# 27 WEB漏洞-XSS跨站之代码及httponly绕过



代码类过滤：Xss-labs

HttpOnly属性过滤防读取

<script>alert(1)</script>

1

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：产生在后台的xss，存储型xss如留言等，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

➢ Xss-labs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