1.用蓝莲花完成cookie获取

使用docker拉取镜像

```
sudo docker pull romeoz/docker-apache-php:5.6
```

```
┌──(kali㉿kali)-[/etc/docker]
└─$ sudo docker pull romeoz/docker-apache-php:5.6
5.6: Pulling from romeoz/docker-apache-php
b849b56b69e7: Retrying in 1 second
42986ef25bcd: Retrying in 1 second
d927c1b717ec: Retrying in 1 second
15b86ea20233: Waiting
aa9c3feeccb0: Waiting
441971529208: Waiting
28e5adee6726: Waiting
a881ee969f12: Waiting
11bc074377ca: Waiting
8960908a4b52: Waiting
7a162f4abcee: Waiting
5.6: Pulling from romeoz/docker-apache-php
b849b56b69e7: Pull complete
42986ef25bcd: Pull complete
d927c1b717ec: Pull complete
15b86ea20233: Pull complete
aa9c3feeccb0: Pull complete
441971529208: Pull complete
28e5adee6726: Pull complete
a881ee969f12: Pull complete
11bc074377ca: Pull complete
8960908a4b52: Pull complete
7a162f4abcee: Pull complete
Digest: sha256:360e48b1adf662c91cf07e6af8dabb468e54b9fc0205cf302594d41a1d86d78b
Status: Downloaded newer image for romeoz/docker-apache-php:5.6
docker.io/romeoz/docker-apache-php:5.6
```

创建容器并运行

```
sudo docker run -d -p 8888:80 --name PHP5.6 romeoz/docker-apache-php:5.6
```

```
┌──(kali㉿kali)-[/etc/docker]
└─$ sudo docker run -d -p 8888:80 --name PHP5.6 romeoz/docker-apache-php:5.6
4cfe688ee4c06e36b374ef8c89cc3f94d4fc36d0c907153e2c2cf6ad83464b74
```

将BlueLotus_XSSReceiver拷贝到容器中

```
sudo docker cp BlueLotus_XSSReceiver 容器ID:/var/www/app
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo docker cp BlueLotus_XSSReceiver 4cfe68:/var/www/app
```

