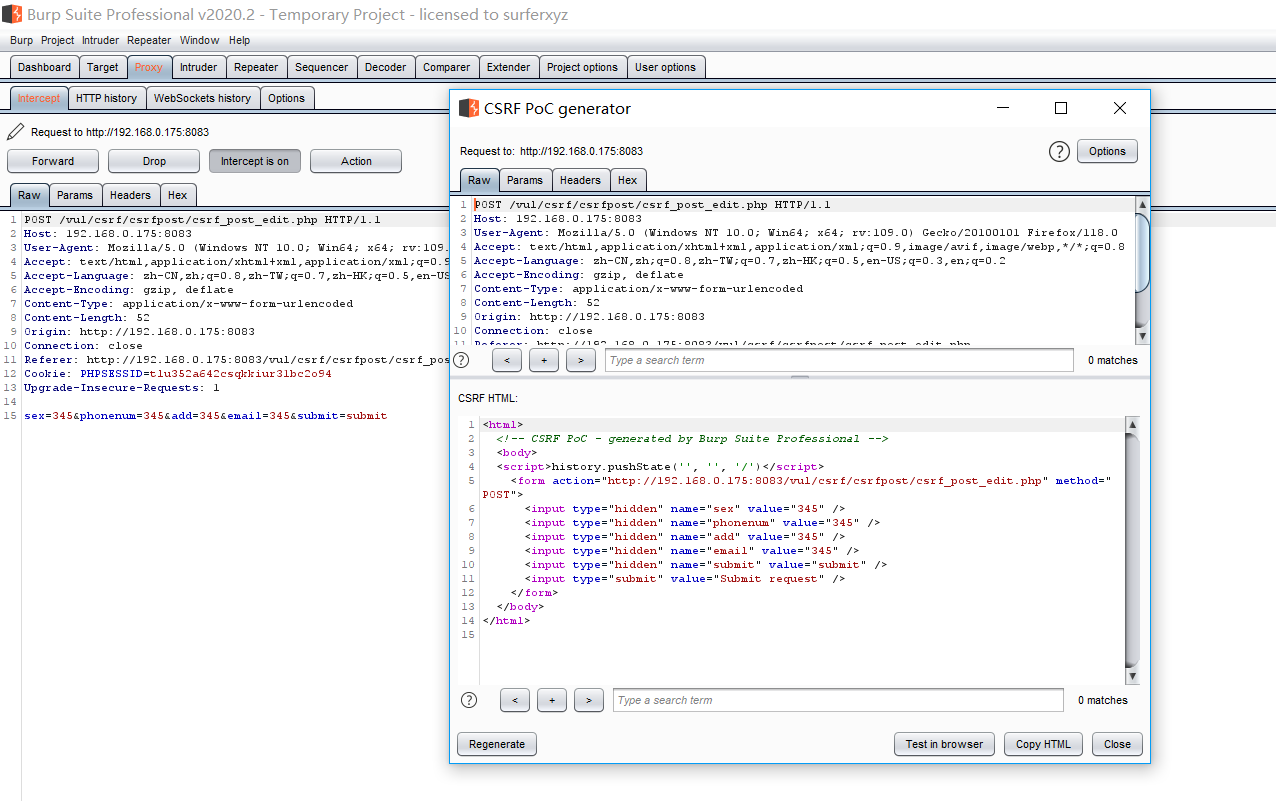
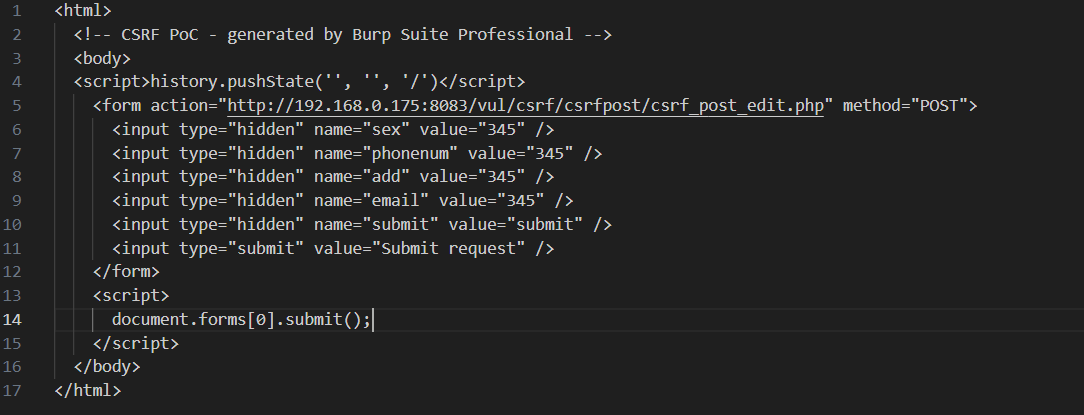
1. CSRF

