# 简介

## 什么是跨站脚本攻击？

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

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

比如借助js实现的双击，在服务端没有对<>进行转译显示的时候发生。导致黑客可以在别人的浏览器上运行任意js代码。

<script>while(1) aleart(1)<sript>

解决方案：在网页内容输出的时候做转译，将<>转译为&lt和&gt，而在nodejs中通过escape库搞定。

## XSS漏洞危害

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

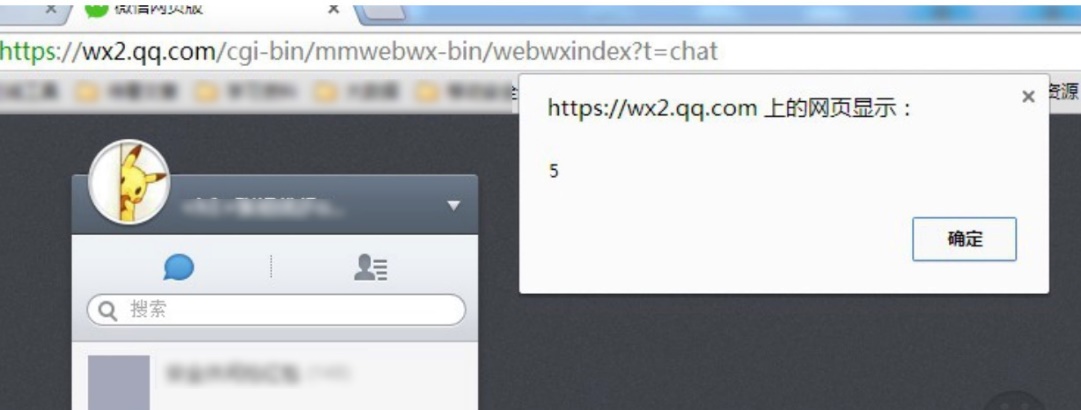
窃取数据

非法转账

挂马

…

## XSS跨站脚本实例



Payload(有效荷载)

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

什么又是PoC？概念验证程序，用来验证漏洞是否存在，无害

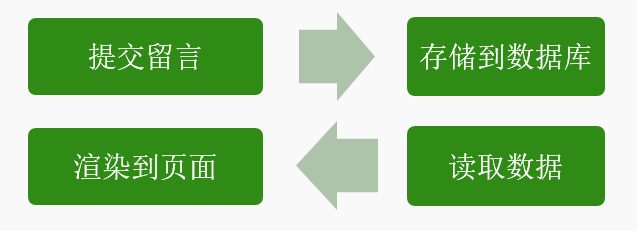
什么又是Exp？利用程序，利用代码（payload）验证漏洞，有害

# 分类

常规的XSS分类

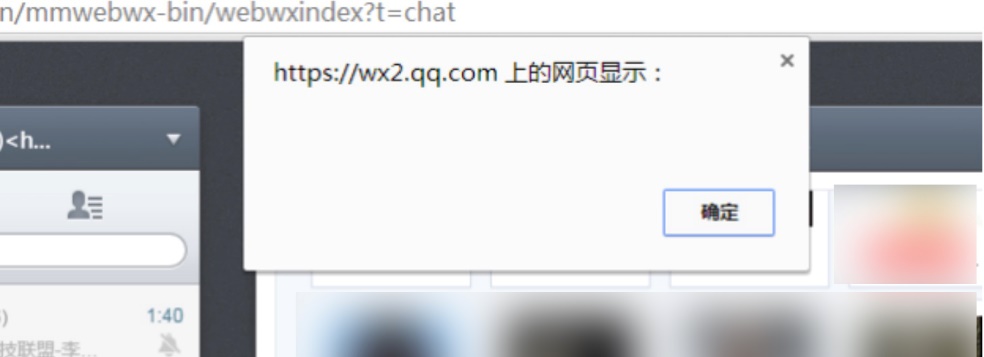
## 存储型(持久型)

如：留言板功能



如果留言功能存在XSS漏洞，则可以将用户留言替换为恶意代码，存储到数据库，下一次访问的时候，则会渲染到页面。

存储型XSS：



## 反射型(非持久型)

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

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



## 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>

DOM型XSS:



## 其他XSS类别

### mXSS(突变型XSS)





### UXSS(通用型XSS)

### Flash XSS

### UTF-7 XSS

### 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

### CSS XSS

<html>

<body>

<style>

body {width:expression(alert(1));: red;}

</style>

</body>

</html>

### VBScript XSS

# 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（比如提交网站意见后统一显示成功或失败，而不是根据输入内容显示不同的信息）。

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 Platform

## 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辅助工具

## HackBar与TamperData的使用

## 使用HackBar模拟请求

## 使用TamperData修改提交的数据

## Fiddler(Watcher/x5s)

# XSS漏洞挖掘

XSS实例

https://xss-game.appspot.com/

答案:http://www.freebuf.com/articles/web/36072.html

# XSS防御

XSS的一些基本转义

html\_escape

javascript\_string\_escape

url\_escape

css\_string\_escape

推荐：《给开发者的终极XSS防御备忘录》

设置字符编码和content-type

字符编码：避免如utf-7 XSS等问题

Conent-type：避免如Json的XSS等问题

HTTP响应头的一些XSS防护指令





## PHP的XSS防护

echo htmlspecialchars($string, ENT\_QUOTES | ENT\_XHTML, 'UTF-8');

## JAVA的XSS防护

使用WASP Java Encoder

Coverity Security Library(CSL)



OWASP ESAPI(The OWASP Enterprise Security API)



## .NET的XSS防护

HttpUtility Class(System.Web.HttpUtility)



AntiXSSencoder类(System.Web.Security.AntiXssEncoder于.NET 4.5)





## Ruby on Rails 框架中的XSS防护







## Python Django框架中的XSS防护