进入容器中删除默认index文件，然后将BlueLotus_XSSReceiver内容移到该目录下并删除空文件夹，最后修改配置

在kali下用此命令进入容器

```
sudo docker exec -it 容器ID /bin/bash
```

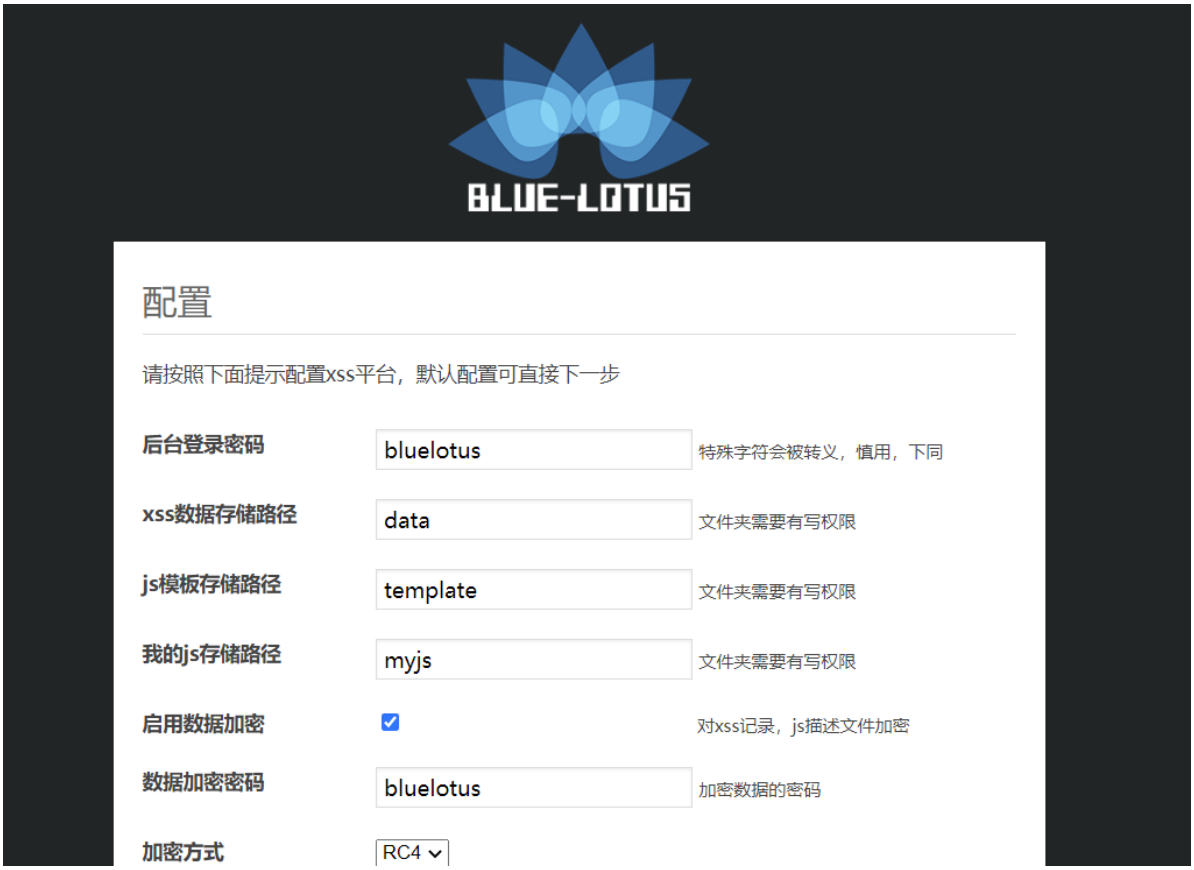
在容器中执行以下命令

```
rm -rf index.php
mv BlueLotus_XSSReceiver/* .
rm -rf BlueLotus_XSSReceiver/
chmod -R 777 myjs
chmod -R 777 data
chmod -R 777 ./
```

