php代码审计基础篇

第5课 csrf

漏洞介绍

CSRF漏洞

CSRF(Cross-site request forgery)跨站请求伪造：攻击者诱导受害者进入第三方网站，在第三方网站中，向被攻击网站发送跨站请求。利用受害者在被攻击网站已经获取的注册凭证，绕过后台的用户验证，达到冒充用户对被攻击的网站执行某项操作的目的。

CSRF则通过伪装来自受信任用户的请求来利用受信任的网站。与XSS攻击相比，CSRF攻击往往不大流行(因此对其进行防范的资源也相当稀少)和难以防范

csrf漏洞的成因就是网站的cookie在浏览器中不会过期，只要不关闭浏览器或者退出登录，那以后只要是访问这个网站，都会默认你已经登录的状态。而在这个期间，攻击者发送了构造好的csrf脚本或包含csrf脚本的链接，可能会执行一些用户不想做的功能(比如是添加账号等)。这个操作不是用户真正想要执行的

漏洞防范

防御CSRF漏洞的最主要问题是解决可信的问题，即使是管理员权限提交到服务器的数据，也不一定是完全可信的，所以针对CSRF的防御有以下两点：1)增加token或者referer验证避免img标签请求的水坑攻击，2)增加验证码。

Token翻译中文为“标志”,在计算机认证领域叫令牌。利用验证Token的方式是目前使用的最多的一种，也是效果最好的-种，可以简单理解成在页面或者cookie里面加一个不可预测的字符串，服务器在接收操作请求的时候只要验证下这个字符串是不是上次访问留下的即可判断是不是可信请求，因为如果没有访问上一个页面，是无法得到这个Token的，除非结合XSS漏洞或者有其他手段能获得通信数据。

验证HTTP Referer字段

根据HTTP协议，在HTTP头中有一个字段叫Referer,它记录了该HTTP请求的来源地址。在通常情况下，访问一个安全受限

页面的请求必须来自于同一个网站

漏洞挖掘思路

寻找敏感操作地方

查找php代码是否存在防护措施

php代码审计

实例代码分析

cms的后台添加管理员账号

某cms的数据库备份

cnvd追溯

谢谢观赏