ctf题目复盘

原创

萍水间人 于 2019-04-07 21:13:21 发布 1145 收藏 1

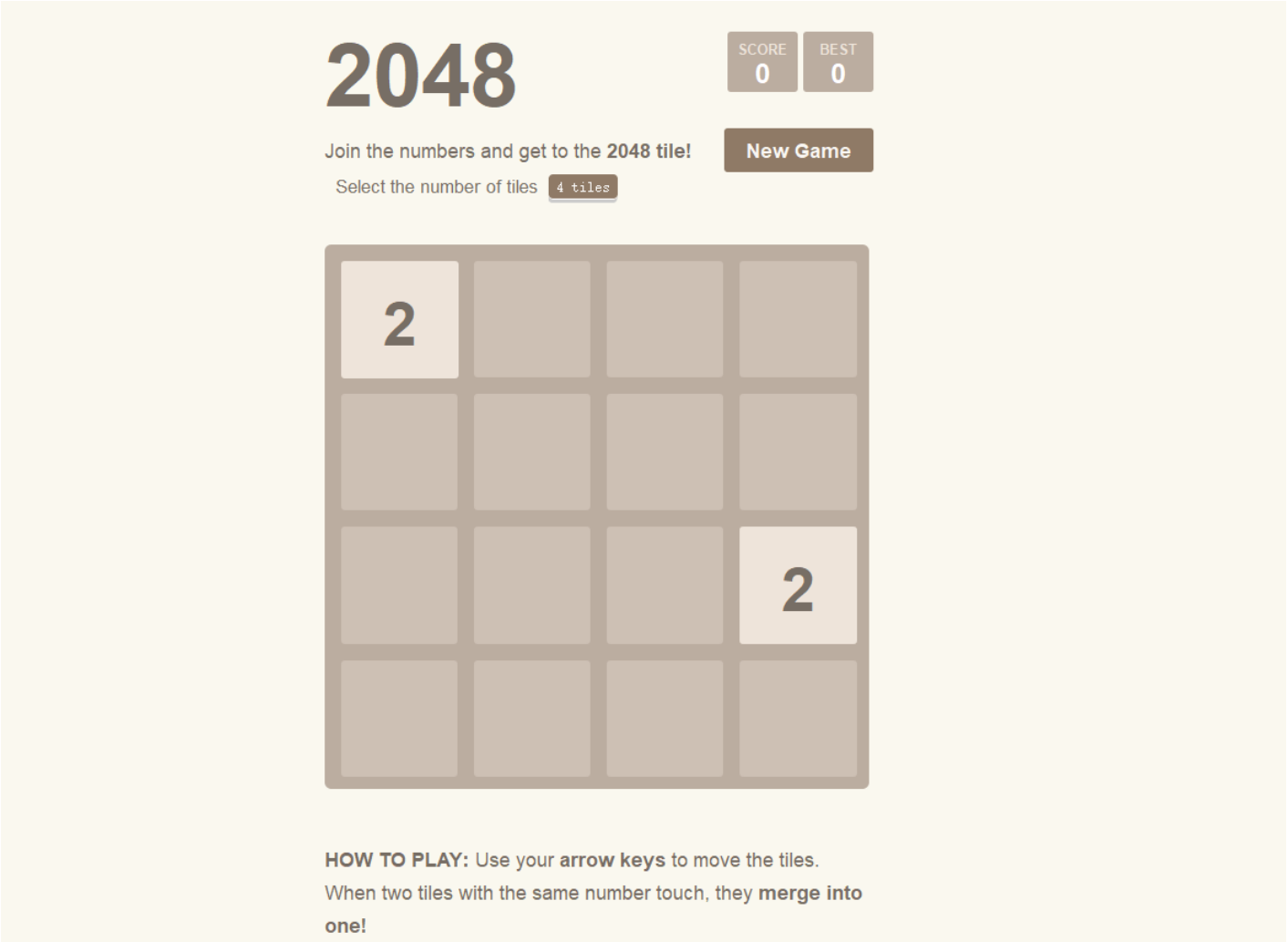
> 为了准备四月下旬的校赛， 豁出去了

2048

首先进去之后是这样一个界面

2048是我喜欢的一个游戏，

然后我女朋友把它玩到了2048， 却啥也没出现。。



网站做的很流畅， 但是我一点思路都没有

开始抓包

```
GET /js/keys.js HTTP/1.1
Host: 192.168.41.145:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.41.145:10000/
Connection: close
If-Modified-Since: Mon, 19 May 2014 14:01:22 GMT
If-None-Match: "fc8-4f9c132bb9080-gzip"
Cache-Control: max-age=0
```

