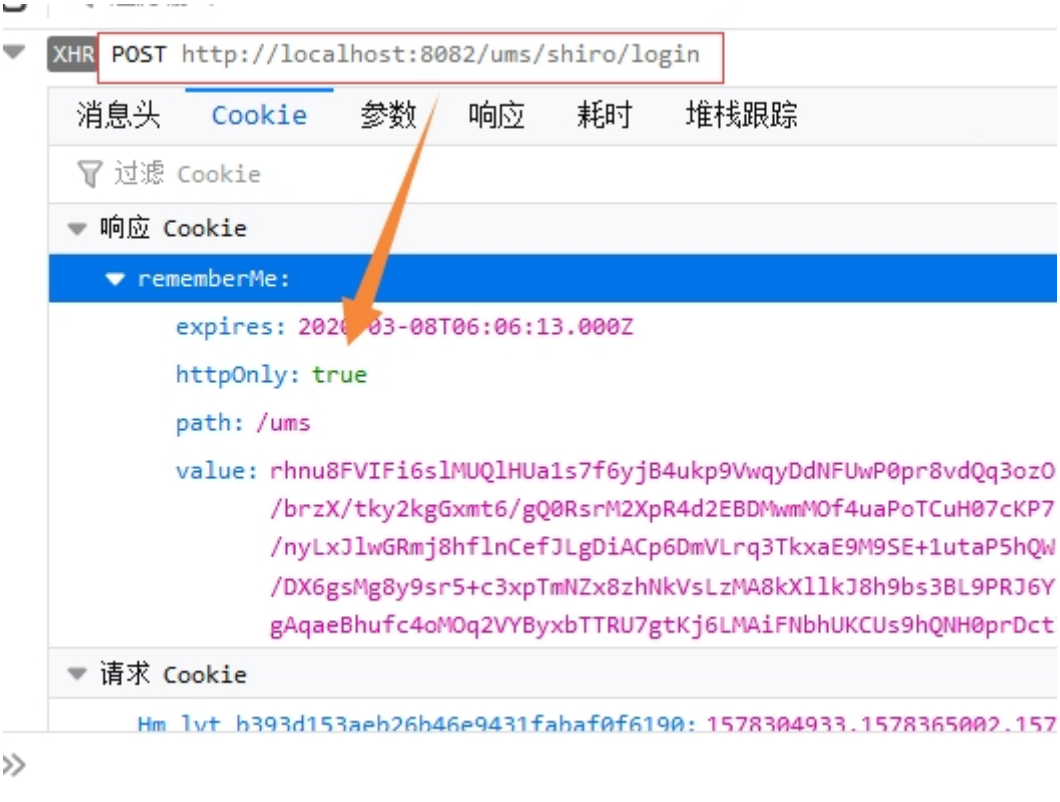
Day27　WEB漏洞–XSS跨站之代码及httponly绕过

27.1 什么是HttpOnly?

如果HTTP响应头中包含HttpOnly标志，只要浏览器支持HttpOnly标志，客户端脚本就无法访问cookie。因此，即使存在跨站点脚本（XSS）缺陷，且用户意外访问利用此漏洞的链接，浏览器也不会向第三方透露cookie。如果浏览器不支持HttpOnly并且网站尝试设置HttpOnly cookie，浏览器会忽略HttpOnly标志，从而创建一个传统的，脚本可访问的cookie。



27.2 JavaEE的API是否支持?

目前sun公司还没有公布相关的API，但PHP、C#均有实现。搞javaEE的兄弟们比较郁闷了，别急下文有变通实现。

27.3 HttpOnly的设置样例

JavaEE:

```
response.setHeader("Set-Cookie",
"cookiename=value;
Path=/;Domain=domainvalue;Max-
Age=seconds;HTTPOnly");
//具体参数的含义再次不做阐述，设置完毕后通过js脚本是读不到该cookie的，但使用如下方式可以读取Cookie
cookies[]=request.getCookies();
```

C#:

```
HttpCookie myCookie = new HttpCookie("myCookie");
myCookie.HttpOnly = true;
Response.AppendCookie(myCookie);
```

VB.NET:

```
Dim myCookie As HttpCookie = new
HttpCookie("myCookie")
myCookie.HttpOnly = True
Response.AppendCookie(myCookie)

但是在.NET1.1中需要手动添加
Response.Cookies[cookie].Path += ";HTTPOnly";
```

PHP4:

```
header("Set-Cookie: hidden=value; httpOnly");
```

PHP5：

```
1  setcookie("abc", "test", NULL, NULL, NULL, NULL,
   TRUE)
2  最后一个参数为httponly属性
```

参考资料：

```
1  http://www.owasp.org/index.php/HTTPOnly
2  转自：http://yzd.iteye.com/blog/787190
3  http://www.oschina.net/question/100267_65116
```

将cookie设置成HttpOnly是为了防止XSS攻击，窃取cookie内容，这样就增加了cookie的安全性，即便是这样，也不要将重要信息存入cookie。如何在Java中设置cookie是HttpOnly呢?

Servlet 2.5 API 不支持 cookie设置HttpOnly 建议升级Tomcat7.0，它已经实现了Servlet3.0但是苦逼的是现实是，老板是不会让你升级的。

那就介绍另外一种办法：

利用HttpResponse的addHeader方法，设置Set-Cookie的值cookie字符串的格式：key=value; Expires=date; Path=path; Domain=domain; Secure; HttpOnly

```
//设置cookie
response.addHeader("Set-Cookie", "uid=112; Path=/; HttpOnly");
//设置多个cookie
response.addHeader("Set-Cookie", "uid=112; Path=/; HttpOnly");
response.addHeader("Set-Cookie", "timeout=30; Path=/test; HttpOnly");
//设置https的cookie
response.addHeader("Set-Cookie", "uid=112; Path=/; Secure; HttpOnly")
//在实际使用中，我们可以使FireCookie查看我们设置的Cookie是否是HttpOnly
```

27.4 使用HttpOnly减轻最常见的XSS攻击

根据微软Secure Windows Initiative小组的高级安全项目经理Michael Howard的说法，大多数XSS攻击的目的都是盗窃cookie。服务端可以通过在它创建的cookie上设置HttpOnly标志来缓解这个问题，指出不应在客户端上访问cookie。客户端脚本代码尝试读取包含HttpOnly标志的cookie，如果浏览器支持HttpOnly，则返回一个空字符串作为结果。这样能够阻止恶意代码（通常是XSS攻击）将cookie数据发到攻击者网站。

27.5 用好Web应用防火墙

如果代码更改不可行或成本太高，可以使用Web应用程序防火墙将HttpOnly添加到会话cookieMod_security - using SecRule and Header directivesESAPI WAF - using add-http-only-flag directive支持HttpOnly的主流浏览器有哪些呢？谷歌了解一下，常见的浏览器都支持。

27.6 HttpOnly绕过

- 浏览器未保存帐号密码：需要xss产生登录地址，利用表单劫持
- 浏览器保存帐号密码：浏览器读取帐号密码

27.7 XSS练习靶场

详情参考XSSlabs靶场笔记

资源：

```
https://github.com/do0dl3/xss-labs
https://www.cr173.com/soft/21692.html
https://www.oschina.net/question/100267_65116
```