



1. Web安全概述

授课教师：游伟 副教授

授课时间：周二10:00 – 11:30 (教二2111)

上机时间：周二12:00 – 13:30 (理工配楼二层机房)

课程主页：<https://www.youwei.site/course/websecurity>

引子



为什么当代大学生爱用匿名墙:

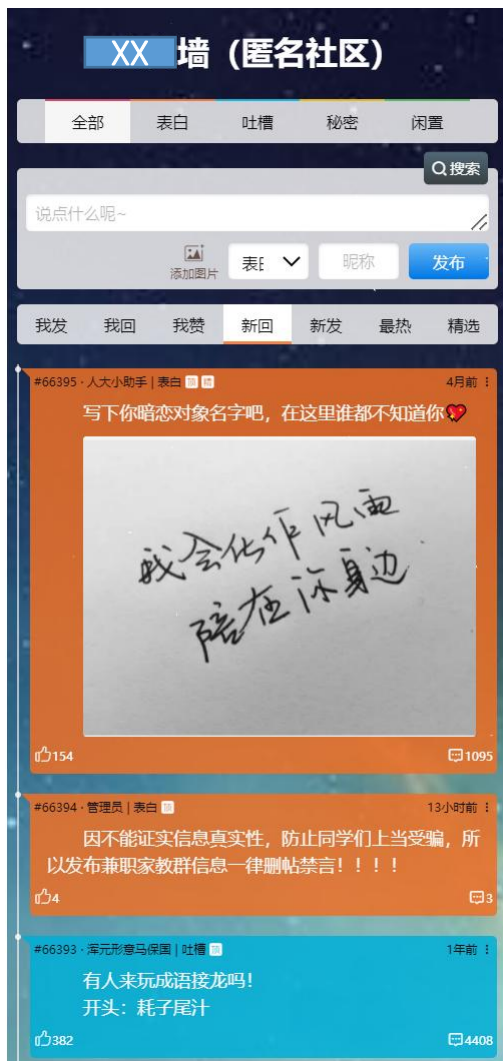
- 匿名性
- 言论自由

匿名墙中的当代大学生关注热点:



by 潘俊达 (21图灵)

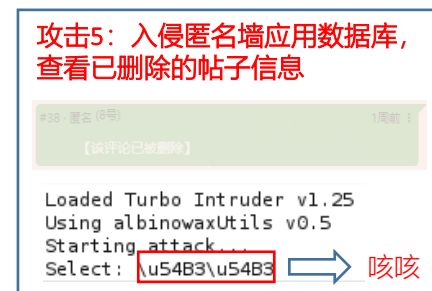
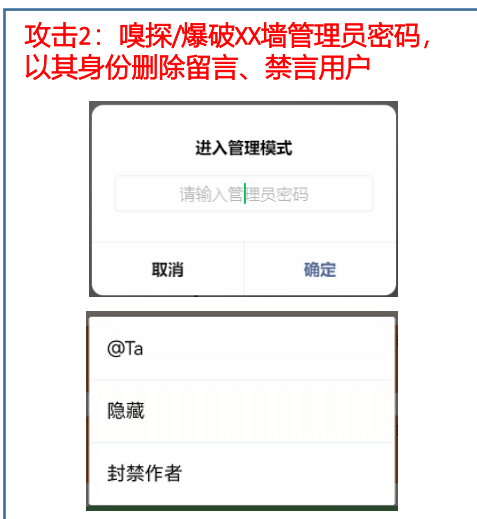
引子



用户 (oZp[redacted]K4g) 发表过5篇帖子

攻击1: 爬取相同匿名用户的发帖信息

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



引子

The screenshot displays a Windows 10 desktop environment. The central focus is a Tencent Meeting window titled "腾讯会议" (Tencent Meeting). The meeting interface shows a grid of participants: "UV的屏幕共享" (UV's screen sharing), "陶俊屹", "薛钦亮", "甘秋燕2021201731", "张扬扬", and "石孟洲". The main content area of the meeting displays a slide titled "人大墙 (匿名社区)" (Renmin University Wall (Anonymous Community)). The slide content includes a search bar for "信息学院周" (Information School Week), a list of posts, and a QR code. A red warning box on the slide reads: "攻击5: 入侵匿名墙应用数据库, 查看已删除的帖子信息" (Attack 5: Breach of anonymous wall application database, view deleted post information). Below the QR code, there is a terminal-like output: "Loaded Turbo Intruder v1.25 Using albinovxutils v0.5 Starting Attack Select: LUS4B3U54B3" with a "爆破" (Exploit) button.

