安全框架使用手册

'背景':随着网络的发展，网络安全问题十分突出，但是大部分公司对安全问题十分不重视，导致我国网络安全问题十分严重，原因在于大部分程序员没有网络安全知识，代码没有很好的安全防范措施，所以我们就有了做安全框架的必要性。

'项目目的':网络的发展让更多人进入网络的世界，B/S端日渐没落，C/S端应用占据了市场的主流，C/S端应用无非是两大块，浏览器和服务器，浏览器的应用涉及JS的知识，我们程序使用Python语言编写，暂时不考虑，我们主要是想在服务端安全上做一些事情，现在服务器端流行MVC框架，我们的程序就是在MVC框架的M与V层之间提供一个安全服务框架，它没有嵌入用户程序中，只是起到一个中转与验证的功能，同时还为没有安全经验的人员提供一些安全工具方便使用，让用户程序没有必要考虑安全问题，程序员可以只处理业务逻辑问题，提高效率。

程序使用需要的环境:

> *程序默认监听8000端口*
> *Python 2.x*
> *Readis缓存框架 默认端口 6379 Python中使用的库: hashlib, socket, urllib2, urlparse, re, uuid, redis,requests*

下面介绍程序提供的功能:

1. 登录
2. 欢迎页面
3. 过滤XSS脚本
4. 过滤标签
5. 判断链接中是否有sql语句

登录

`POST /login`

介绍

所有的功能使用都必须登录都才能使用
1.配置登录密码
在程序中运行EncryptoMessage.py文件，程序要求输入登录密码和MD5盐
2.使用
登录密码：第一次访问时需要访问登录接口，用post方式在body内传送密码，程序判断密码是否正确(密码会以MD5值存放，防止密码泄露)，登录后程序会将特定的值放入Redis缓存框架中，就可以使用程序的功能，一段时间后密码会失效，需要重新登录
MD5盐：程序在登录成功后回生成随机字符串和用户设定的盐求MD5，存储在Redis中并返回给用户，由于Redis所有程序都可以访问，用户可以通过返回的值，设定服务端程序，实现单点登录，如果不需要可以不使用

欢迎页面

`GET /`

介绍

直接访问，不带后缀访问欢迎页面，可以看到程序的功能使用说明

过滤XSS脚本

`POST /filterXSS`

介绍

过滤XSS脚本,用户传送需要过滤的文本，程序返回过滤成功的文本，程序采用白名单机制，只允许特定的标签使用
h1, h2, h3, h4, strong, em, p, ul, li, br

请求体

用post方式在body中传送需要过滤的文本

请求示例

```
< h1 style="font-size:expression(alert('XSS'))">Hello!</h1>
<img src='http://0.0.0.0:8080/static/test/jpg' alt='我是一副正常的图片'
onerror='alert("你才不正常呢！你全家都不正常")'/>
<a href='javascript:alert(1);'>Hello</a>
<a href='http://www.baidu.com'<script>alert(1);</script>'
title='sddasdsadsd'/>
```

响应示例

```
< h1>Hello!</h1>

<img alt="我是一副正常的图片" src="http://0.0.0.0:8080/static/test/jpg"/>

<a>Hello</a>

<a href="http://www.baidu.com">alert(1);</a>' title='sddasdsadsd'/&gt;
```

过滤标签

`POST /filterAll`

介绍

过滤所有html标签，返回过滤后的信息

请求体

用post方式在body中传送需要过滤的文本

请求示例

```
< h1 style="font-size:expression(alert('XSS'))">Hello!</h1>
<img src='http://0.0.0.0:8080/static/test/jpg' alt='我是一副正常的图片'
onerror='alert("你才不正常呢！你全家都不正常")'/>
<a href='javascript:alert(1);'>Hello</a>
<a href='http://www.baidu.com'<script>alert(1);</script>'
title='sddasdsadsd'/>
```

