



第一讲 Web安全概述

陈伟

Email: chenwei@njupt.edu.cn

Tel: 18951896489



课程内容

1

课程概况

2

Web安全现状

3

什么是Web应用

4

脆弱的Web应用

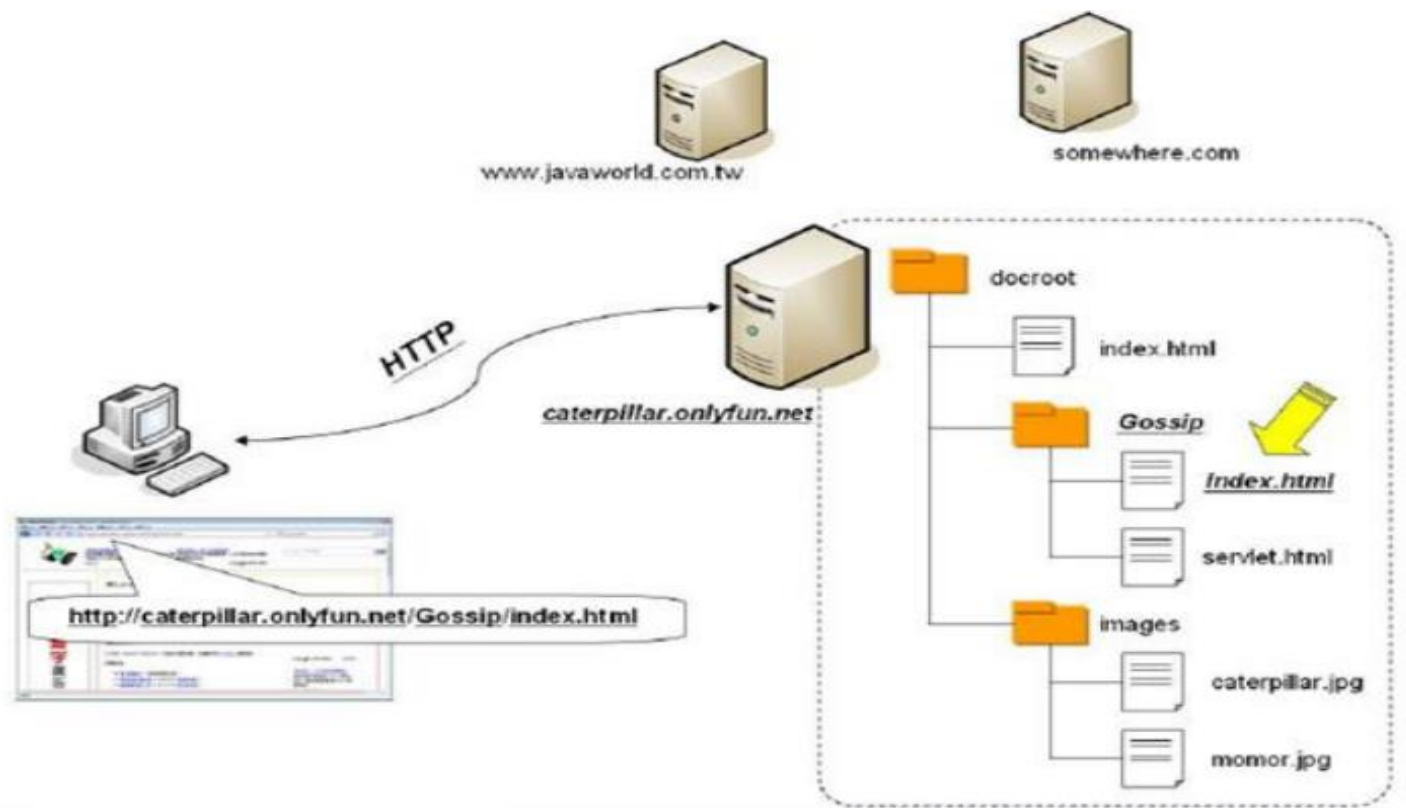
5

什么是Web安全



什么是Web应用？

❖ 通常情况下，我们了解到的Web应用是指提供Web服务的应用系统，其实通俗讲就是一个网站。



Web应用



