

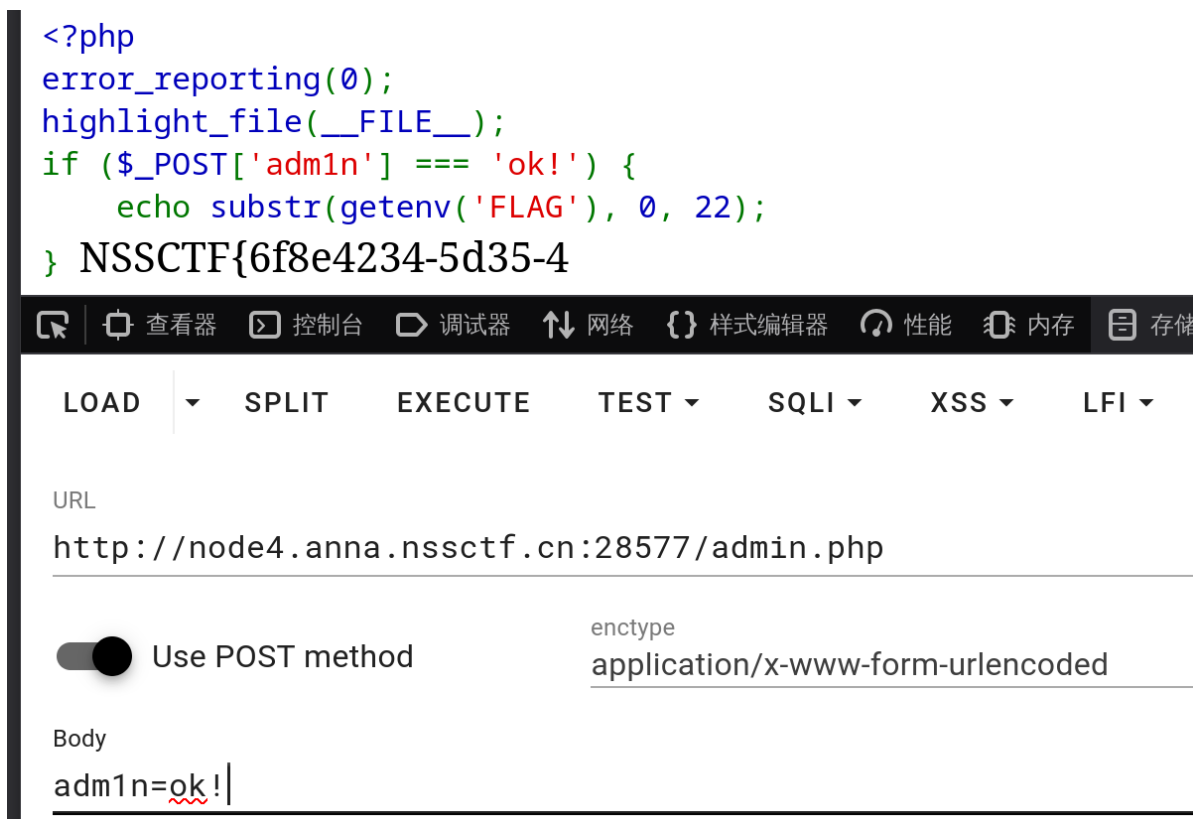
# where i am?

## 1. 直接dirsearch目录扫描

```
[15:43:39] Scanning:
[15:43:46] 200 - 1KB - /admin.php
[15:43:53] 200 - 11B - /index.html
[15:43:58] 200 - 46B - /robots.txt
[15:43:58] 403 - 288B - /server-status/
[15:43:58] 403 - 288B - /server-status
```

## 2. 先访问admin.php，post传参adm1n=ok!即可获得第一部分flag

```
<?php
error_reporting(0);
highlight_file(__FILE__);
if ($_POST['adm1n'] === 'ok!') {
    echo substr(getenv('FLAG'), 0, 22);
} NSSCTF{6f8e4234-5d35-4
```



The screenshot shows a web security tool interface. At the top, there's a code editor with PHP code. Below it, there's a toolbar with icons for various actions. The main area shows a POST request configuration. The URL is set to `http://node4.anna.nssctf.cn:28577/admin.php`. The 'Use POST method' toggle is turned on. The 'Body' field contains `adm1n=ok!`. The 'Content-Type' is set to `application/x-www-form-urlencoded`.

