【封神台】cookie伪造目标权限

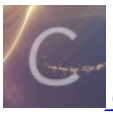
原创

00勇士王子 于 2021-11-17 14:56:05 发布 132 收藏

分类专栏： web CTF 漏洞复现 文章标签： web安全


web 同时被 3 个专栏收录

18 篇文章 0 订阅
订阅专栏


CTF

22 篇文章 1 订阅
订阅专栏


漏洞复现

45 篇文章 14 订阅
订阅专栏

题目

解题过程

访问网站，是一个留言板

先用普通的xss测试一下

成功弹窗，说明地处存在xss漏洞

选择一个在线的xss平台，创建项目后输入平台的xss代码（我随便在网上找了一个xss平台如下：https://xss8.cc）

原理就是当管理员查看留言页面时触发xss,将管理员的cookie发送到该平台上面，从而实现利用管理员的cookie进行伪造目标权限

因为xss bot 每10秒访问一次页面，相当于管理员每10秒看一次留言，触发一次xss代码，所以在10秒后，xss平台接收到了目标的cookie，在其中读取到了flag

+全部	时间	接收的内容	Request Headers	操作
-折叠	2021-11-17 14:47:37	• location : http://59.63.200.79:8004/FeedbackView.asp • toplocation : http://59.63.200.79:8004/FeedbackView.asp • cookie : ASPSESSIONIDACQTQQAS=LEOJFAODCJCELLLDEIDOIHIE; flag=zkz{xsser-g00d}; ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC	• HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34 • REMOTE_ADDR : 59.63.200.79 • IP-ADDR : 操作系统：Windows 7 浏览器：Safari(版本:unknown)	删除

- title : 掌控安全学院实战演练靶场
- charset : GB2312
- platform : Win32
- screen : 1920x1080
- htmlyuanma :

```
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<title>掌控安全学院实战演练靶场</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<meta content="掌控安全学院实战演练靶场" name="keyword
```

- origin : http://59.63.200.79:8004

因为是靶场，我们的目标就是获取flag，真实情况下我们可以使用这个cookie尝试进行登录，从而伪造管理员的身份进行登录。