2021-2022学年秋季学期

Web安全技术

Web Security

授课团队：刘奇旭、刘潮歌

助　　教：陈艳辉、杨毅宇、李寅

Web安全技术

Web Security

课程简介

刘奇旭

liuqixu@iie.ac.cn

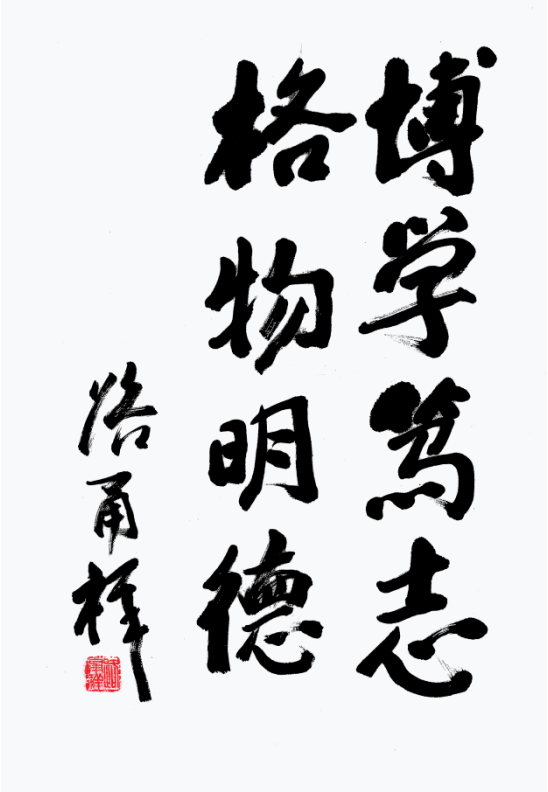
2021年09月07日

中国科学院大学
University of Chinese Academy of Sciences

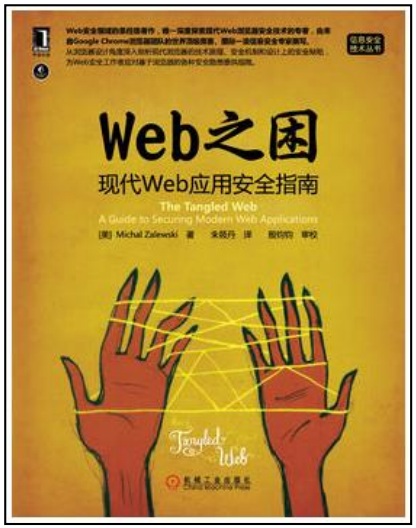
课程简介

课程类型：专业普及课

- **学时学分：40学时 / 2学分**
- **上课时间&地点（雁栖湖）**
  - 周二，3～4节课(10:30-12:10)，教1-009
  - 周四，3～4节课(10:30-12:10)，教1-009
- **预修课程：无**
- **课程教材：文献阅读**
- **授课周次： 2~12周**



主要参考书目


Web之困
现代Web应用安全指南
The Tangled Web
A Guide to Securing Modern Web Applications
Tangled Web


