问服务器时的作用与安全风险，掌握Firefox浏览器插件的安装与使用方法，熟悉Chrome浏览器与Burpsuit软件进行代理抓包的设置与使用。

## 实验环境

渗透平台：Kali

用户名：college

密码：360College

工具：Burpsuite、Firefox

目标网站：DVWA

用户名：360college

密码：360College

工具：PHPStudy

## 实验原理

### (1) Cookie简介

Cookie指的是当你浏览某网站时，网站存储在你电脑上的一个小文本文件，伴随着用户请求和页面在 Web 服务器和浏览器之间传递。它记录了你的用户ID，密码、浏览过的网页、停留的时间等信息，用于用户身份的辨别。

因为HTTP协议是无状态的，对于一个浏览器发出的请求，服务器无法区分是不是同一个来源，无法知道上一次用户做了什么。所以，需要额外的数据用于维护会话。Cookie 正是这样的一段随HTTP请求一起被传递的额外数据，用于维护浏览器和服务器的会话。我们可以想象一个场景，你没有登录京东时在京东上购物，选择了3件商品放入购物车，在结算时，京东可以通过Cookie知道这三件商品是什么。

在网上，cookie篡改（cookie poisoning）是攻击者修改cookie（网站用户计算机中的个人信息）获得用户未授权信息，进而盗用身份的过程，攻击者可能使用此信息打开新账号或者获取用户已存在账号的访问权限。

### (2) Cookie Edit编辑工具简介

Cookie Bro插件是一款可以管理Firefox浏览器cookies的插件，浏览器保存用户信息到本地浏览器的方式都是使用cookies的方式，cookies虽然可以为用户的一些操作带来便捷，但也存在着隐私隐患，通过Cookie Bro浏览器cookies管理插件，用户可以利用它添加、删除、编辑、搜索、锁定和屏蔽cookies。

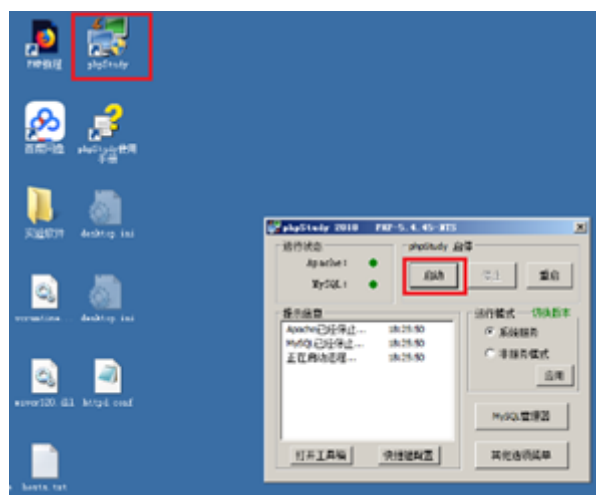
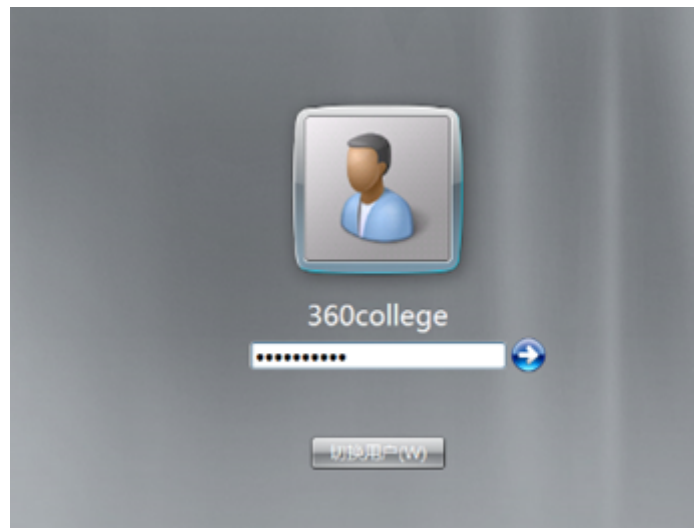
Cookie Bro可以实现编辑浏览器中已经存在的cookies，还可以在cookies创建的时候阻止它。也可以在浏览器中创建一个新的cookies，从其他地方导入导出cookies，或者是给当前的某个cookies加上一个时间期限来让它在一定时间后过期。