Surrounding the meeting window are other desktop elements: a File Explorer window on the left showing a folder structure with "ppt" files; a taskbar at the bottom with various application icons and a system tray showing the time as 11:01 on 2022/4/23; and a right-side panel with system information like "U盘(F:) 安全防护已开启" and "剩余空间: 453.3G".

网络空间安全的伦理规范

- 【被试者知情】告知实验对象即将参与的实验内容和可能造成的危害
- 【最小化危害】将危害降低到最小限度
- 【受限环境】尽可能在测试环境而非真实中进行实验
- 【恢复初始状态】实验完成后，尽可能恢复所造成的损害
- 【科技向善】不用所掌握的知识作恶和非法牟利

网络空间安全的伦理规范

■ 匿名墙给我们的启示

- 网络不是法外之地，言论自由要建立在法律和道德框架内
- 互联网是有记忆的，黑历史会长久留下痕迹
- 理性吐槽、合理发表意见，避免肆无忌惮、无端谩骂地匿名“喷喷”

做负责任的安全研究人员



新人大墙漏洞报告

作者：人大信息学院21级图灵班崔钰锟、潘俊达

邮箱：1572161937@qq.com

我们针对新人大墙展开了一系列安全测试和攻击测试，发现其存在比较明显的可利用的安全漏洞。

我们的发现如下：

漏洞	严重性
敏感接口未进行权限验证	高危
openid 可篡改	中危
管理员权限仅通过 openid 检验	高危

.....

可能影响

控制台一行命令就可以使用和管理员一样的功能，操作难度比发包还低，传播开后极容易被各种人利用。

修改建议

管理员应该用更强的验证手段保护，至少加入密码，同时应该是强密码，否则可能会被爆破出来。

总结

我们重点关注了 `openid` 的问题。

首先为了匿名墙的匿名性，他人的 `openid` 是绝不可以被任何手段获取的。

另外是管理员的 `openid` 已经泄露了，所以如今再修补隐蔽获取 `openid` 的接口可能为时已晚。我们建议慎重考虑是完善服务端对管理员 `openid` 的验证，还是直接抛弃，转而用密码等方式。

- 发现漏洞后及时上报
- 撰写完善的漏洞报告
- 积极协助修复漏洞
- 在漏洞修复前不公布信息
- 不利用漏洞牟利

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
5. 身边的Web应用安全问题

1.1 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

1.2 Web应用程序概述

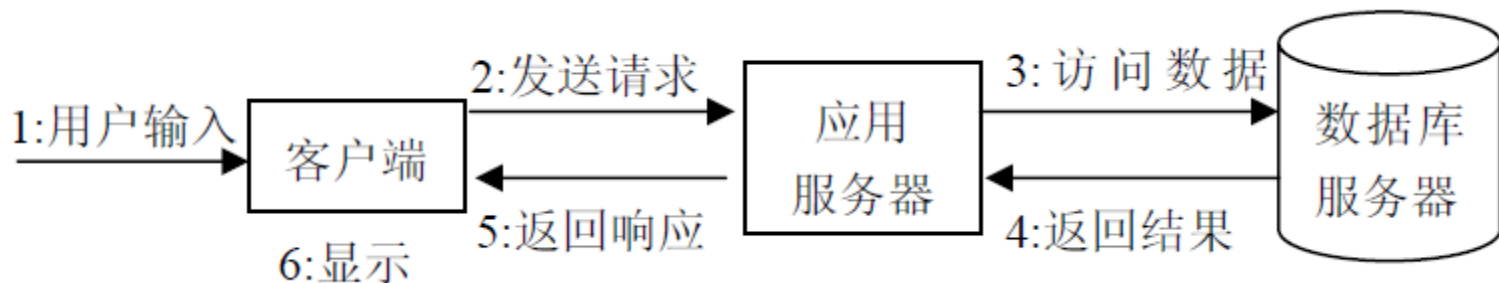
■ Web应用特点

- 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



1.2 Web应用程序概述

■ 每一次浏览网站

🌐 1. DNS解析——找到目标

当你输入一个网址时，其实你是在和一个“名字”打交道，但互联网只理解“IP地址”（就像邮递员只认地址）。浏览器会先查看本地缓存，看看有没有这个地址。如果没有找到，就会去问DNS服务器，最终得到目标服务器的IP地址。