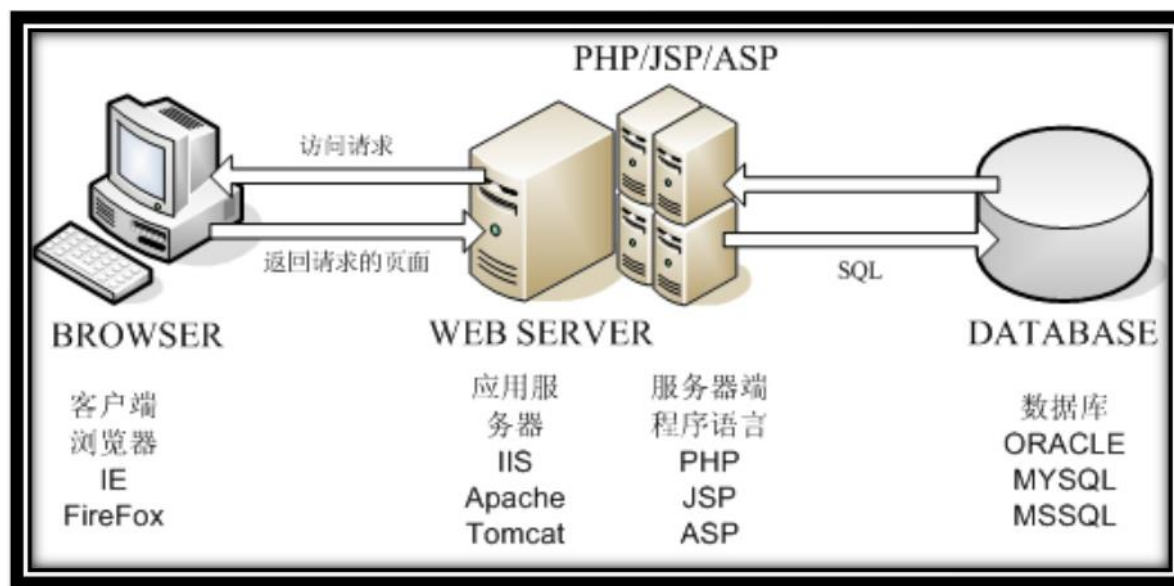
❖ Web应用对于我们现在的生活已经越来越紧密了，去搜资料、网上购物、看视频、玩游戏、社交等等活动都与Web应用息息相关。

❖ 现在大部分的单位、公司都会建立自己的门户网站。而且我们只需要使用客户端(浏览器)就可以对这些Web应用进行访问了



Web应用系统架构

- ❖ 实际上一个Web应用并不是我们所理解的那么简单，它是一个由多个要素构成的系统。Web应用程序的设计者、Web应用服务器、动态脚本引擎、数据库是构成Web应用必不可少的要素



