信息安全实验报告

警示

1.实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2.当次小组成员成绩只计学号、姓名登录在下表中的。
3.在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4.实验报告文件以 PDF 格式提交。

院系	数据科学与计算机实验	班 级	14M3，14C1		组长	白冰
学号	14353355	14353002				
学生	杨金华	白冰				
实验分工						
杨金华	编写网页，进行欺骗，编写实验报告		白冰	设计实验场景，参与实验		

cookies 欺骗与防御实验

【实验目的】

了解 cookies 欺骗与防御的基本原理，掌握欺骗的几种途径，学会防御。

【实验原理】

Cookies 是浏览某网站时，由 Web 服务器置于你硬盘上的一个非常小的文本文件，它可以记录用户 ID、密码等敏感信息。当你再次来到该网站时，网站通过读取 Cookies，得知你的相关信息，就可以做出相应的动作，如不用输入 ID、密码就直接登录等等。因此，通过盗取别人的 Cookies，即可在没有获得密码的情况下登录别人的账号，如果盗取的是管理员账号，造成的危害更大。

【实验环境】

Windows 10，Chrome 浏览器

【实验要求】

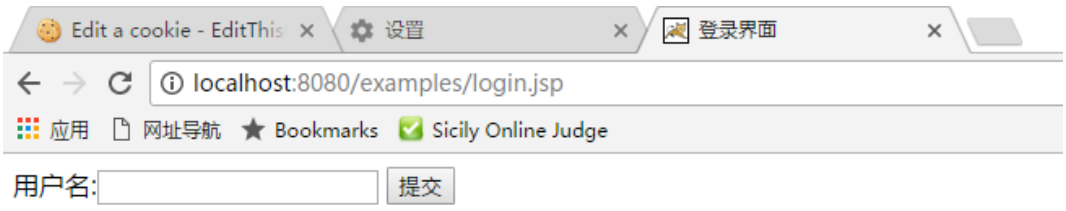
1. 设计实验场景，必要的话画出拓扑。

实验场景：某人登录某论坛（cookies 已经记录）后，发现一个很吸引人的链接，点击进去以后发现只有空白页，也不怎么在意就把网页给关了。

2. 适当选取实验对象，进行欺骗（详述方法），并将其截图。

由于当前很多网站和论坛都对 cookie 欺骗进行了防御，而且为了不给自己找来麻烦，我们自己用 JSP 编写了两个极为简单的网页，login.jsp 和 index.jsp. login.jsp 为登录界面，index.jsp 为登录后的欢迎界面（为了简便起见，只有用户名，没有密码、布局等复杂设计，已经足够完成本次实验），代码在后面会给出。