🔑 2. TCP连接——建立通道

通过IP地址找到目标后，浏览器和服务器通过TCP协议建立一条安全稳定的连接，这就是俗称的“三次握手”。

第一次：浏览器问“你在吗？”

第二次：服务器回应“在呢，你找我？”

第三次：浏览器说“好，那我们正式沟通吧！”

📄 3. HTTP请求/响应——提出要求/获得反馈

连接建立后，浏览器向服务器发出“请求”（HTTP/HTTPS协议）。比如说：“请给我首页的数据（HTML、CSS、JS等）！”如果一切正常，服务器会返回状态码200，表示成功响应。如果服务器忙不过来或者发生错误，可能会返回404（找不到页面）或500（服务器出错）。

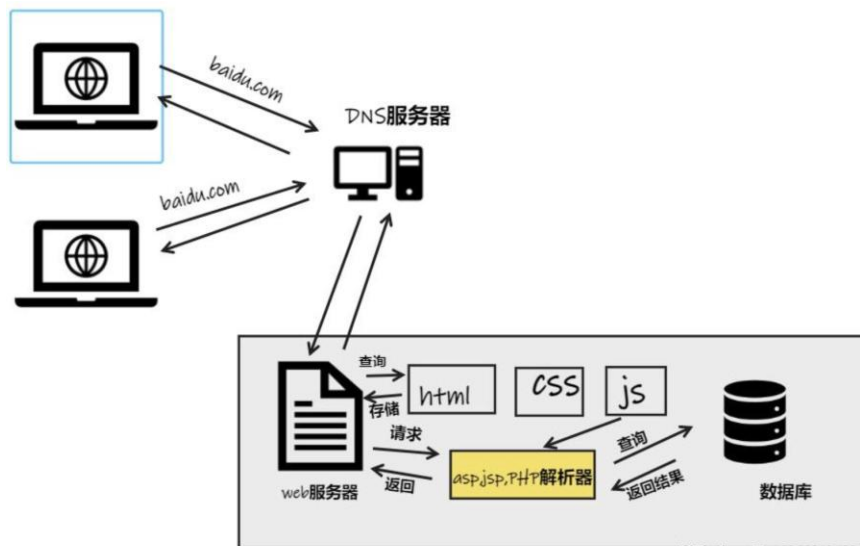
📄 4. 页面加载——拼装内容

拿到服务器返回的HTML后，浏览器开始分步骤“组装”页面：

解析HTML：找到需要加载的内容和引用的资源（CSS、JS、图片等）。

渲染页面：通过渲染引擎把代码翻译成你看到的页面，并执行JS代码来完成交互功能。

绘制图层：逐层渲染后，屏幕上呈现出完整的页面。

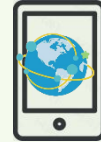
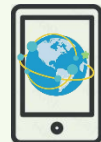
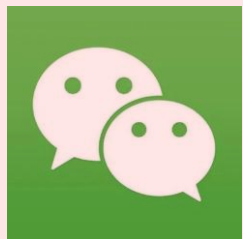


腾讯微信运营团队

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

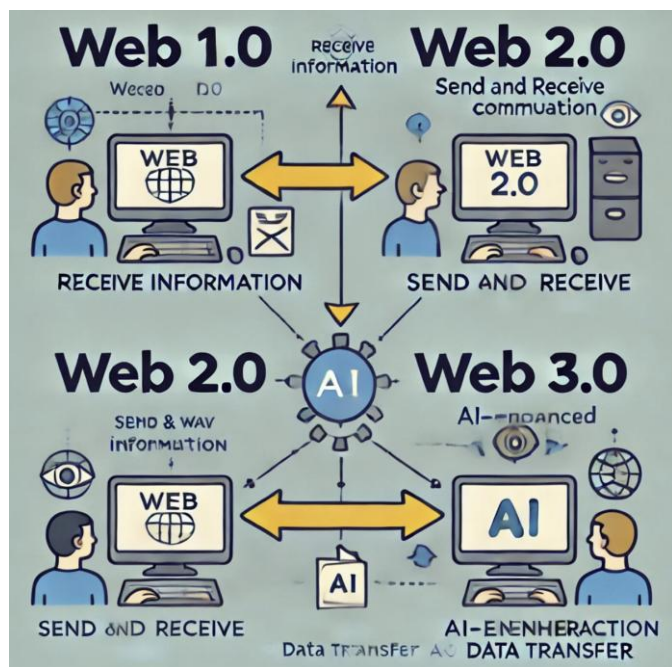
服务器端

客户端

1.2 Web应用程序概述

■ Web发展简史

- 被动的Web 1.0：打开一个电子图书应用，只能看书架上已有的书
- 交互的Web 2.0：不仅可以看已有的书，还可以进行评价
- 智能的Web 3.0：除了浏览和评价，还会根据浏览历史自动推荐



