php代码审计基础篇

第4课 xss

php代码审计xss漏洞

漏洞介绍

xxs学名为跨站脚本攻击

跨站脚本攻击是指恶意攻击者往Web页面里插入恶意Script代码，当開户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的目的。

xss漏洞通常是通过php的输出函数将javascript代码输出到html页面中，通过用户本地浏览器执行的，所以xss漏洞关键就是寻找参数未过滤的输出函数

反射性xss和存储型xss漏洞

第一种是通过外部输入然后直接在浏览器端触发，即为反射性xss

第二种是先把利用的代码保存在数据库或者文件中，

当web程序读取利用代码并且输出在页面上时候触发漏洞，也就是存储xssxss可以进行钓鱼，盗取cookie等等操作

防护

一般xss漏洞都是因为没有过滤特殊字符

htmlspecialchars()函数把预定义的字符转换为HTML实体。

预定义的字符是：　　&(和号)成为&　　“(双引号)成为"　　‘(单引号)成为'

<(小于)成为<　　>(大于)成为>

替换，匹配htmlentities()函数，用于转义处理在页面上显示的文本

str_replace()函数以其他字符替换字符串中的一些字符

preg_replace函数执行一个正则表达式的搜索和替换。

黑名单过滤，白名单过滤

漏洞挖掘思路

用户可控输入，有过滤函数，无过滤函数，可绕过

白盒审计中

我们首先要寻找带参数的输出函数，接下来通过输出内容回溯到输入参数，看有没有过滤函数寻找未过滤的输入点和未过滤的输出函数

黑盒配合白盒

表单提交

留言板，注册界面，发消息，填个人信息等等，一切用户可控的输入地方。

php代码审计xss漏洞

实例代码分析

后台xss

前台xss

工具

seay ,burp,phpstudy

下载地址

http://www.pcfinal.cn/channel/ecms.html

http://175.6.244.211:88/code/200912/bluecms.rar

谢谢观赏