GTE请求
发现了一个ETag的东西， 怎么把其下载下来呢？

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2019 11:25:12 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Mon, 19 May 2014 14:01:22 GMT
ETag: "fc8-4f9c132bb9080-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 4040
Connection: close
Content-Type: application/javascript
```

response响应
怎么把它下载下来呢？

...
扫描后台也没有发现什么， 重点应该就是放在这个压缩包了

初识HTTP缓存

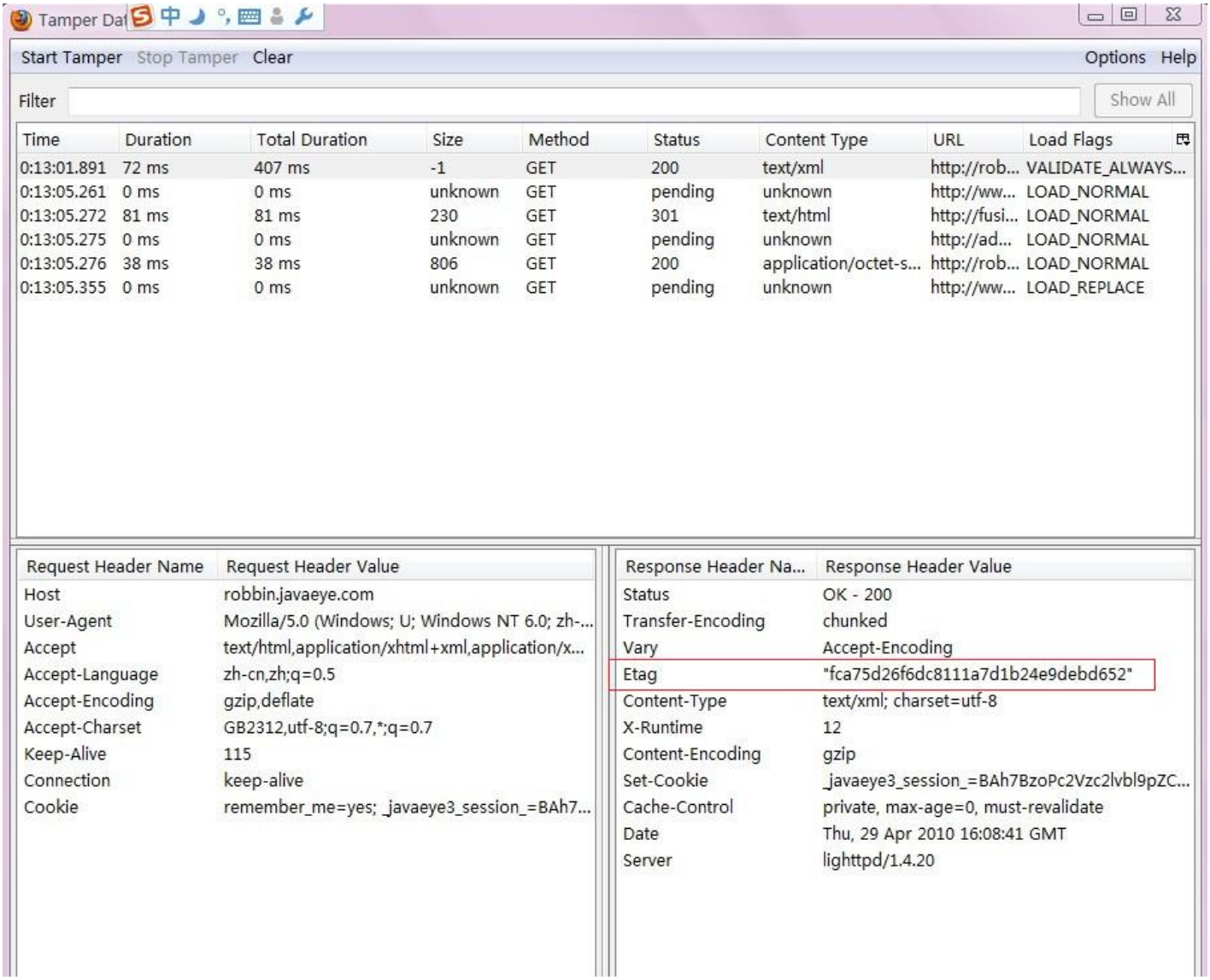
Etag 是URL的Entity Tag，用于标示URL对象是否改变，区分不同语言和Session等等。具体内部含义是使服务器控制的，就像Cookie那样。

HTTP协议规格说明定义ETag为“被请求变量的实体值”。另一种说法是，ETag是一个可以与Web资源关联的记号（token）

既然是一个资源实体，那应该怎么下载下来呢

> 想必许多网友都有订阅某些大虾的RSS的习惯吧，但是大虾也是人，也要吃饭睡觉打豆豆，所以不可能无时无刻的在从事文学创作，因此一般产量较高的大虾也许平均每天能更新两篇已经是不错了，但是网友们却总是不断的去刷新RSS订阅的内容，期望在下次刷新中又有新的劲爆文章出现，如果我们每次刷新，都要从服务器端重新获取内容（事实上，几乎一天内95%以上的刷新返回的都是相同内容，因为刚才也说了，大虾一般一天也就出一两篇新文章而已，所以大部分时间内，内容都是相同的），如果订阅量相当巨大，这对于服务器的压力还是带宽都是一个严重的挑战。