用户也可以在网站的cookies列表中直接删除相应的cookies，或者是彻底屏蔽该网站的cookies信息来防止一些恶意的网站抓取用户的信息。

## 实验步骤

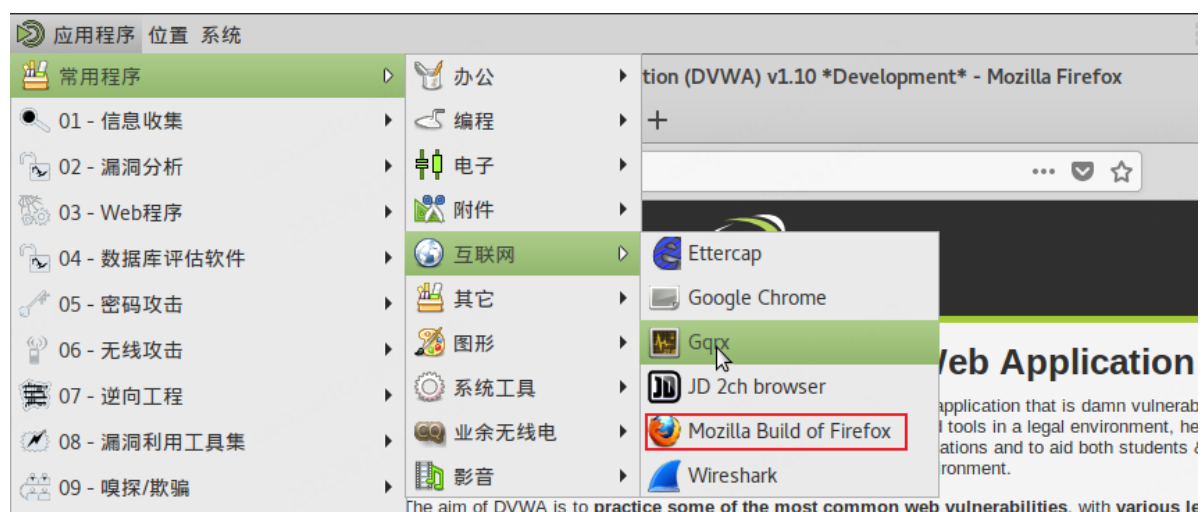
## 第一步 目标网站使用PHPStudy开启web服务