访问BlueLotus_XSSReceiver后台

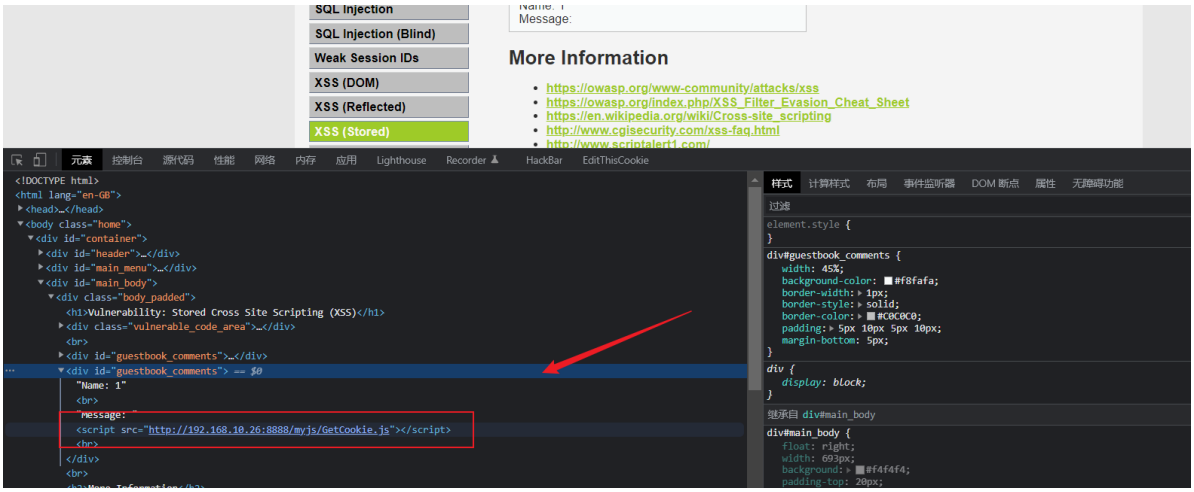
`http://docker宿主机ip:8888/admin.php`

进行配置，全部默认

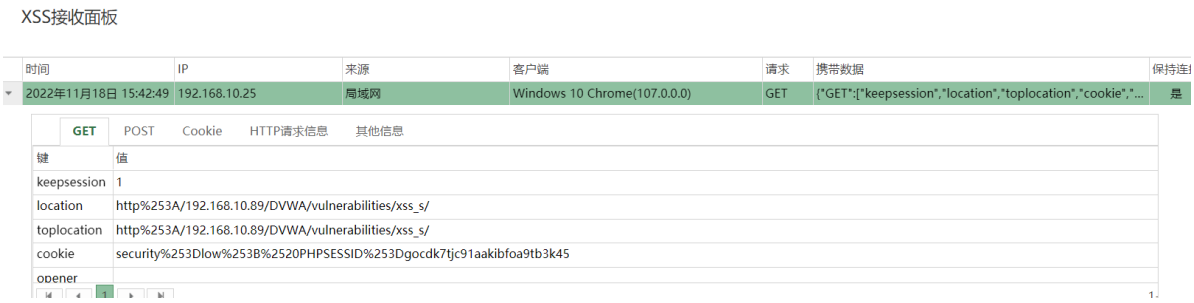


将公共模板中的default.js复制到我的JS下写入地址和端口后生成payload

然后将payload注入网站



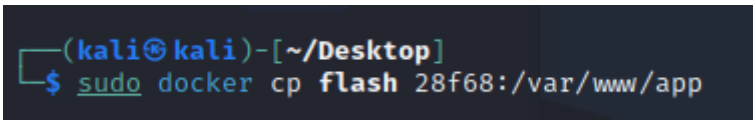
其他用户打开后即可得到cookie



2.完成Flash钓鱼

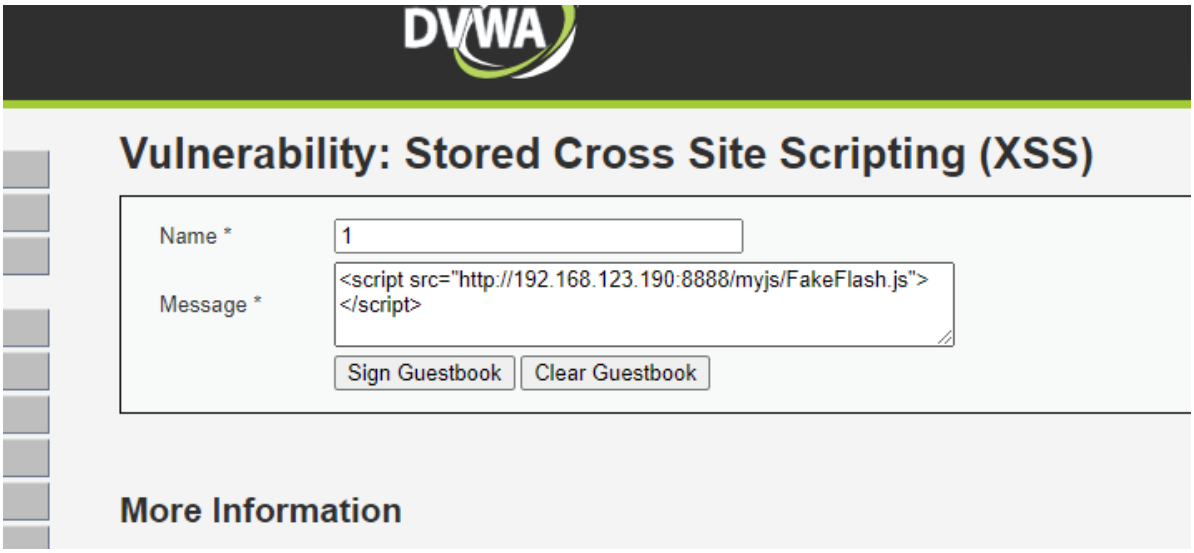
将flash文件放置在docker下

```
sudo docker cp flash 28f68:/var/www/app
```