其实真正需要服务器重新返回内容是大虾们更新了新的文章后，而其他时间我们无论怎么刷新服务器最好能做到不需返回任何数据，这才是一个比较好的方案，而我们的主角etag响应头的出现正是为了解决这个问题。

我们来看下图
服务器端返回了最新的内容



1
然后我们尝试刷新，以希望能获得最新的内容，

但是服务器端并不上当

Request Header Name	Request Header Value
Host	robbin.javaeye.com
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 6.0; zh-...
Accept	text/html,application/xhtml+xml,application/x...
Accept-Language	zh-cn,zh;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	GB2312,utf-8;q=0.7,*;q=0.7
Keep-Alive	115
Connection	keep-alive
Cookie	remember_me=yes; _javaeye3_session_=BAh7...
If-None-Match	"fca75d26f6dc8111a7d1b24e9debd652"
Cache-Control	max-age=0

2

如果某大虾并没在这段时间内发表任何文章，于是webserver端的rss文件没有任何变化，于是If-None-Match值和server端的etag值相比较完全相等， 就会发送304响应码

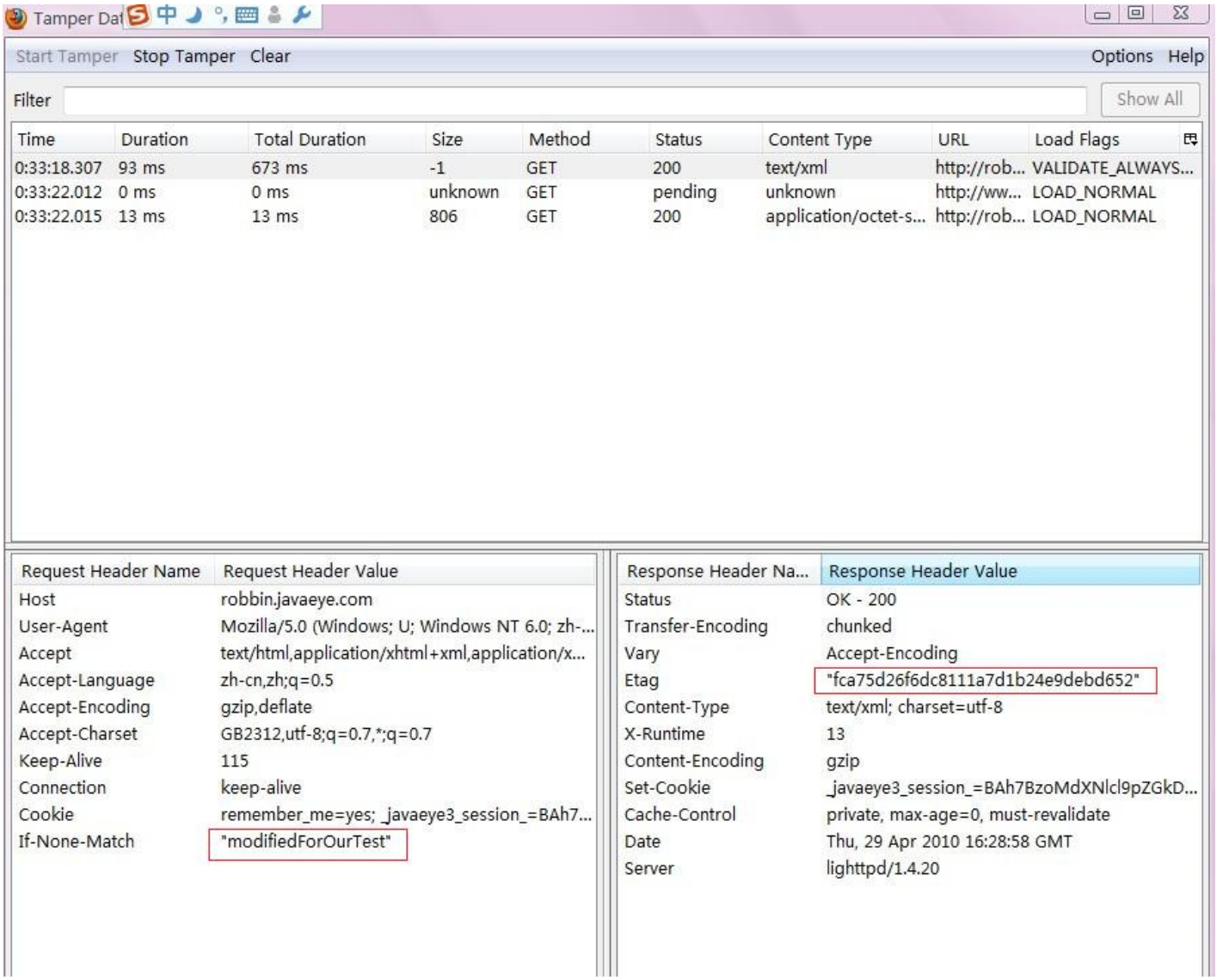
Response Header Na...	Response Header Value
Status	Not Modified - 304
Etag	"fca75d26f6dc8111a7d1b24e9debd652"
X-Runtime	12
Set-Cookie	_javaeye3_session_=BAh7BzoPc2Vzc2lvbl9pZC...
Cache-Control	private, max-age=0, must-revalidate
Date	Thu, 29 Apr 2010 16:16:15 GMT
Server	lighttpd/1.4.20

3

如果某大虾刚发表了一篇新的文章，因此在webserver中的rss的内容发生了改变，因此他的etag值就会发生改变，于是服务器会拿http请求中的If-None-Match的

值和改变和的etag值做对比，显然不正确的，于是webserver就会发送一个新的rss内容给客户端，这里我不能强制要求某大虾来配合我们的实验去立马发表新文章，

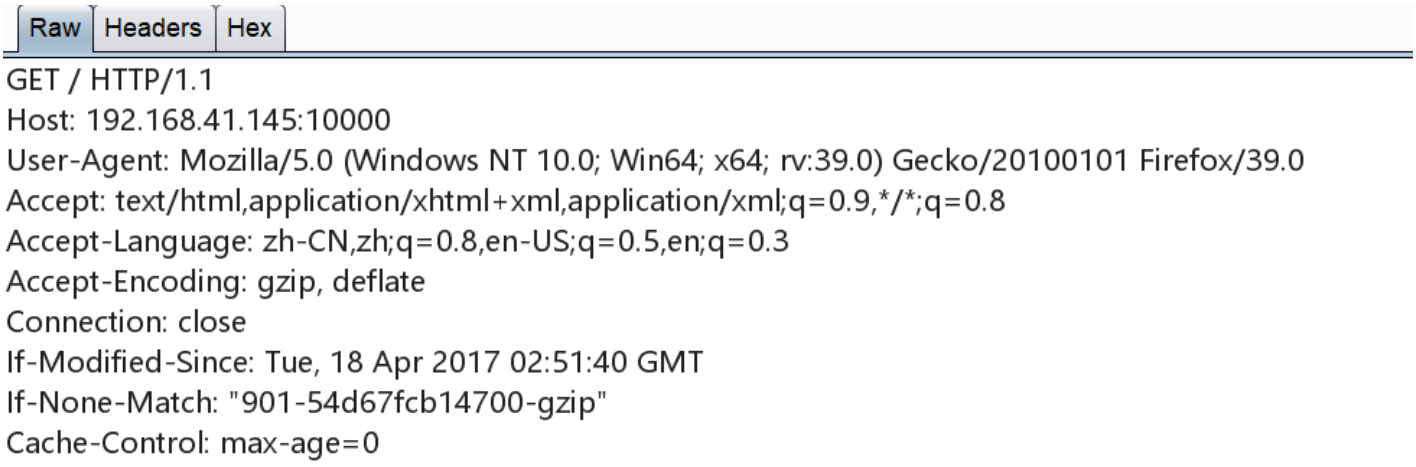
所以我们就变相做，也就是我们故意修改http请求头中的If-None-Match的值，这样就和服务器端的etag就不会匹配了，显然这时候服务器就会受骗发送一份“新”的回来



4

Etag精解

然而我并不知道下一步该怎么办



https://www.jianshu.com/p/e9923b65789e

HTTP/1.1 200 OK
Date: Mon, 01 Apr 2019 11:49:39 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Mon, 19 May 2014 14:01:22 GMT