使用用户名:360college与密码:360College登录DVWA靶机，在桌面快捷方式中找到PHPStudy，双击启动web服务。

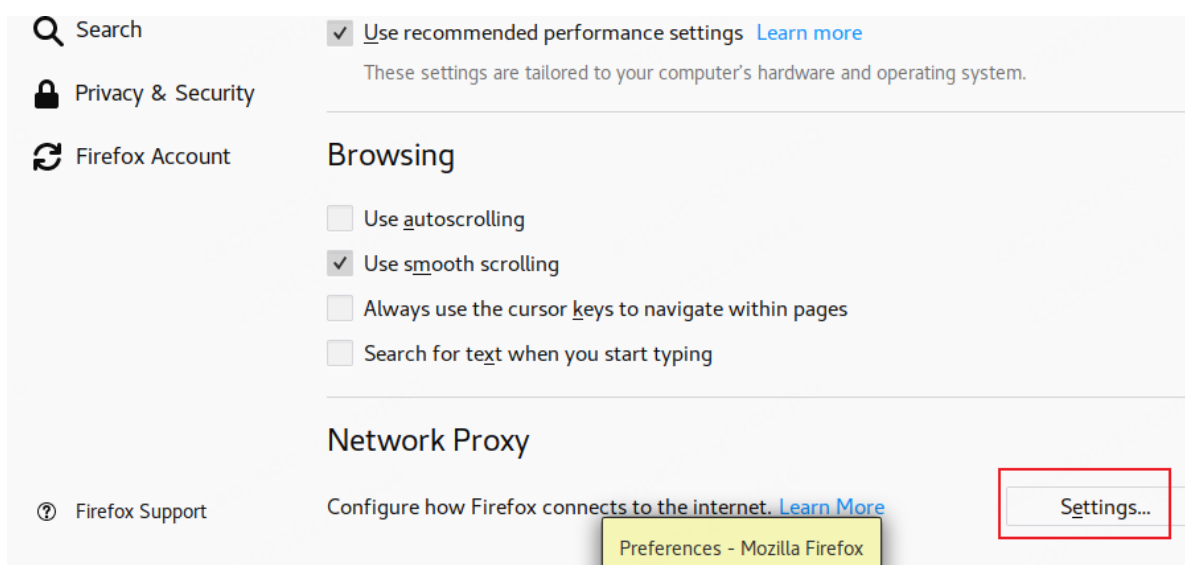
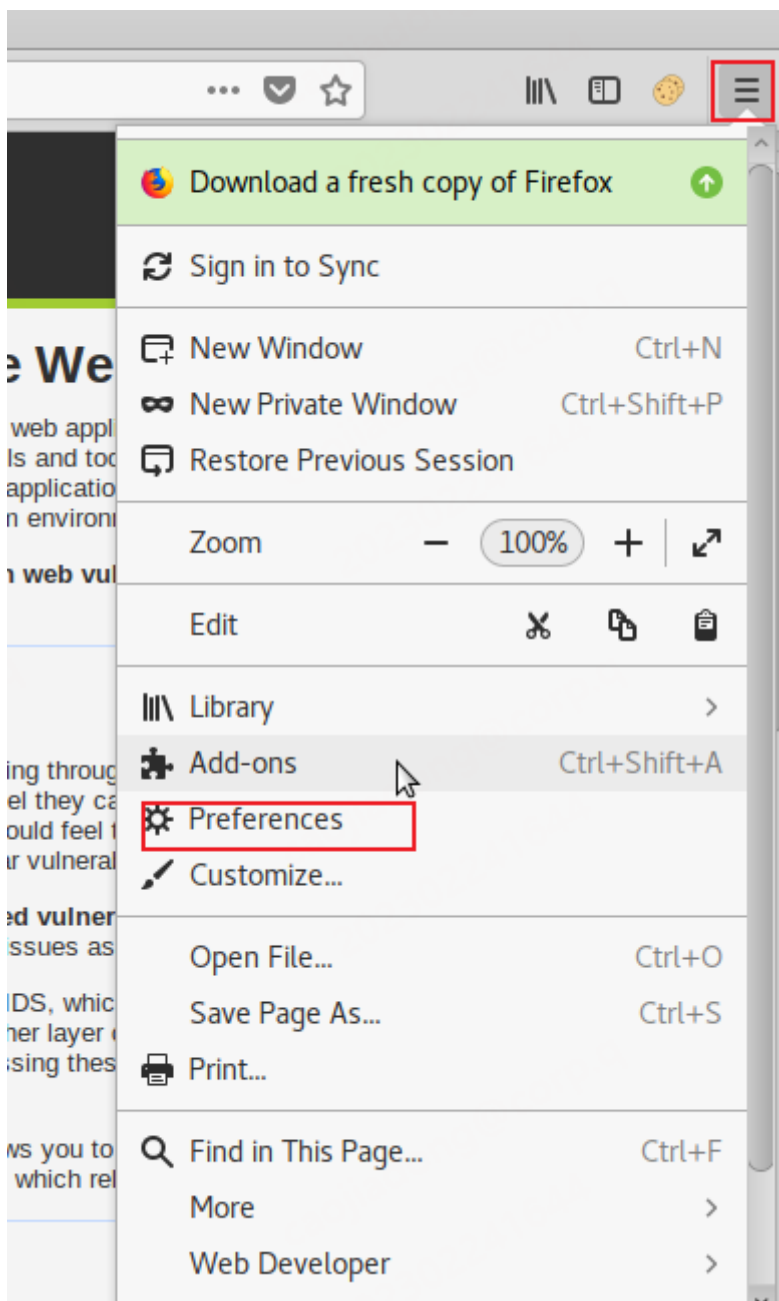