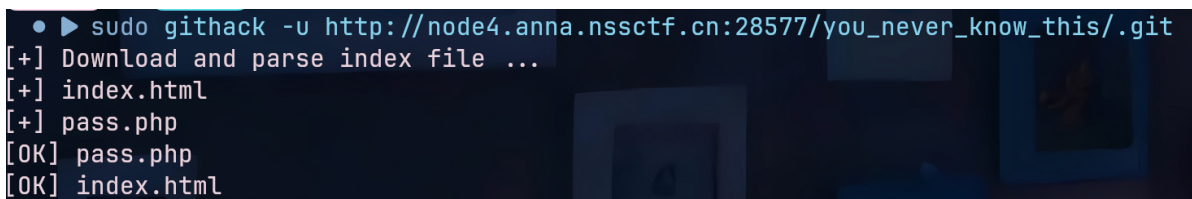
## 3. 访问robots.txt，有一个不同意的目录，我们直接访问，得到提示应该是git泄露

User-agent: \*  
Disallow: /you\_never\_know\_this/

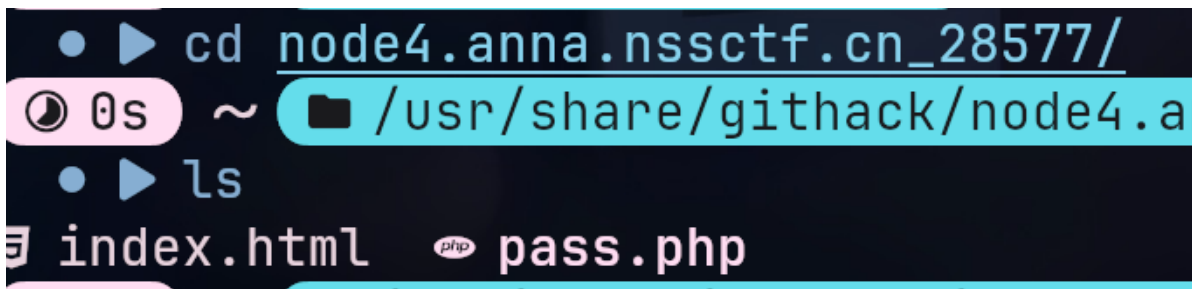
我们使用了git来管理版本



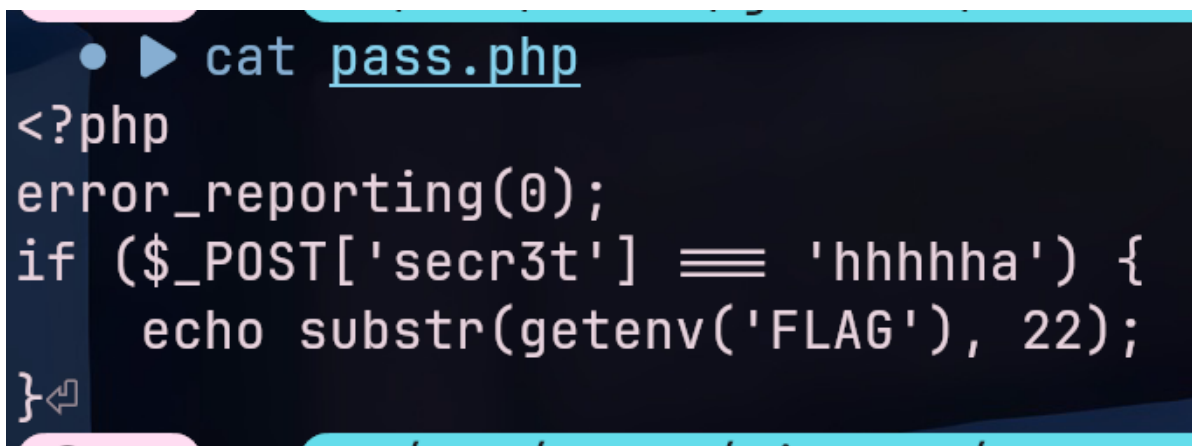
4.使用githack把.git目录的文件全部下载好



5.访问可以看到除了index.html还有pass.php




6.查看pass.php内容



7.回到浏览器访问post传参secr3t=hhhhhha即可获得flag最后一部分

f61-b682-fe797b968b1f}



LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SS

URL

http://node4.anna.nssctf.cn:28577/you\_never\_know\_this/pass.php

Use POST method

enctype  
application/x-www-form-urlencoded

Body

secr3t=hhhhha