ETag: "27ce-4f9c132bb9080-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 10190
Connection: close
Content-Type: application/javascript

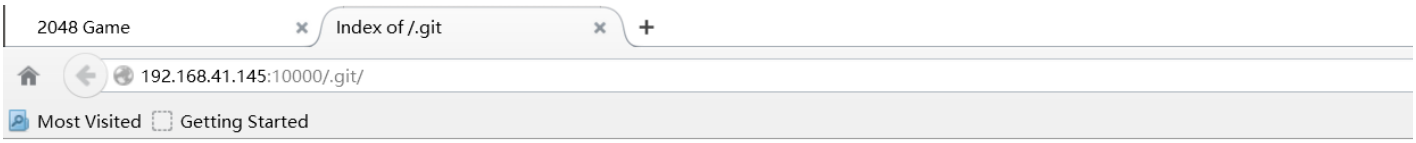
修改了之后感觉没啥用

每次返回给我的ETag值都不一样。。

我很懵。

看WP了。 发现居然是.git源码泄露。

首先是怎么知道是.git源码泄露的呢？



Index of /.git

Name	Last modified	Size	Description
Parent Directory		-	
COMMIT_EDITMSG	2017-04-18 09:21	23	
HEAD	2017-04-18 09:17	23	
ORIG_HEAD	2017-04-18 09:20	41	
branches/	2017-04-18 09:17	-	
config	2017-04-18 09:17	92	
description	2017-04-18 09:17	73	
hooks/	2017-04-18 09:17	-	
index	2018-05-17 05:00	709	
info/	2017-04-18 09:17	-	
logs/	2017-04-18 09:20	-	
objects/	2017-04-18 09:21	-	
refs/	2017-04-18 09:17	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.41.145 Port 10000

直接用工具下载好了。。