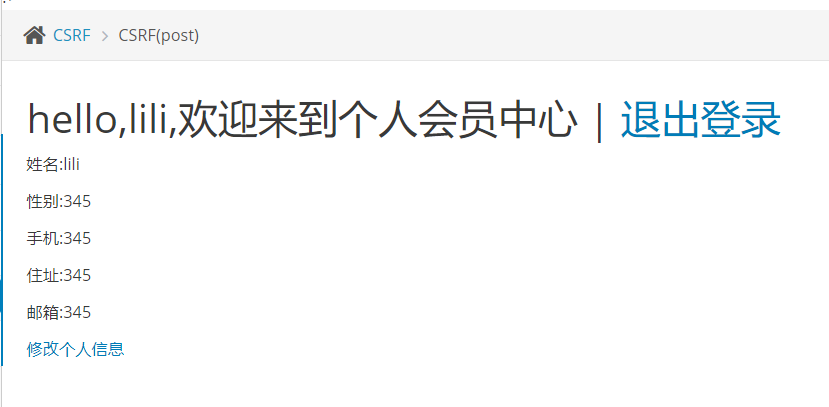
* DVWA-High 等级

使用用户名pablo在谷歌浏览器进行登录，然后点击xss(Reflected)模块，然后输入<img src=x OnerrOr=alert(document.cookie)>；获取到PHPSESSID。

