



中國人民大學

RENMIN UNIVERSITY OF CHINA

信息学院

SCHOOL OF INFORMATION

新生研讨课
(网络空间的安全攻防)

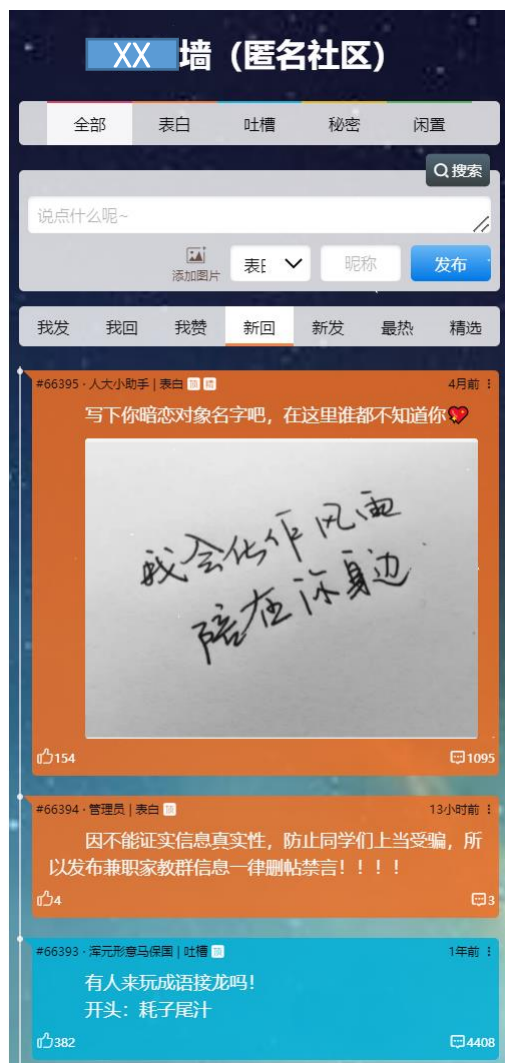
2. Web安全概述

授课教师：游伟 副教授

授课时间：周一16:00 – 17:30（立德0412），周二14:00 – 15:30（教二2402）

课程主页：<https://rucsesec.github.io/cybersecurity>

引子



用户 (oZp[redacted]K4g) 发表过5篇帖子

id: 5848151	nickname: 21图灵程设	time: 2021-12-01 19:11:23
id: 6159625	nickname: test	time: 2022-01-12 17:57:15
id: 6299038	nickname: 新生研讨课	time: 2022-02-15 16:40:01
id: 6322407	nickname: 图灵新生研讨课	time: 2022-02-21 14:17:31
id: 6327481	nickname: 明理新生研讨课	time: 2022-02-22 10:56:25

攻击1：爬取相同匿名用户的发帖信息

攻击2：嗅探/爆破xx墙管理员密码，
以其身份删除留言、禁言用户

进入管理模式

请输入管理员密码

取消 确定

@Ta

隐藏

封禁作者

攻击3：窃取用户ID和身份凭证，
以其身份发表言论



攻击4：诱骗用户授权，获得其昵称和头像

申请

获取你的昵称、头像

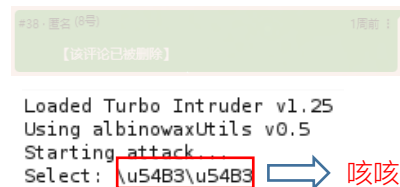
UV 微信昵称头像

使用其他头像和昵称

取消 允许

openid_wxwall	oZp[redacted]K4g
openid_myapp	oAp[redacted]Kfw
昵称	UV
头像	

攻击5：入侵匿名墙应用数据库，
查看已删除的帖子信息





目录

1. Web概述
2. Web应用程序概述
3. Web应用开发语言
4. Web应用安全概览

2.1 Web概述

- **万维网**（亦作Web、WWW、W3，全称World Wide Web），是一个由许多互相链接的超文本文档组成的系统
- 在这个系统中，每个资源由一个全局的统一资源标识符（**URI**）标识
- 资源通过超文本传输协议**HTTP**（Hypertext Transfer Protocol） / **HTTPS**（Hyper Text Transfer Protocol over SecureSocket Layer）传输
- 用户通常通过点击相应的**URL**链接来获得资源，URL是带有访问方式（如http://、https://、ftp://、file://等）的URI
- Web常被当成**互联网**的同义词，但其实Web仅仅是互联网（Internet）中的服务之一