```
abc@ubuntu:~/GitHacker$ python2 GitHacker.py 127.0.0.1:10000/.git
Saved working directory and index state WIP on master: e29cc00 Update README.md
[+] Make dir : ./127_0_0_1:10000_/.git/info/
[!] Getting -> http://127.0.0.1:10000/.git/info/exclude
[+] Success!
[+] Make dir : ./127_0_0_1:10000_/.git/
[-] Folder already existed!
[!] Getting -> http://127.0.0.1:10000/.git/index
[+] Success!
[+] Make dir : ./127_0_0_1:10000_/.git/refs/heads/
[!] Getting -> http://127.0.0.1:10000/.git/refs/heads/master
[+] Success!
[+] Make dir : ./127_0_0_1:10000_/.git/refs/remotes/origin/
[!] Getting -> http://127.0.0.1:10000/.git/refs/remotes/origin/HEAD
[-] [404]
[+] Make dir : ./127_0_0_1:10000_/.git/refs/
[-] Folder already existed!
[!] Getting -> http://127.0.0.1:10000/.git/refs/stash
[-] [404]
[+] Make dir : ./127_0_0_1:10000_/.git/hooks/
[!] Getting -> http://127.0.0.1:10000/.git/hooks/update.sample
[+] Success!
[+] Make dir : ./127_0_0_1:10000_/.git/hooks/
[-] Folder already existed!
[!] Getting -> http://127.0.0.1:10000/.git/hooks/pre-receive.sample
[+] Success!
[+] Make dir : ./127_0_0_1:10000_/.git/hooks/
[-] Folder already existed!
```

进入目录之后，使用git log可以看到每次提交就下来的东东