登录界面

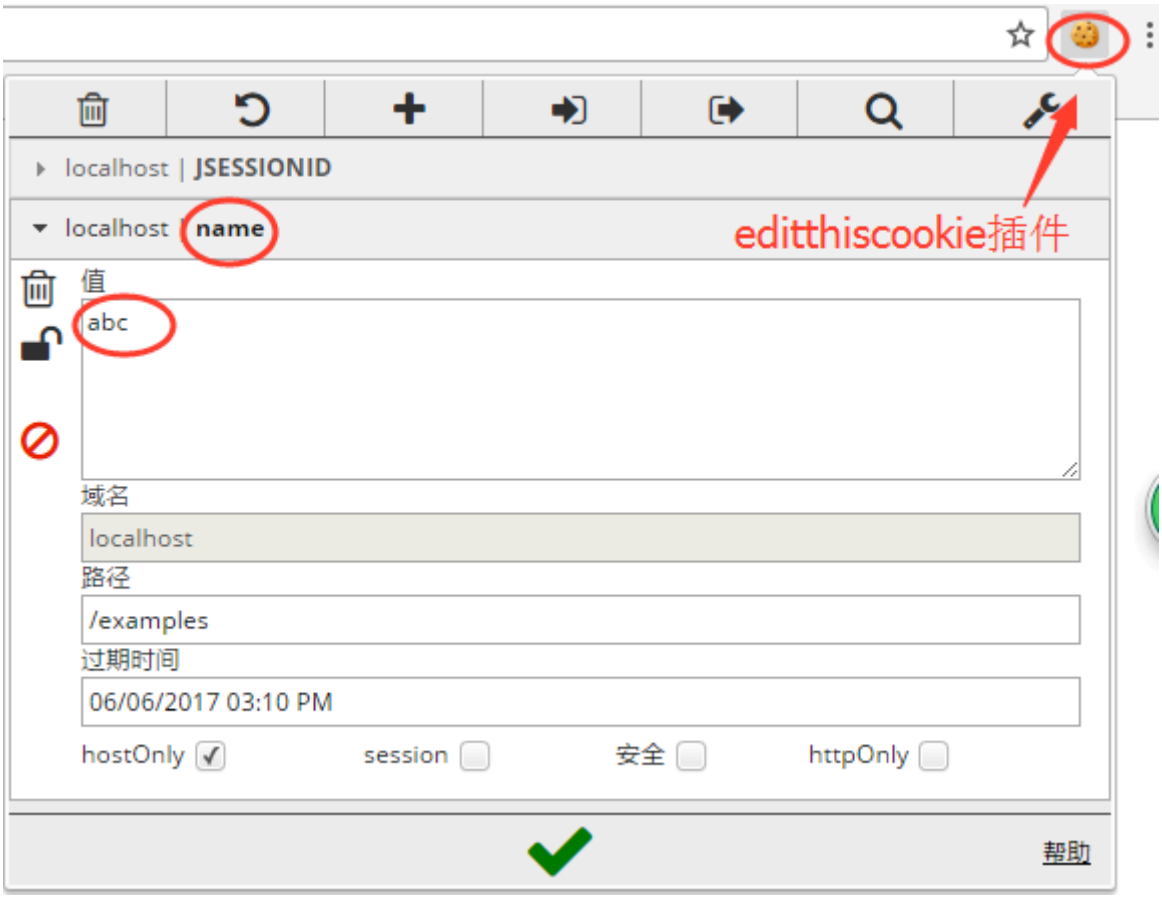


登录后的欢迎界面（abc 即为用户名）

欺骗过程：

我们通过 XSS 攻击（之前的实验有实现过）获得了某管理员的 cookies，假如他的账户名称为 bcd。在现实中，这些信息一般是由 MD5 进行加密，这里只是实验，就采用了明文，但操作是一样的。

首先，我们先登录自己在该网站上的账号，即上图显示。这里我们采用了 chrome 浏览器扩展程序商店里的 editthiscookies 插件，安装后，在该界面上点击它，得到以下界面。



这个时候，我们把值里面的 abc 改成管理员的账号 bcd（真实攻击也只要改成通过 XSS 攻击获得的 cookie 即可），点击下面的 √ 保存即可。

最后，我们只要刷新界面，就会发现，我们已经以管理员身份登录了该网站，可以做自己想要做的事情了。

3. 验证欺骗，观察防火墙对其反应情况，说明原因。

防火墙无反应。因为本人在 Windows 防火墙里允许浏览器访问专用和公用网络。

4. 针对欺骗者，设计防御方法，并进行验证。

禁用 cookies。则欺骗者无法获得 cookies，所以无法进行 cookie 欺骗。

5. 提出 **cookies 欺骗的一般防御**策略。

在网站建立者的角度上，必须完善网站的防御系统，最好安装 web 应用防火墙。针对 cookies 欺骗，可采用 cookie+ip 认证或 cookie+session 混合存储等手段，不能只依赖 cookie 进行验证。

在用户自身角度上，不要在网吧等公共场合上保存 cookie，不要随意点击来历不明的链接或者一些故意吸引眼球的链接，以防 cookie 被盗。

6. 写出实验体会。

通过本次实验，我们感受到了 cookies 给我们带来便利的同时，也给我们带来了一些潜在的安全隐患。MD5 加密虽然保证了我们的账号密码不能被直接获取，但在一些防御措施不够的网站上，这些看似乱码的东西却也能顺利登录我们的账号。所以我们在网络使用中，一定要注意保护自己的账号安全。

以下附上实验中用到的代码：

```
<%@ page language="java" contentType="text/html; charset=UTF-8"
    pageEncoding="UTF-8"%>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>登录界面</title>
</head>
<body>
    <form action="index.jsp" method="post">
        用户名:<input type="text" name="name"/>
        <input type="submit" value="提交"/>
    </form>
</body>
</html>
```

Login.jsp

信息安全实验报告

```jsp
<%@ page language="java" contentType="text/html; charset=UTF-8"
    pageEncoding="UTF-8"%>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>欢迎您</title>
</head>
<body>
    <%
        String name = request.getParameter("name");
        if(name != null && !name.trim().equals("")){
            Cookie cookie = new Cookie("name",name);
            cookie.setMaxAge(3000); //设置cookie有效期为30s
            response.addCookie(cookie);
        }else{
            Cookie[] cookies = request.getCookies();
            if(cookies != null && cookies.length > 0){
                for(Cookie cookie:cookies){
                    String cookieName = cookie.getName();
                    if("name".equals(cookieName)){
                        String val = cookie.getValue();
                        name = val;
                    }
                }
            }
        }
        if(name != null && !name.trim().equals("")){
            out.print("hello: " + name);
        }else{//否则重定向到登录界面
            response.sendRedirect("login.jsp");
        }
    %>
</body>
```

Index. jsp

【交实验报告】

上传实验报告：ftp://222.200.180.109/ 截止日期（不迟于）：两周完成

上传小组实验报告。上传文件名格式：小组号_ 防火墙管理实验.pdf （由组长负责上传）

例如：文件名“6_ 防火墙管理实验.pdf”表示第 6 组的防火墙管理实验报告

注意：不要打包上传！