2.2 Web应用程序概述

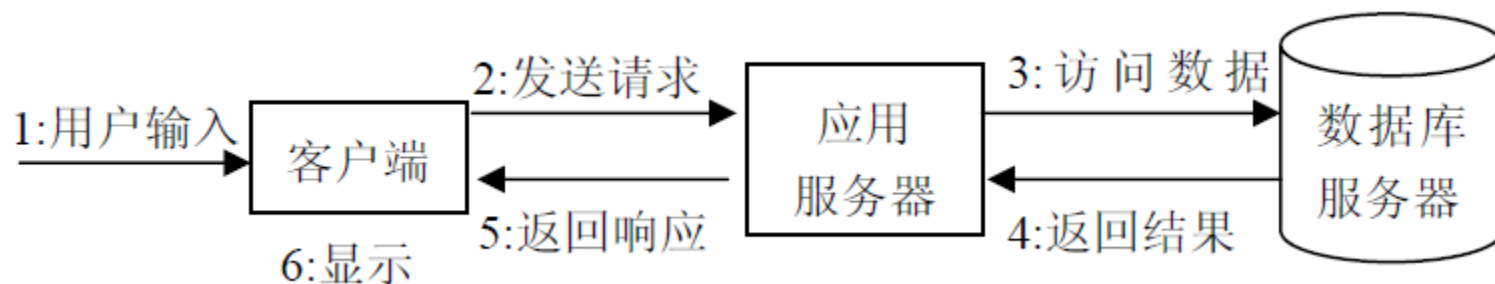
■ Web应用特点

- 与平台无关（便于开发，不同平台相同开发模式）
- 分布式（便于维护，客户端一般无需更新）

■ Web应用在架构上属于B/S（浏览器/服务器）模式

- 主要应用逻辑在服务器端实现，运行结果以Web页面形式返回到客户端
(用户难以直接操控服务端逻辑)
- 为缓解服务器端压力，部分逻辑在客户端本地以脚本形式运行
(客户端逻辑具有较大可操作空间)

■ Web应用的简要工作流程

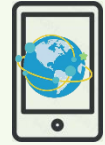
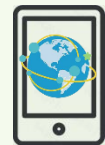


腾讯微信运营团队

小小微信墙开发者

xx墙管理员

普通用户



注册应用

App

返回AppId和AppSecret

申请应用服务

返回media_id和pass

发布人大墙地址
(带media_id的连接)

禁言用户(media_id, pass, openid)

返回设置结果

登陆匿名墙(media_id)

请求鉴权(AppId, AppSecret)

返回用户的openid

返回用户的openid及其对应的身份凭证vid

发表帖子(media_id, openid, vid, message)

返回发帖结果和帖子的cid

查看帖子(media_id, cid)

返回帖子内容

服务器端

客户端

2.3 Web应用开发语言

■ 服务器端程序设计语言：

- PHP (PHP: Hypertext Preprocessor) , 是一种可嵌入HTML、可在服务器端执行的内嵌式脚本语言。其语法混合了 C、Java、Perl 。PHP执行效率比CGI要高许多 (可由Web服务器的线程来解释执行)
- JSP (Java Server Pages) , 是Sun公司提出的一种动态网页技术标准, 在传统的网页HTML文件中嵌入Java程序段 (Scriptlet) 、Java表达式 (Expression) 或者JSP标记 (tag) , 从而形成实施应用逻辑的JSP文件
- ASP (Active Server Page) , 意为“动态服务器页面”, 是微软公司开发的一种编程规范, 主要运行于微软的Web Server服务器IIS上, 可方便地与数据库和其它程序进行交互
-

2.3 Web应用开发语言

■ 客户端程序设计语言：JavaScript（事实上的标准）

- JavaScript是一种基于对象和事件驱动脚本语言，主要运行于客户端。客户端浏览器可以直接解释执行JavaScript（新版浏览器中的JavaScript引擎为了提高效率加入了JIT运行时编译）
- 一些不用和服务端打交道的界面交互逻辑（如动态界面、账号是否为空的判断等），可以直接用JavaScript在客户端实现，提高用户体验，减轻服务器的负担
- 浏览器需要包含有JavaScript的解释执行引擎，乃至编译器（Chrome中的JavaScript引擎：V8）
- 经过多年快速进化（浏览器竞争十分激烈！），JavaScript的效率得到了极大的提高，使得JavaScript语言已经被用于桌面和服务端程序设计（可不一定是Web应用），如Node.js

2.4 Web应用安全概览

- URL安全：通过URL来对Web应用进行攻击是一种最为简单的攻击方式，但危害不可忽视。URL攻击主要利用：服务器端参数检测的不完备、以及嗅探关键的参数信息
- 跨站脚本攻击：一种浏览器中的代码注入漏洞，在远程的Web页面的HTML代码中插入具有恶意目的的代码。当用户访问此页面时，用户浏览器将会执行嵌入其中的脚本
- SQL注入：是现今存在最广泛的WEB漏洞之一。标准的数据库操作是通过SQL语言进行。当攻击者可以影响到数据库服务器执行的SQL语句的构成时（而非只是查询参数），则会导致SQL注入漏洞