脆弱的Web应用

- ❖ 有时候我们在访问网站的时候经常会看见各种各样的奇怪的事物，比如博彩、黑页、暗链、反共等等事件出现在各大网站上。

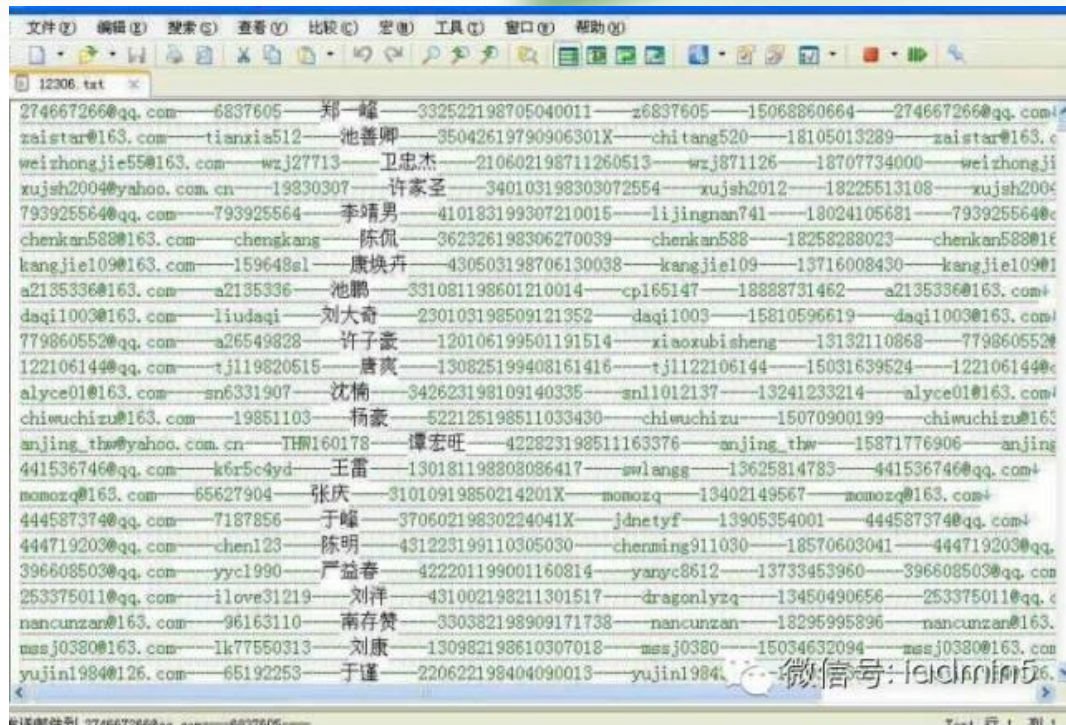




```
Chrome 文件 编辑 视图 历史记录 书签 用户 窗口 帮助
view-source:www.监察网- gov.cn
view-source:www. gov.cn/index.php
407 <div><br /><br /></div><div><br /><br /></div><div><br /><br /></div>
408 <div><br /><br /></div><div><br /><br /></div><div><br /><br /></div>
409 <div><br /><br /></div><div><br /><br /></div><div><br /><br /></div>
410 <div><br /><br /></div><div><br /><br /></div><div><br /><br /></div>
411 <div><br /><br /></div><div><br /><br /></div><div><br /><br /></div>
412 <div style="padding:0px">
413 <a href="http://" www.fhdgkj.com" target="_blank">太湖字谜汇总更新
414 <a href="http://www.whcgkx.com" target="_blank">3d钓叟太湖字谜</a>
415 <a href="http://www.whdgkc.com" target="_blank">三d字谜太湖今天</a>
416 <a href="http://www.nsgrfb.com" target="_blank">今日3d字谜总汇</a>
417 <a href="http://www.nsgrfw.com" target="_blank">3d焰舞字谜今天</a>
418 <a href="http://www.nssrfl.com" target="_blank">3d字谜总汇大全</a>
419 <a href="http://www.khygkw.com" target="_blank">真实谎言3d字谜</a>
420 <a href="http://www.nsgrft.com" target="_blank">今日3D太湖字谜</a>
421 <a href="http://www.whjgkk.com" target="_blank">太湖字谜3d太湖</a>
422 <a href="http://www.whjgkg.com" target="_blank">3d钓叟太湖字谜</a>
423 </div>
424
425 <div>
426 <a href="http://www.giblar.com" target="_blank" >真人ag</a>
427 <a href="http://www.lywmhq.com" target="_blank" >ag亚游</a>
428 </div>
429
430 </div>
431
432 </div>
433 </div>
434
435 </div>
```



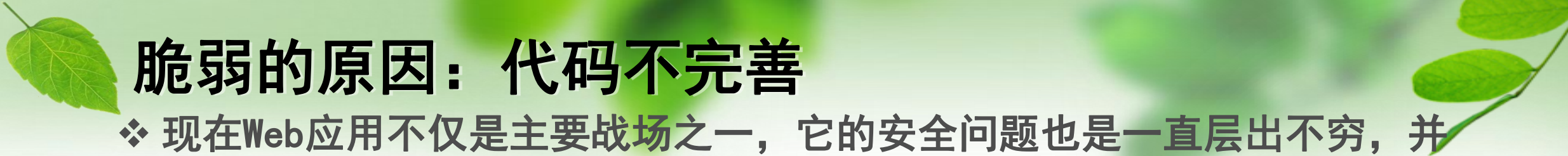
拖库攻击



2020年赏金最高的十大漏洞类型

- ❖ 根据HackerOne发布的十大漏洞列表，跨站点脚本（XSS）仍然是影响力最大的漏洞，因此该漏洞在2020年连续第二年为白帽子黑客获得了最高的回报——2020年为黑客赢得了420万美元的漏洞赏金，比2019年增长了26%

| | Weakness Type | Bounties Total Financial Rewards Amount | YOY % Chage |
|----|---|---|-------------|
| 1 | XSS | \$4,211,006 | 26% |
| 2 | Improper Access Control - Generic | \$4,013,316 | 134% |
| 3 | Information Disclosure | \$3,520,801 | 63% |
| 4 | Server-Side Request Forgery (SSRF) | \$2,995,755 | 103% |
| 5 | Insecure Direct Object Reference (IDOR) | \$2,264,833 | 70% |
| 6 | Privilege Escalation | \$20,017,592 | 48% |
| 7 | SQL Injection | \$1,437,341 | 40% |
| 8 | Improper Authentication - Generic | \$1,371,863 | 36% |
| 9 | Code Injection | \$982,247 | -7% |
| 10 | Cross-Site Request Forgery (CSRF) | \$982,247 | -7% |