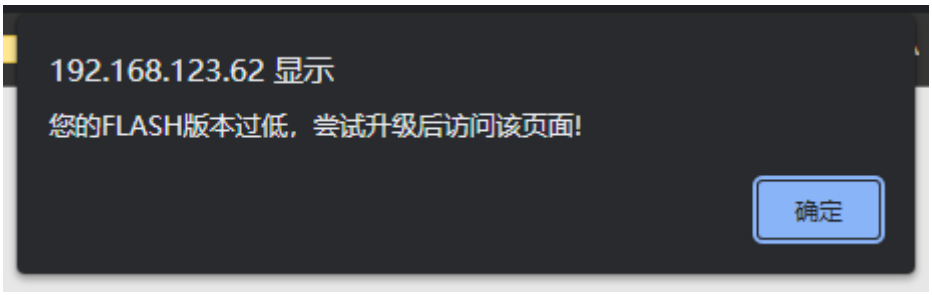


修改JS文件为自己的flash地址并放入蓝莲花

将payload插入有xss漏洞处



成功钓鱼



3.完成cobalt strike钓鱼，获取用户名和密码

配置JDK环境

```
sudo apt install openjdk-11-jdk
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ java -version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
openjdk version "11.0.16" 2022-07-19
OpenJDK Runtime Environment (build 11.0.16+8-post-Debian-1)
OpenJDK 64-Bit Server VM (build 11.0.16+8-post-Debian-1, mixed mode, sharing)
```

解压CS并启动服务端

```
unzip -d CS cs4.4-jdk11.zip
```

```
chmod +x teamserver
sudo ./teamserver ip地址 密码
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ unzip -d CS cs4.4-jdk11.zip
Archive:  cs4.4-jdk11.zip
  inflating: CS/agscript
  inflating: CS/c2lint
  inflating: CS/cobaltstrike
  inflating: CS/cobaltstrike.jar
  inflating: CS/Cobaltstrike_EN.vbs
  inflating: CS/CobaltStrikeCN.jar
  inflating: CS/icon.jpg
   creating: CS/logs/
  inflating: CS/peclone
  inflating: CS/teamserver
  inflating: CS/TeamServer.prop
   creating: CS/third-party/
  inflating: CS/third-party/README.winvnc.txt
  inflating: CS/third-party/winvnc.x64.dll
  inflating: CS/third-party/winvnc.x86.dll
  inflating: CS/update.jar
```

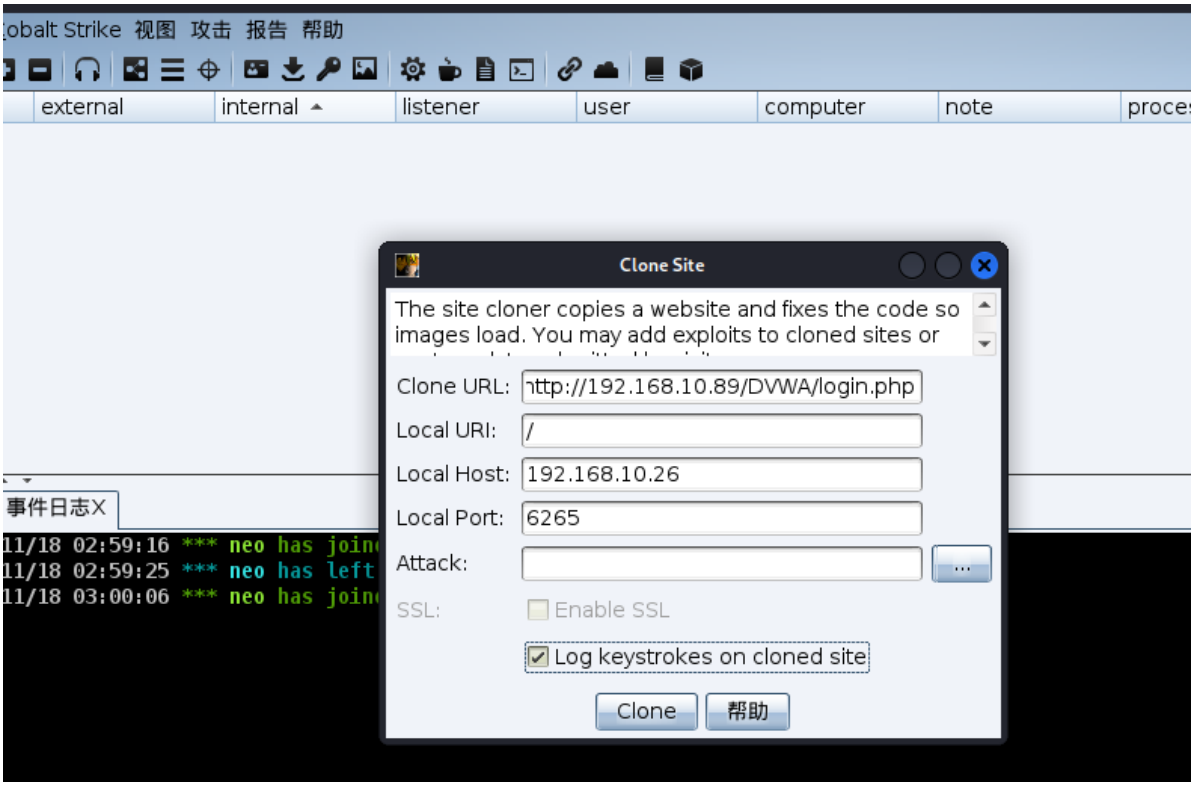
```
┌──(kali㉿kali)-[~/Desktop/CS]
└─$ chmod +x teamserver

┌──(kali㉿kali)-[~/Desktop/CS]
└─$ sudo ./teamserver 192.168.10.26 password1
[*] Generating X509 certificate and keystore (for SSL)
[*] Loading properties file (/home/kali/Desktop/CS/TeamServer.prop).
[*] Properties file was loaded.
[+] Team server is up on 0.0.0.0:50050
[*] SHA256 hash of SSL cert is: 518b180f0f8fc6d0d56c6da63fefbff2bf9f14ff9a1d30d3b6d8bf6c51665b6c
```

