

一、前言

ImXSS是国内首套Java研发的Xss跨站脚本测试平台。ImXSS前身是XssAPP，秉承高效、快速、稳定、易用的原则。主要用于技术研究与交流

在线地址：<http://imxss.com/>、<http://xssapp.com/>

开源地址：<http://code.taobao.org/p/imxss/src/>

二、业务说明

跨站脚本攻击（也称为XSS）指利用网站漏洞从用户那里恶意盗取信息。

三、背景

网站中包含大量的动态内容以提高用户体验，比过去要复杂得多。所谓动态内容，就是根据用户环境和需要，Web应用程序能够输出相应的内容。动态站点会受到一种名为Site Scripting, 安全专家们通常将其缩写成XSS,原本应当是css,但为了和层叠样式表（Cascading Style Sheet,CSS）有所区分，故称XSS）的威胁，而静态站点则完全不受其影响。

四、简介

用户在浏览网站、使用即时通讯软件、甚至在阅读电子邮件时，通常会点击其中的链接。攻击者通过在链接中插入恶意代码，就能够盗取用户信息。攻击者通常会用十六进制

五、技术介绍

首页模板：收集于chinaz.com，由于本系统为非盈利性产品，故此感谢网友分享。

前端UI：采用Amaze UI

后端语言：Java

技术框架：Spring SpringMvc Jdbc (XssAPP采用的是SpringMvc+ Hibernate)

技术特征：全MVC模式，内置缓存功能，缓存接口(可拓展集群版)，无跨表操作，轻量化框架。

自主技术：

在线调试平台：<https://www.oschina.net/p/simple-debug>

切面缓存：<https://www.oschina.net/p/simple-cache>

多主从Orm：<https://www.oschina.net/p/simple-edbc>

六、业务特征

支持屏蔽来源地址(屏蔽方式：Ant通配表达式)，解决部分无用信封轰炸问题。

支持对来源地址单独定制模板(Ant表达式)，解决对某些站点定制规则。

支持自定义发信服务器，解决平台信封过多导致发信失败问题。

支持Http/Https同时使用，解决不确定后台站点协议问题。

PC端

调试中心

移动端 h5自适应

设计文档: <https://pan.baidu.com/s/1i4K9tat> 密码: 2333

点击收藏 | 0 关注 | 0

[上一篇：【reCAPTCHA】一款识别图形...](#) [下一篇：【菜鸟腾飞】Mysql数据库渗透及...](#)

1. 6 条回复



[Coody](#) 2017-11-02 15:36:19

666666

0 回复Ta



[91shell](#) 2017-11-02 15:54:20

大佬，有没有相关的部署教程

0 回复Ta



[godsec](#) 2017-11-02 16:08:14

看起来很厉害的样子 但是我不会部署

0 回复Ta



[hades](#) 2017-11-02 22:37:11

@godsec

- 1、请将本项目打包成War
- 2、放置Tomcat下运行即可
- 3、项目运行后，访问安装。
- 4、JDK版本1.8、Tomcat版本8

0 回复Ta



[小哲](#) 2018-01-02 10:11:08

[@91shell](#) 后续会出个傻瓜式部署教程

0 回复Ta



[hades](#) 2018-01-04 14:31:20

[@小哲](#) 快

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)