1.3 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
-

1.3 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）
- 一些不用和服务器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

示例：验证用户名和密码是否正确

```
1 <html>
2 <head>
3   <title>login</title>
4 </head>
5
6 <body>
7
8 <?php
9 $username = $_GET["username"];
10 $password = $_GET["password"];
11
12 if ($username == "admin" &&
13     $password == "1234567") {
14   echo "login succeeded";
15 } else {
16   echo "login failed";
17 }
18 ?>
19
20 </body>
21 </html>
```

```
1 <html>
2 <head>
3   <title>login</title>
4 </head>
5 <body>
6 <script>
7   function validate() {
8     var username = document.getElementById("username").value;
9     var password = document.getElementById("password").value;
10    if (username == "" || password == "") {
11      alert("Please input username and password");
12      return false;
13    }
14    return true;
15  }
16 </script>
17 <form action="login.php" method="get" onsubmit="return validate()">
18   username: <input id="username" name="username" type="text" />
19   <br/>
20   password: <input id="password" name="password" type="password" />
21   <br/>
22   <input type="submit" value="submit" />
23 </form>
24 </body>
25 </html>
```

服务器端

login succeeded

login failed

username:

password:

客户端

1.4 Web应用安全概览

- 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。
- 客户端逻辑劫持：是指攻击者通过篡改前端代码或利用漏洞，操纵客户端逻辑以执行未经授权的操作，从而窃取数据或破坏应用功能。客户端逻辑主要通过JavaScript代码实现，可以通过“开发者工具”进行客户端调试。
- 越权攻击：Web应用程序中一种常见的漏洞，Web应用十大安全隐患的第二名。该漏洞是指应用在检查授权时存在纰漏，使得攻击者在获得低权限用户账户后，利用一些方式绕过权限检查，访问或操作其他用户或者更高权限。

1.5 身边的Web应用安全问题



刘博宇2021201675的个人会议室

会议号：979 510 7602

开始录制时间：2023/10/22 22:39:14

创建者：刘博宇2021201675

1.5 身边的Web应用安全问题

微人大 | 中国人民大学 | 高校网络安全管理运维赛 | YOJ2.0 首页

不安全 | yoj.ruc.edu.cn/index.php/index/index/index.html

YOJ2.0 首页 题库 考试 评测 排名 课程 登录

热门题目

ID	标题
788	基数排序练习
787	快速排序练习
790	二维查找树
791	平面最近点查询
803	Longest Common Subsequence
802	Weighted Interval Scheduling
786	矩阵乘法
785	平面最近点对
680	棍子的长度
661	五、移动火柴

开发者寄语

本网站建议使用 [Chrome](#), [Edge](#), [Safari](#), [Firefox](#) 等主流浏览器。不支持IE。联系我们

一言

极霸矛，相阿痕啊啊。
——中华inm

最近更新

ID	标题
1138	Rank
1137	test_oj
1135	圆覆盖
1134	圆
1133	球心
1128	管理公司
1127	社交网络
1126	最大团
1125	朋友
1124	牧场的安排

排名(昵称可在登录后前往"修改资料"编辑)

#	昵称	个性签名	通过题目数
1	哼，哼，哼，啊啊啊啊 啊啊啊啊啊啊啊啊	逸一时，误一世	346
2	满好好好	天不生我汉维贾ruc万古如长夜511名 小哥哥好厉害我也有个人网站啦 cnblogs.com/DVDx	304
3	何如屋漏痕	凤凰于飞，翱翔其羽	303
4			291

28°C 局部晴朗 17:33 2024/4/25

1.5 身边的Web应用安全问题

 腾讯会议

刘博宇2021201675的个人会议室

会议号：979 510 7602

开始录制时间：2023/12/15 14:58:23

创建者：刘博宇2021201675

1.5 身边的Web应用安全问题