然后用admin用户登录，通过burp获取到修改密码的参数，修改安全等级 去掉tonken ，修改session 参数



* 使用 Burp 生成 CSRF 利用 POC
* 
* 生产poc文件
* 



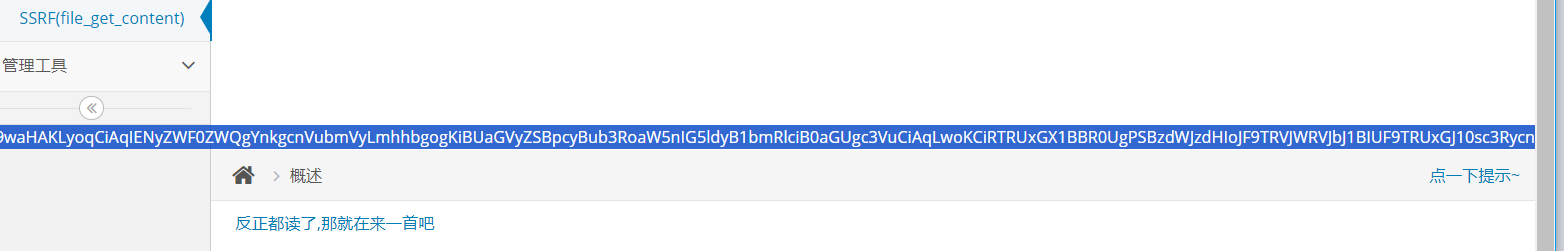
可以查看发现信息已经被修改

1. SSRF（file\_get\_content），要求获取 ssrf.php 的源码；

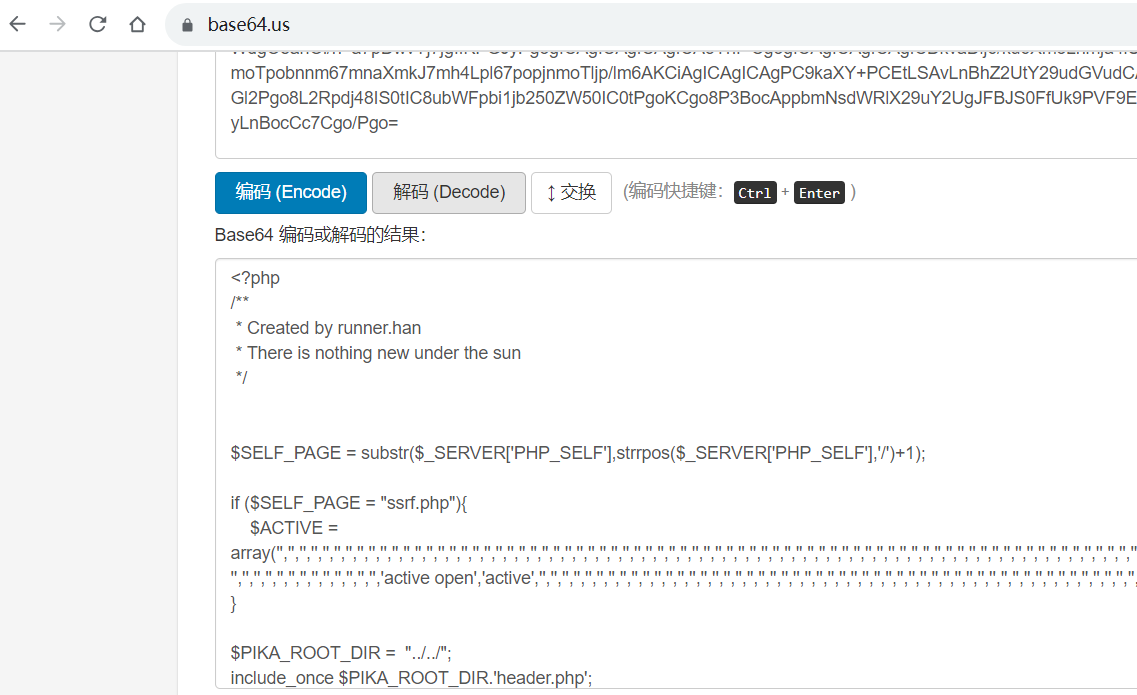
我们用php://filter 来读取php源码，可以看到访问成功



在read参数中加入 convert.base64-encode拿到php源码



利用解码工具base64.us进行解码：



1. 远程代码执行漏洞：Weblogic RCE。

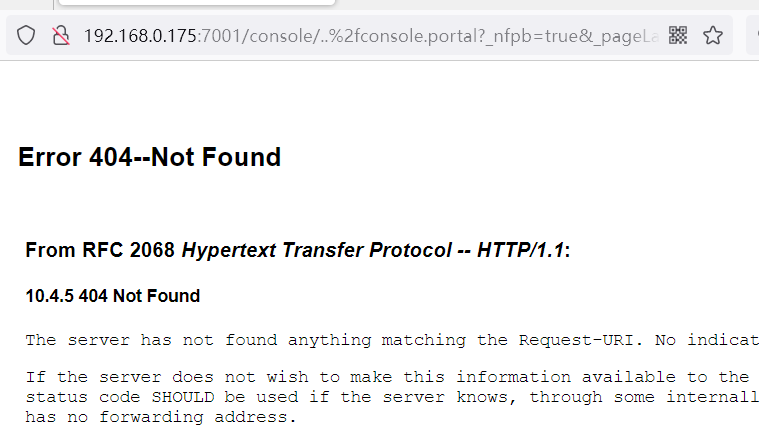
启动镜像



上传xml文件



执行构造后的url



生成文件