响应示例

```
Hello!

     Hello
     alert(1);' title='sddasdsadsd'/>
```

判断链接中是否有sql语句

`POST /sendSQL`

介绍

判断链接中是否有sql，防止sql注入,如果有sql就返回空，如果没有就访问链接，返回链接的内容

请求体

用post方式在body中传送需要判断的链接

请求示例

```
list?id = 1 and 1=1 union select * from user
```

响应示例

```

```

请求示例

```
http://www.baidu.com
```

响应示例

```
<!DOCTYPE html>

<html>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=Edge">
        <meta content="always" name="referrer">
        <meta name="theme-color" content="#2932e1">
        <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
        <link rel="search" type="application/opensearchdescription+xml"
href="/content-search.xml" title="百度搜索" />
        <link rel="icon" sizes="any" mask
href="//www.baidu.com/img/baidu.svg">
        <link rel="dns-prefetch" href="//s1.bdstatic.com"/>
        <link rel="dns-prefetch" href="//t1.baidu.com"/>
        <link rel="dns-prefetch" href="//t2.baidu.com"/>
        <link rel="dns-prefetch" href="//t3.baidu.com"/>
        <link rel="dns-prefetch" href="//t10.baidu.com"/>
        <link rel="dns-prefetch" href="//t11.baidu.com"/>
        <link rel="dns-prefetch" href="//t12.baidu.com"/>
        <link rel="dns-prefetch" href="//b1.bdstatic.com"/>
        <title>百度一下，你就知道</title>
        ...
```

表单内容验证

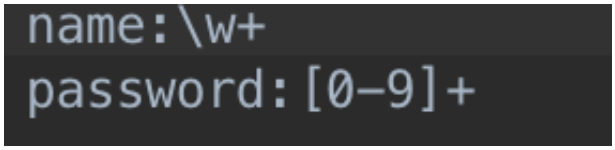
`POST /formSerach/(name)/(mode)`

请求体

参数名	类型	描述
name	string	配置文件名称
mode	int	程序中转后表单数据传送的格式

介绍

用户可以在程序中配置表单数据的格式((传送的名称).txt)，用正则表达式表示，程序会判断用户输入是否合法，如果不合法就返回，合法就根据mode的值，1表示用默认的形式传送(name=wsd&password=123),2表示用json的格式传送({‘name’:'wsd', 'password':'123'}),需要在表单中加入一个隐藏输入项(name=url,value=提交的真正地址)，程序返回真正地址返回的内容



请求示例

```
POST localhost:8000/formSerach/test/1

name=wsd&password=123&url=http://www.baidu.com
```

响应示例

```
<html>


    <head>

        <meta http-equiv="content-type" content="text/html;charset=utf-8">

        <meta http-equiv="X-UA-Compatible" content="IE=Edge">

        <title>页面不存在_百度搜索</title>

        <script type='text/javascript'>
        ...
```

请求示例

```
POST localhost:8000/formSerach/test/1

name=wsd&password=w123&url=http://www.baidu.com
```

响应示例

```
False
```

判断文件真正类型

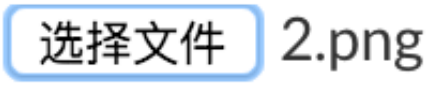
`POST /sendFile`

介绍

用户将文件上传给程序，程序通过文件名和文件内容判断文件类型，我们知道文件上传漏洞十分威胁服务器安全，我们通过两方面的机制判断文件的类型，程序会读取文件内容，根据每种类型文件的不同判断，判断的准确度更高，也不容易被上传可执行文件

请求示例

我们将一个jpg文件改成png文件上传给程序



响应示例

程序返回正确的类型
EXT_JPG

请求示例

我们将一个php脚本改成png文件上传给程序

响应示例

```
程序无法判断文件的类型
unknown
```

安全工具

`GET /list`

介绍

许多不是很掌握网络安全的人员经常会有一些安全的需求，程序提供一些安全工具，在网站上可以方便用户使用，也避免的跨平台的限制

主要功能

弱口令检测
网站ip获取
MD5加密

弱口令检测

用户输入密码，程序判断密码是否安全

网站ip获取

用户输入网站url，程序输出网站对应的ip

MD5加密

用户输入需要加密的信息，程序输出MD5后的值

安全框架自身的安全机制

介绍

程序所有功能的使用需要登录后使用，用户可以配置登录密码
程序检测用户ip，如果在1秒内3次访问就禁止访问，防止了恶意使用程序的用户

程序后续的改进计划

介绍

框架有些功能还是有一些漏洞，无法保证用户的安全，所有要完善一些安全机制，还要安全工具也会加上一些常用工具的在线版本

作者

王维国 冯翰滔