```
abc@ubuntu:~/GitHacker/127_0_0_1:10000_$ git log
commit 36215508245866608ddb1ce1f712c45f251ddf6db (HEAD -> master)
Author: WangYihang <wangyihanger@gmail.com>
Date:   Tue Apr 18 17:21:20 2017 +0800

    Add my fancy 2048 game

commit 007081d370ec45fe10628304e5abe010903a9a16
Author: WangYihang <wangyihanger@gmail.com>
Date:   Tue Apr 18 17:20:05 2017 +0800

    Add README.md
```

更确切的做法应该是 git reflog

```
    Add README.md
abc@ubuntu:~/GitHacker/127_0_0_1:10000_$ git reflog
3621550 (HEAD -> master) HEAD@{0}: reset: moving to HEAD
3621550 (HEAD -> master) HEAD@{1}: commit: Add my fancy 2048 game
007081d HEAD@{2}: reset: moving to 007081d370ec45fe10628304e5abe010903a
9a16
3465ee8 HEAD@{3}: commit: Add my secret
007081d HEAD@{4}: commit (initial): Add README.md
```

然后就是git 的版本回退啦

git reset --hard 3465ee

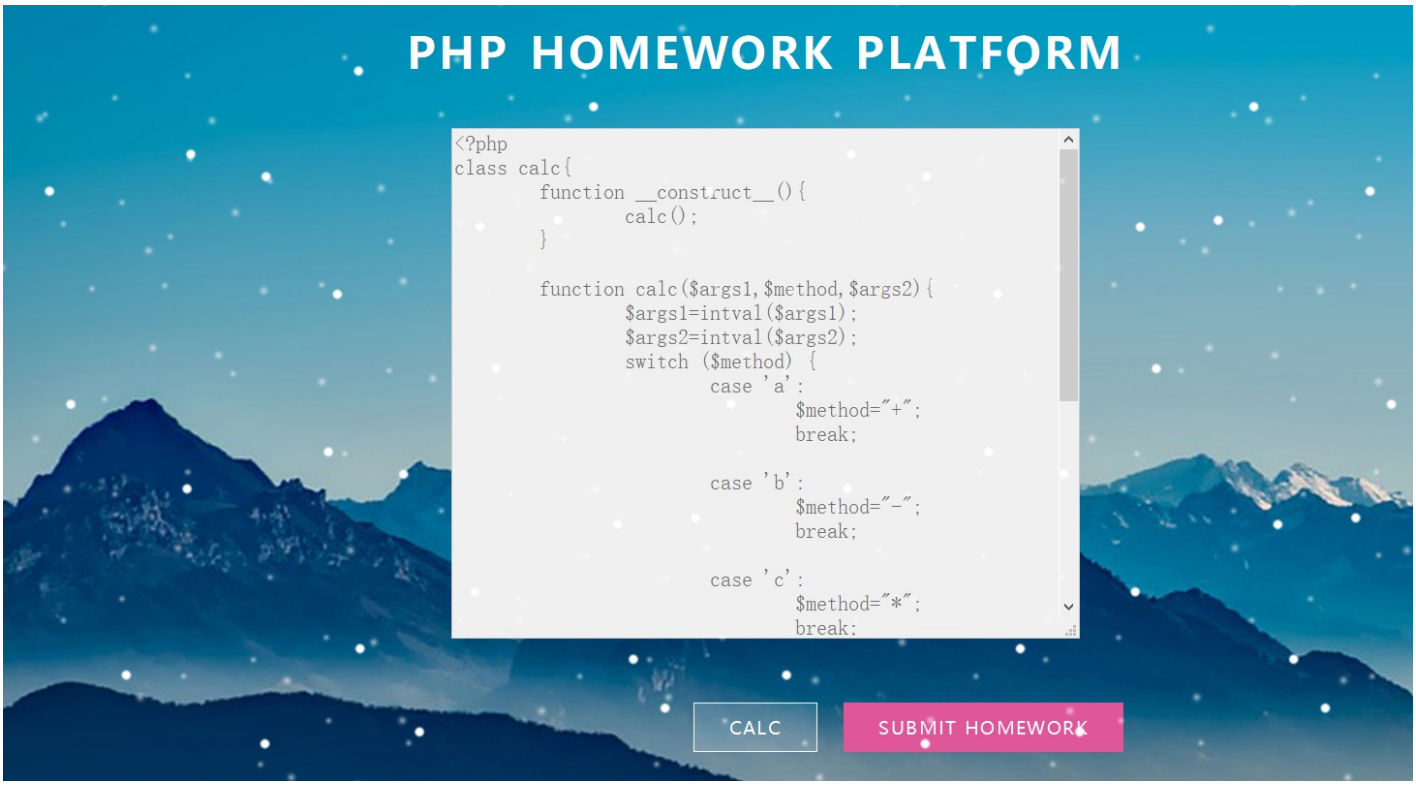
然后。。 flag就出来了

image.png
参考
https://blog.csdn.net/qq_35078631/article/details/77777416

https://www.jianshu.com/p/e9923b65789e

2018-suctf-homework

进去之后是一个很漂亮的网页



看到一串代码， 估计就是代码审计了

```php
<?php
class calc{
    function __construct__(){
        calc();
    }

    function calc($args1,$method,$args2){
        $args1=intval($args1);
        $args2=intval($args2);
        switch ($method) {
            case 'a':
                $method="+";
                break;

            case 'b':
                $method="-";
                break;

            case 'c':
                $method="*";
                break;

            case 'd':
                $method="/";
                break;