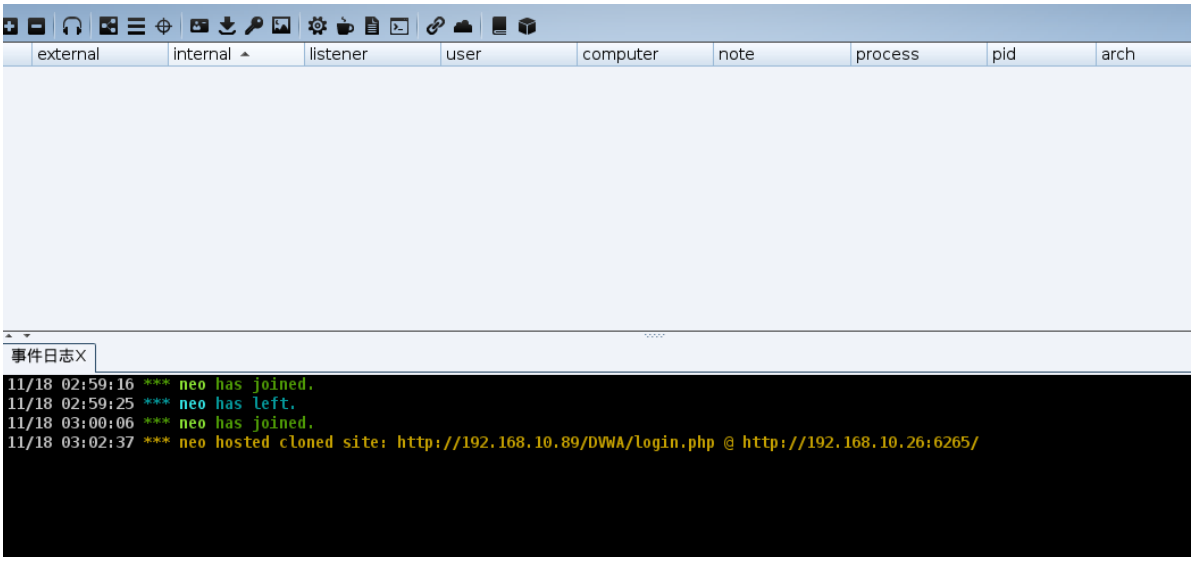
启动客户端

```
chmod +x cobaltstrike
./cobaltstrike
```

