封神台的困难与复现

原创

Clancy_ 于 2020-11-29 11:10:00 发布 82 收藏
分类专栏： 靶机 # 封神台 文章标签： 靶机


靶机 同时被 2 个专栏收录
1 篇文章 0 订阅
订阅专栏


封神台
1 篇文章 0 订阅
订阅专栏

第二章：遇到阻难！绕过WAF过滤！

1. 我们尝试，将测试语句放到cookie里面，再发送给服务器，因为网页防护一般只拦截Get、post传参。
2. 我们打开火狐浏览器，这里用到了ModHeader插件
3. 我们点击+号新增一个Request头。
4. 我们添加一个Cookie头，并写值为id=171，并确保已开启（打勾）
5. 我们直接访问http://59.63.200.79:8004/shownews.asp返回显示正常
6. 这证明cookie里的id=171，也能正常传参，被当作sql语句拼接。那我们直接进行注入。
7. 我们输入Cookie值为：id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin(这是ACCESS数据库的语法)
8. 继续猜测是否存在admin表（+号代替空格，不然会出错）发现页面回显了2、3、7、8、9。
9. 没有出现数据库错误，这证明admin表是存在的。且第2、第3、7、8、9字段，可以用来猜测字段名，同时，可以直接回显在页面上。
10. 我们接着尝试猜测最常见的管理表字段名Username和Password，我们在2、3、7、8、9中任选两个，分别填入Username和Password
11. id=171+union+select+1,username,password,4,5,6,7,8,9,10+from+admin
12. 接着刷新页面，发现页面返回了admin表中，username和password字段的值：admin、b9a2a2b5dffb918c
13. 这应该就是管理员用户名和密码了，但管理员密码看起来有些奇怪。字母+数字的16位组合，很像md5的特征。将b9a2a2b5dffb918c进行解密。
14. 尝试打开后台：http://59.63.200.79:8004/admin/出现管理员登录页面，输入用户名admin、密码welcome，填写验证码。