基本信息

漏洞类型：URL跳转漏洞

漏洞等级：低危

厂商信息：此处需要手动搜索

漏洞简述

漏洞描述

url跳转漏洞是指后台服务器在告知浏览器跳转时，未对客户端传入的重定向地址进行合法性校验，导致用户浏览器跳转到钓鱼页面的一种漏洞。

漏洞危害

1.服务端未对传入的跳转url变量进行检查和控制，可能导致可恶意构造任意一个恶意地址，诱导用户跳转到恶意网站。  
 2.由于是从可信的站点跳转出去的，用户会比较信任，所以跳转漏洞一般用于钓鱼攻击，通过转到恶意网站欺骗用户输入用户名和密码盗取用户信息，或欺骗用户进行金钱交易；还可以造成xss漏洞。

漏洞详情

网站漏洞报表

漏洞网址:http://lib.scnu.edu.cn/dzzy2/dzzy\_open-n.asp?id=248&url=http%3A%2F%2Fwww.langzi.fun

网站信息报表

百度权重 3

网站主页 http://lib.scnu.edu.cn

网站描述 "" /

网站标题 华南师范大学图书馆

IP\_\_坐标 广东省 电信

所属\_\_IP 121.8.171.26

网站年龄 6年4月（创建于2013年01月17日,过期时间为2018年01月17日)

备案编号 粤ICP备05008875号-1

备案性质 事业单位

备案名称 华南师范大学

备案时间 2005/4/25 0:00:00

百度收录 暂无信息

协议类型 HTTP/1.1 200 OK

页面类型 text/html

服务类型 CloudWAF

程序语言 -

网站漏洞复现(使用Firefox浏览器)

访问链接

http://lib.scnu.edu.cn/dzzy2/dzzy\_open-n.asp?id=248&url=http%3A%2F%2Fwww.langzi.fun

返回结果



复现完成，验证存在URL跳转漏洞

修复建议

代码原理防护

1.若跳转的URL事先是可以确定的，包括url和参数的值，则可以在后台先配置好，url参数只需传对应url的索引即可，通过索引找到对应具体url再进行跳转；  
 2.若跳转的URL事先不确定，但其输入是由后台生成的（不是用户通过参数传人），则可以先生成好跳转链接然后进行签名，而跳转cg首先需要进行验证签名通过才能进行跳转；  
 3.若1和2都不满足，url事先无法确定，只能通过前端参数传入，则必须在跳转的时候对url进行按规则校验：即控制url是否是你们公司授权的白名单或者是符合你们公司规则的url：  
 function checkURL ( sURL) {  
 return (/^(https?:\/\/)?[\w-.]+.(yourDomainA|yourDomainB|yourDomainC).com($|\/|\)/i).test(sUrl)||(/^[\w][\w\/.-\_%]+$/i).test(sUrl)||(/^[\/\][^\/\]/i).test(sUrl) ? true : false;  
 }