选择攻击 -> 钓鱼攻击 -> 克隆网站

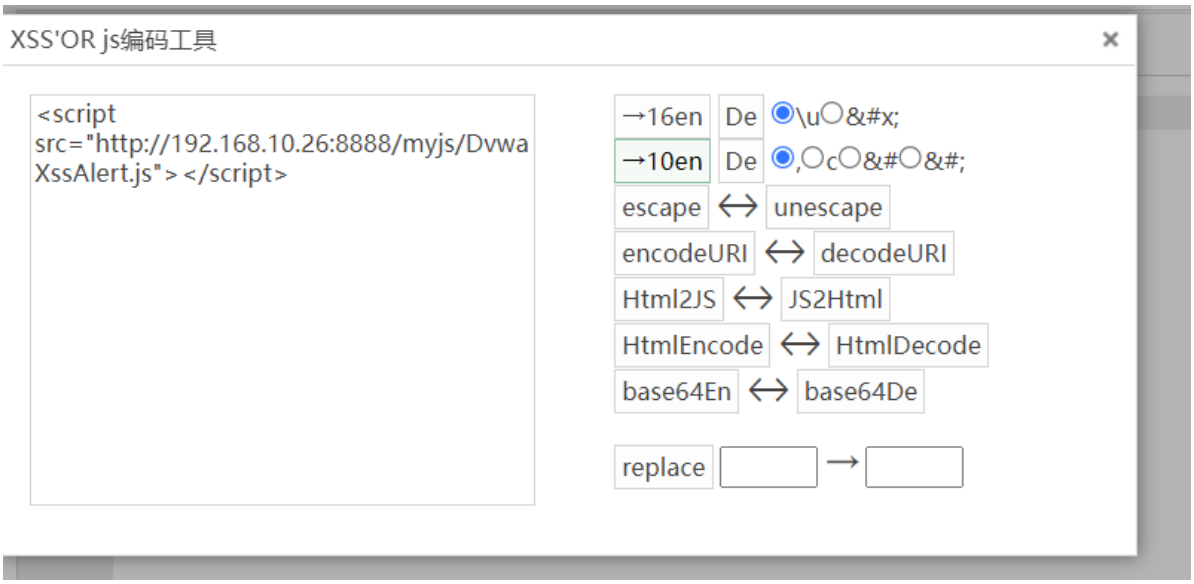


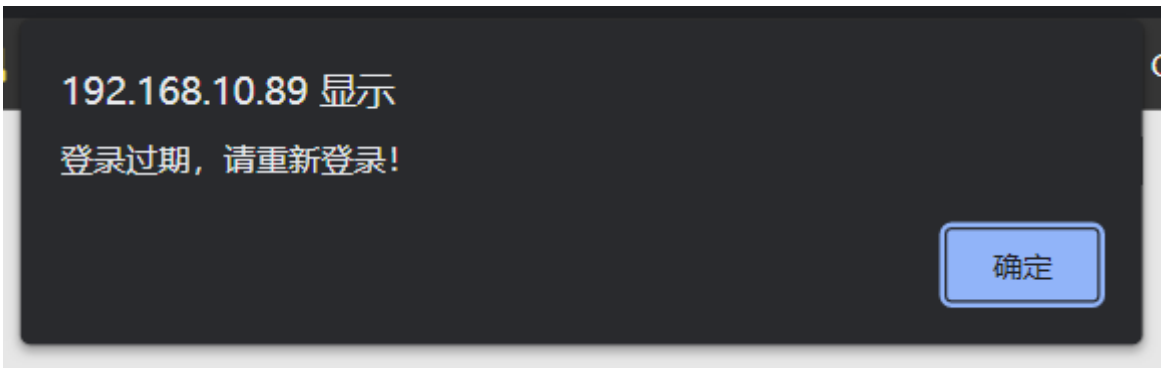
克隆成功



在蓝莲花中创建JS代码

在原本的页面利用XSS漏洞插入代码，引诱用户进入钓鱼网站





用户在钓鱼页面中输入网站即可在CS中获取账户密码