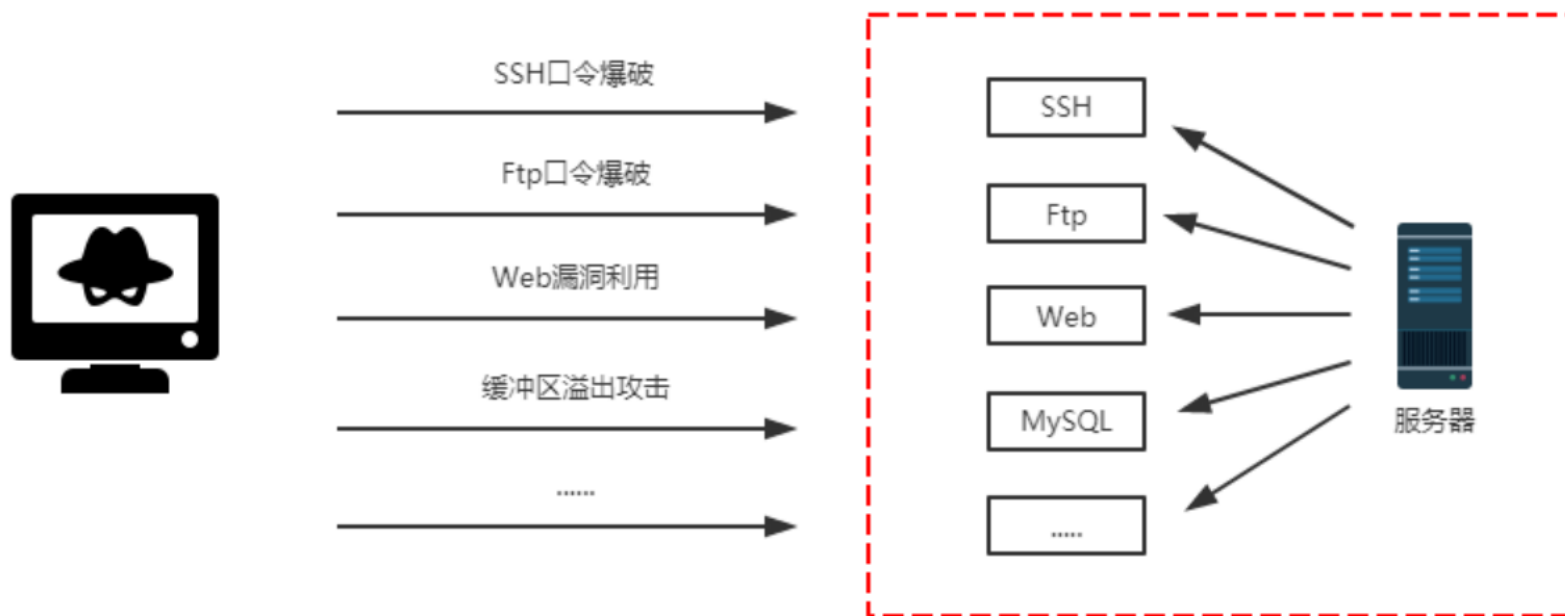
脆弱的原因：代码不完善

- ❖ 现在Web应用不仅是主要战场之一，它的安全问题也是一直层出不穷，并且到现在仍没有被冲淡。原因有很多：
 - 程序开发人员没有安全意识。开发者不知道哪里的代码存在“Bug”，功能的确是开发完成了，但是开发的代码上出现了漏洞。
 - 有经验的程序员可能会考虑安全问题，但毕竟不是专业的安全人员，并且并不是每一个人都是“大牛”。
 - 当项目上线之后的服务器环境可能会有变化，本来没有问题的代码可能就变得有问题了。
 - 后台管理的弱口令、一些配置型错误等都会存在安全问题。
- ❖ 并且对于攻击者的技术门槛也并不高，所以对于它的很多攻击手段并没有我们想象中的那么“难”



脆弱的原因：端口开放

- ❖ 对于服务器的入侵方式有很多，比如端口扫描、SSH口令爆破、Ftp爆破、缓冲区溢出攻击等等去直接获取目标的权限。
- ❖ 由于现在Web应用的飞速发展，现在战场逐渐转移到了Web之上





什么是Web安全？

- ❖ Web应用安全是现代计算机安全界中的一个重要组成部分。自互联网出现以来，关于Web应用的安全问题就一直层出不穷。
- ❖ 我们常说的Web安全一般是指Web应用中存在着的不安全的隐患，对于这些不安全的隐患，我们常称之为“漏洞”。
- ❖ 黑客利用网站操作系统和Web服务程序的各类漏洞得到Web服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。

