攻防世界web新手writeup

原创

花少。 于 2019-11-03 16:31:31 发布 129 收藏

分类专栏： ctf

本文链接：https://blog.csdn.net/qq_42912607/article/details/102883357

1，view_source

F12查看源代码，注释中获取flag

2，get_post

get提交a=1

火狐hackbar工具Post提交后获得flag

3，robots

robots.txt后

f1ag_1s_h3re.php

4，backup

提示index.php的备份文件

后缀为.bak

下载后记事本打开获取flag

5，cookie

burp抓包需要cookie.php，

加载Url后让看响应包

抓包送到repeater,go 响应包中获得flag。

6，disabled_button

检查按钮元素，发现disabled 删除后点击按钮获得flag

7，simple_js

抓包发现没有拦到，本地js验证

查看源码，发现一串16进制，转换后获得flag

8，xff_referer

burp抓包后送到repeater
加X-Forwarded-For为127.0.01
后发现要来自谷歌 增加referer
go

9，weak_auth

burp抓包，送到intruder爆破，已经提示username为admin
爆破出密码为123456

10，webshell

菜刀连接 密码为shell
获取flag

11，command_execution

用此寻找flag地址
127.0.0.1;find / -name “flag.txt”
后cat 获取flag

12，simple_php

is_numeric() 函数用于检测变量是否为数字或数字字符串。
?a==0&b=123456aaaaaaaaaaa绕过
得到flag