## 第二步 Kali平台上使用插件替换cookie

打开 Firefox 浏览器



关闭代理。



**Configure Proxy Access to the Internet**

☒ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☐ Manual proxy configuration

HTTP Proxy  Port

☐ Use this proxy server for all protocols

SSL Proxy  Port

FTP Proxy  Port

SOCKS Host  Port


☐ SOCKS v4 ☒ SOCKS v5

No Proxy for

[Help](#) [Cancel](#) [OK](#)

1. 访问 DVWA的IP: 8085 , 并输入账户密码。

192.168.10.11:8085/login.php

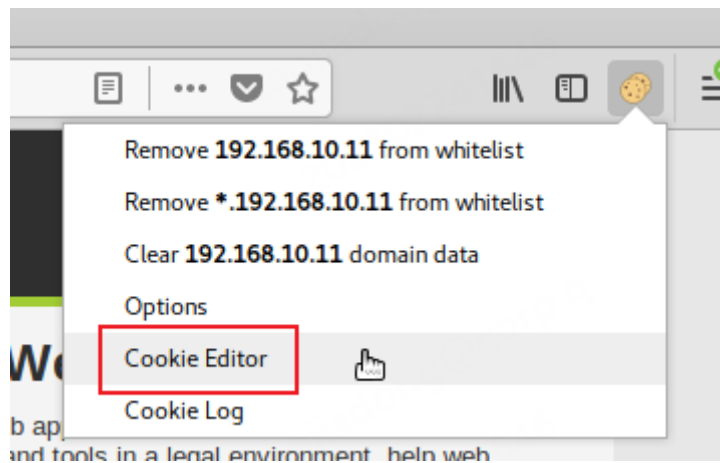


**Username**

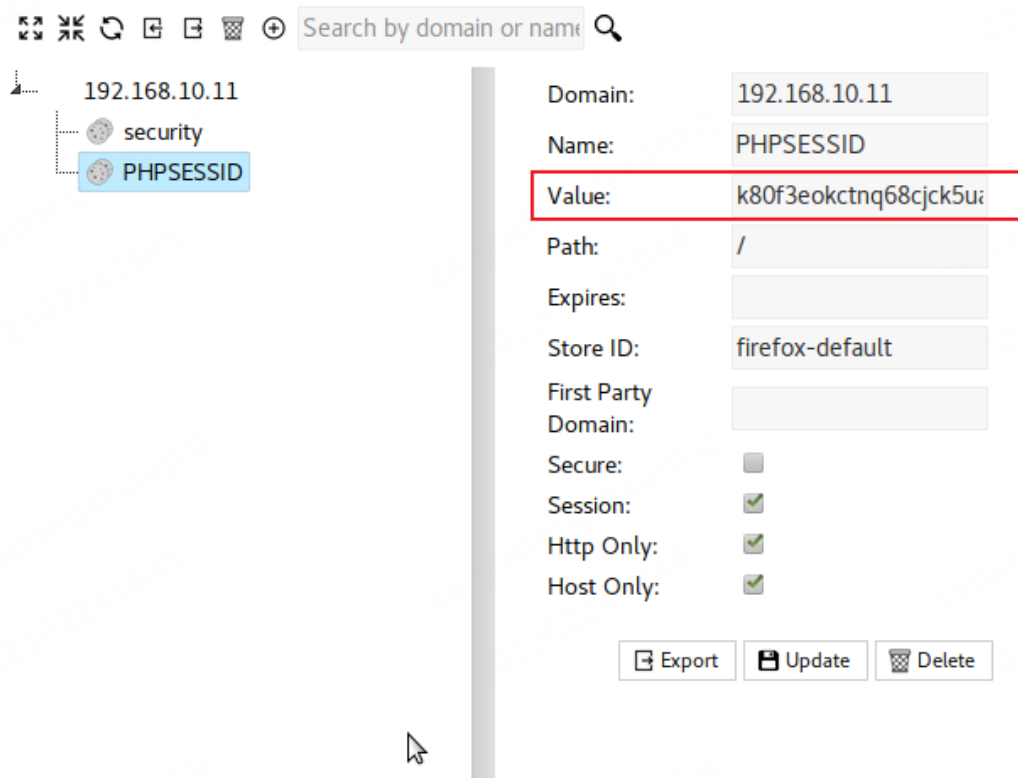
**Password**

[Login](#)

