web安全评测解决方案与代码编写规范

这里给出一些防范XSS 攻击的措施。必须说明的是，对于XSS 攻击，并不像SQLInjection 那样可以有一劳永逸的解决方案——只需要grep 一下所有的sql 调用。这是一场长期的斗争，而且往往需要我们采取修改业务流程、产品设计等看似削足适履的手段。  
  
先总结一下常见的攻击手法：  
  
1. 依赖跨站漏洞，需要在被攻击网站的页面种入脚本的手法  
  
1.1. Cookie 盗取，通过javascript 获取被攻击网站种下的cookie，并发送给攻击者。  
  
1.1.1. 从cookie 中提取密码等隐私  
  
1.1.2. 利用cookie 伪造session，发起重放攻击  
  
1.2. Ajax 信息盗取，通过javascript 发起ajax 请求。  
  
1.2.1. 从ajax 结果中获取隐私。  
  
1.2.2. 模拟用户完成多页表单。  
  
2. 不依赖跨站漏洞的手法  
  
2.1. 单向HTTP 动作，通过img.src 等方法发起跨站访问，冒充被攻击者执行  
  
特权操作。但是很难拿到服务器的返回值。  
  
2.2. 双向HTTP 动作，如果服务器产生一段动态的script，那么可以用  
  
script.src 的方法发起跨站访问并拿到服务器的返回值。  
  
防范手法如下：  
  
1. 防堵跨站漏洞，阻止攻击者利用在被攻击网站上发布跨站攻击语句

不可以信任用户提交的任何内容，首先代码里对用户输入的地方和变量都需要仔细检查长度和对”<”,”>”,”;”,”’”等字符做过滤；其次任何内容写到页面之前都必须加以encode，避免不小心把html tag 弄出来。这一个层面做好，至少可以堵住超过一半的XSS 攻击。  
  
2. Cookie 防盗  
  
首先避免直接在cookie 中泄露用户隐私，例如email、密码等等。其次通过使cookie 和系统ip 绑定来降低cookie 泄露后的危险。这样攻击者得到的cookie 没有实际价值，不可能拿来重放。  
  
3. 尽量采用POST 而非GET 提交表单  
  
POST 操作不可能绕开javascript 的使用，这会给攻击者增加难度，减少可利用的跨站漏洞。  
  
4. 严格检查refer  
  
检查http refer 是否来自预料中的url。这可以阻止第2 类攻击手法发起的http 请求，也能防止大部分第1 类攻击手法，除非正好在特权操作的引用页上种了跨站访问。  
  
5. 将单步流程改为多步，在多步流程中引入效验码  
  
多步流程中每一步都产生一个验证码作为hidden 表单元素嵌在中间页面，下一  
  
步操作时这个验证码被提交到服务器，服务器检查这个验证码是否匹配。  
  
首先这为第1 类攻击者大大增加了麻烦。其次攻击者必须在多步流程中拿到上  
  
一步产生的效验码才有可能发起下一步请求，这在第2 类攻击中是几乎无法做  
  
到的。  
[web安全评测解决方案与代码编写规范\_文档下载](http://www.wendangxiazai.com/b-e453dd9828ea81c759f57821-8.html)http://www.wendangxiazai.com/b-e453dd9828ea81c759f57821-8.html