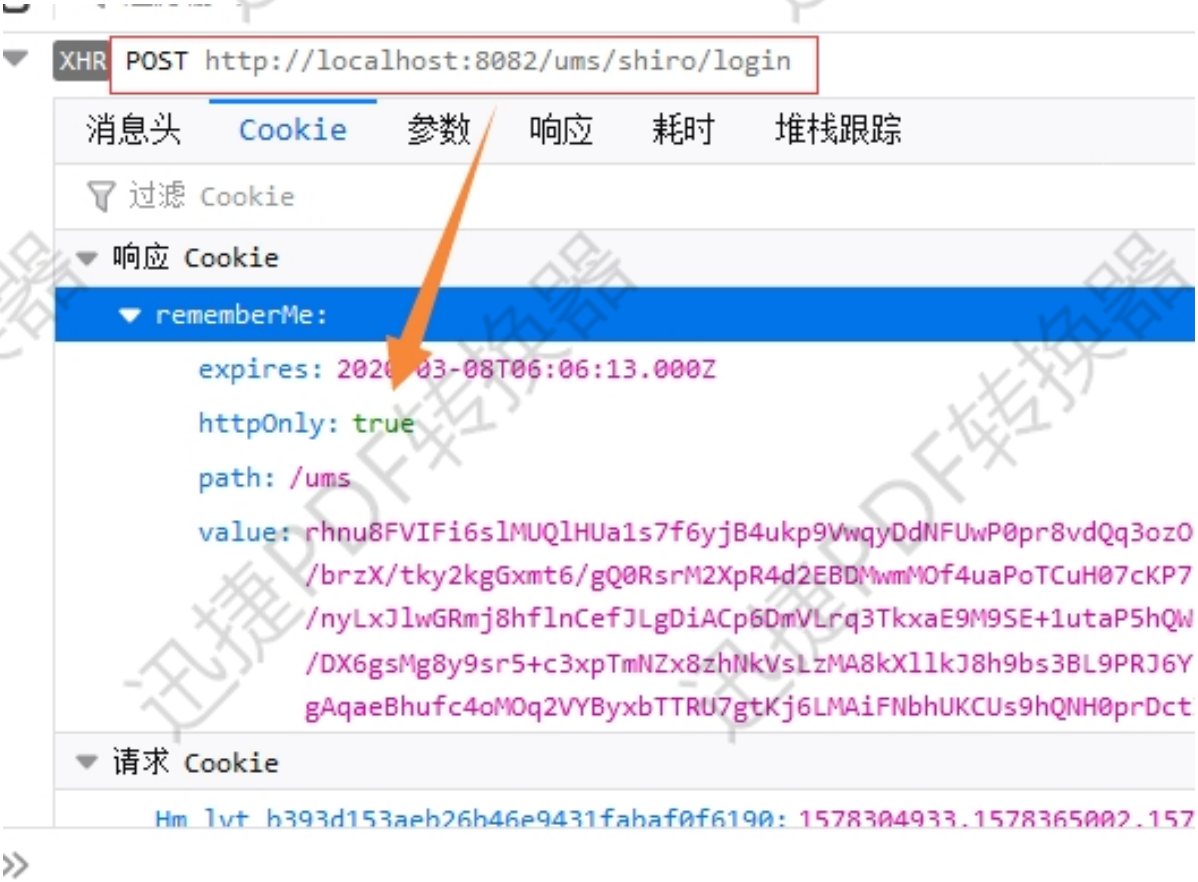
WEB 漏洞-XSS 跨站之代码及 httponly 绕过



代码类过滤：Xsslabs
HttpOnly 属性过滤防读取
<script>alert(1)</script>

绕过 httponly：
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

演示案例：

- HttpOnly 安全过滤测试
- HttpOnly 安全过滤绕过思路
- Xsslabs 关卡代码过滤绕过测试

涉及资源：

https://github.com/do0dl3/xss-labs

https://www.cr173.com/soft/21692.html

https://www.oschina.net/question/100267_65116