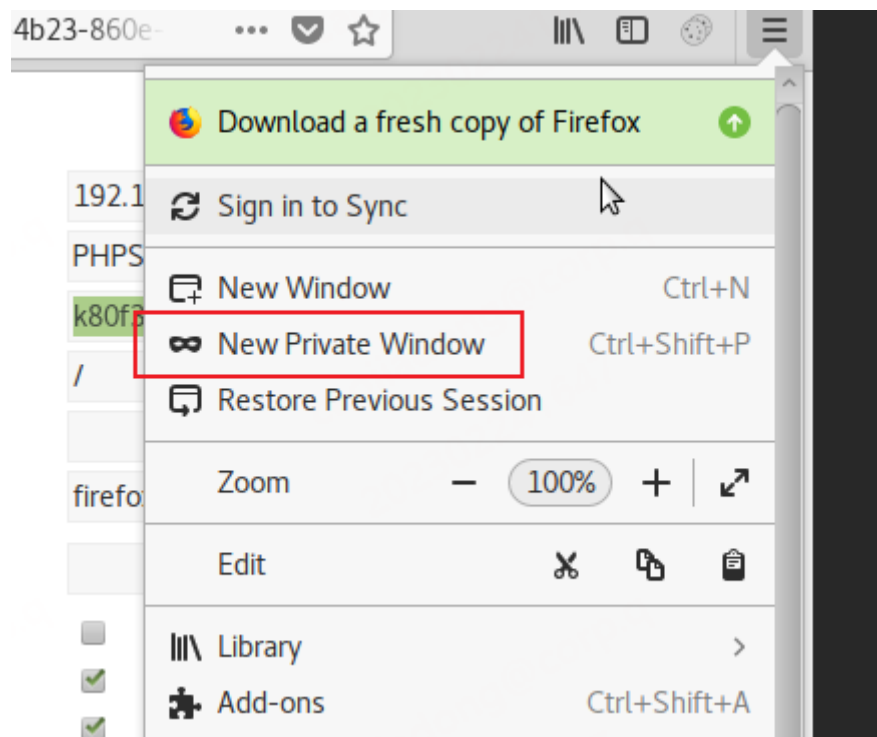
2. 登录成功使用插件查看cookie



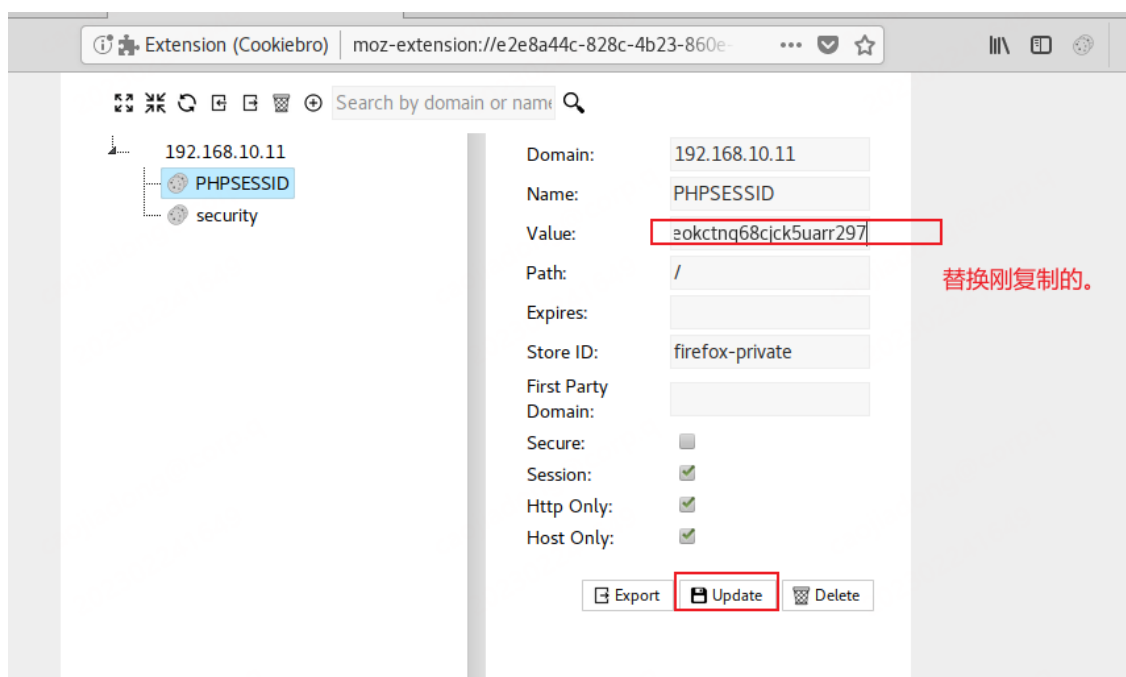
3. 复制cookie值。然后关闭cookie配置页面



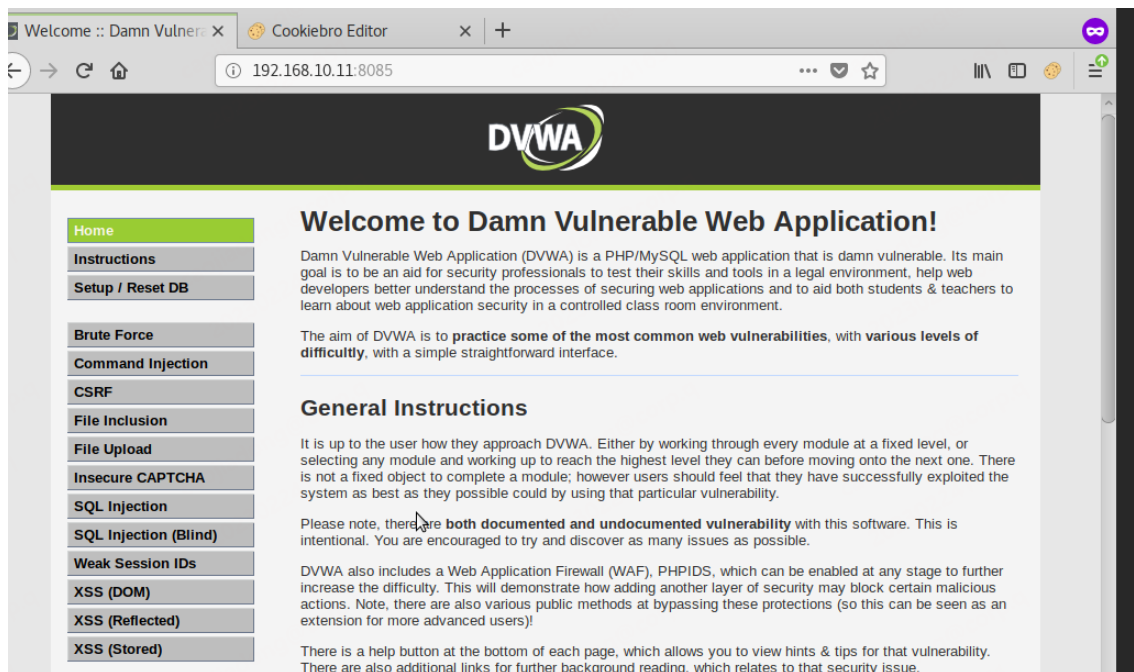
4. 开启隐身窗口。访问 DVWA的IP: 8085



5. 在隐身窗口点击插件，替换cookie值。



6. 刷新一下页面，去掉login.php 登录成功。



## 思考与总结

通过本次实验，成功实现了使用修改后的Cookie值绕过了用户名与密码验证登录到了目标网站，掌握了firefox浏览器插件的安装与使用，体验了cookie面临的安全风险。