            default:
                die("invalid input");
        }
        $Expression=$args1.$method.$args2;
        eval("\$r=$Expression;");
        die("Calculation results:".$r);
    }
}
```

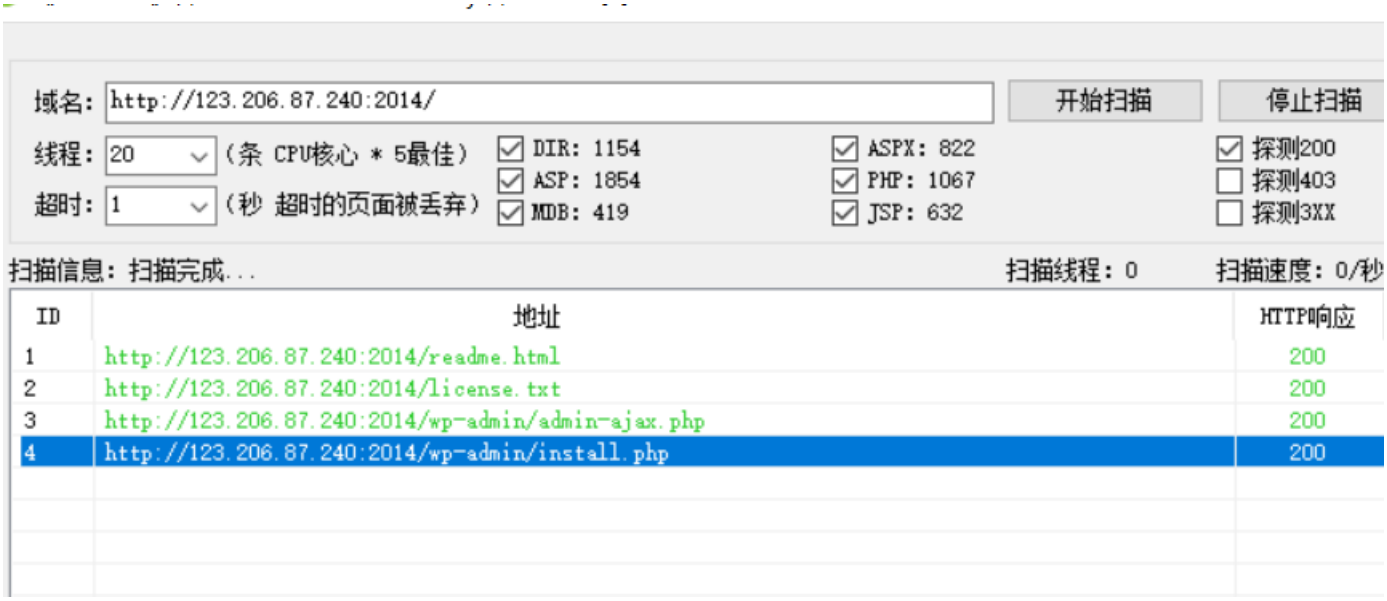
孙xx的博客

一个很漂亮的wordpress网站

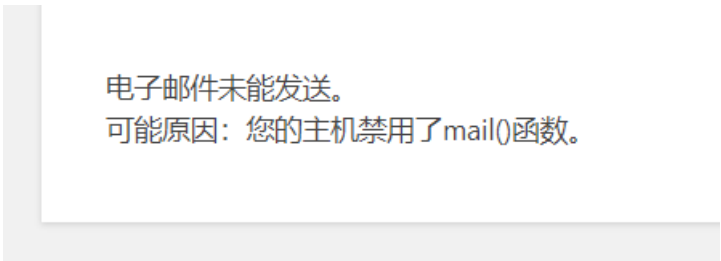
```
abc@ubuntu:~$ nikto -h http://123.206.87.240:2014/
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          123.206.87.240
+ Target Hostname:    123.206.87.240
+ Target Port:        2014
+ Start Time:         2019-04-04 19:39:04 (GMT-7)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'link' found, with contents: <http://123.206.87.240:2014/?rest_route=/>; re
l="https://api.w.org/"
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

nikto扫描一下

御剑感觉扫出了很多东西


域名: http://123.206.87.240:2014/
开始扫描
停止扫描
线程: 20 (条 CPU核心 * 5最佳)
超时: 1 (秒 超时的页面被丢弃)
DIR: 1154
ASP: 1854
MDB: 419
ASPX: 822
PHP: 1067
JSP: 632
探测200
探测403
探测3XX
扫描信息: 扫描完成...
扫描线程: 0
扫描速度: 0/秒
ID
地址
HTTP响应
1 http://123.206.87.240:2014/readme.html 200
2 http://123.206.87.240:2014/license.txt 200
3 http://123.206.87.240:2014/wp-admin/admin-ajax.php 200
4 http://123.206.87.240:2014/wp-admin/install.php 200


错误: 无效用户名。 忘记密码?
用户名或电子邮件地址
密码
记住我的登录信息
登录
忘记密码?


电子邮件未能发送。
可能原因: 您的主机禁用了mail()函数。

看来用户名就是sun

image.png

看了好多wp都说是找到了phpmyadmin。。

算了我找不到

参考

又找到一个很好的工具

专为ctf而生的扫描工具

好想自己写一个扫描工具啊