白帽子讲
Web安全


Broadview
Web前端
黑客技术揭秘


CTF
特训营
CTF
SPECIAL
TRAINING
CAMP
技术详解、解题方法与
竞赛技巧
FlappyPig战队 —— 著

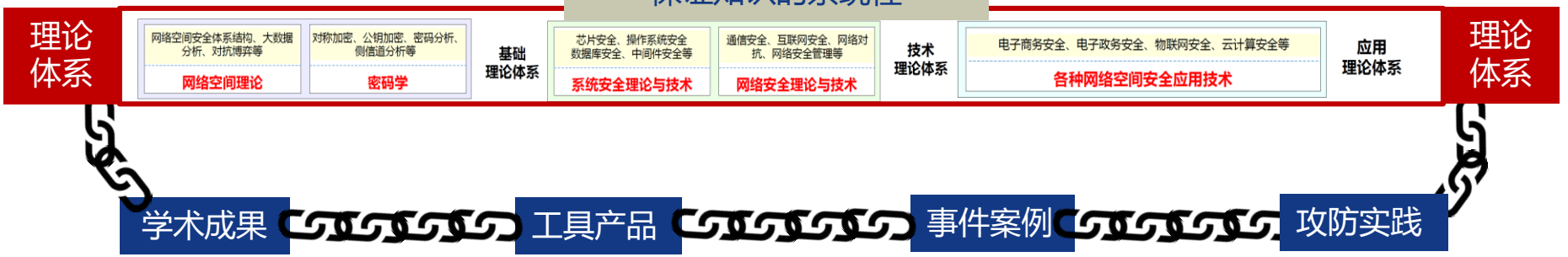
开课目的

- 本课程为网络空间安全及相关学科研究生的专业普及课。
- 掌握Web安全技术的基础概念及原理。
- 熟知Web安全技术的问题及解决方案。
- 跟进国内外学术界及工业界最新进展。
- 加强Web安全实践。

授课方法

知识链牵引

保证知识的系统性



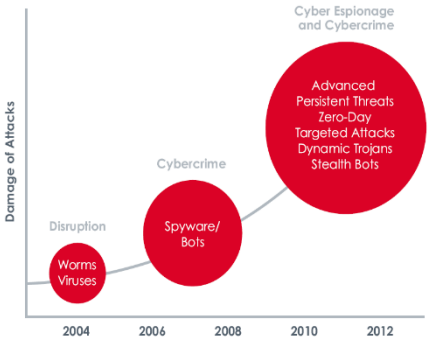
中国计算机学会推荐国际学术会议
(网络与信息安全)

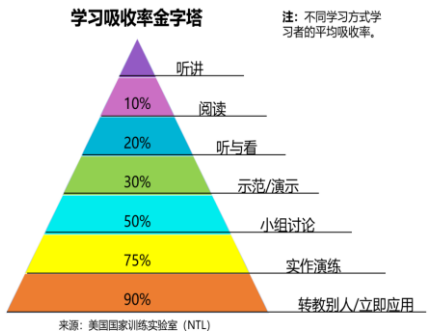
A类

序号	刊物名称	刊物全称	出版社
1	CCS	ACM Conference on Computer and Communications Security	ACM
2	CRYPTO	International Cryptology Conference	Springer
3	EUROCRYPT	European Cryptology Conference	Springer
4	S&P	IEEE Symposium on Security and Privacy	IEEE
5	USENIX Security	Usenix Security Symposium	USENIX Association

新兴领域安全技术		国外厂商	国内厂商
云安全	流量分析、恶意样本分析、虚拟化安全等	趋势科技、迈克菲、卡巴斯基、Cisco、美特尔、EMC、亚马逊、谷歌等	阿里、腾讯、百度、华为、山石网科、杭州安恒、网康科技、
数据安全	数据加密、自然语言处理、数据挖掘与聚类分析等	赛门铁克、迈克菲、趋势科技、RSA 等	启明星辰、天融信、绿盟科技、神州泰岳、时代亿信、明朝万达、中国软件、中电长城网际、上海观安、360、亿阳、鼎普等
APT 攻击检测与防护	网络流量分析、恶意样本分析、关联分析、网络及终端取证等	FireEye、Bit9、趋势科技、RSA 等	360、阿里（瀚海源）、安天、知道创宇、绿盟科技、金山安全等
威胁情报分析及安全态势感知	爬虫技术、关键字匹配、模板数据分析、机器学习、可视化、社会工程学等	戴尔、赛门铁克、迈克菲、FireEye、RSA 等	360、阿里（瀚海源）、知道创宇、安天、微步在线等
智能制造安全	兼容协议、轻量级设备、攻击识别、基础防护等	GE、西门子、英特尔、AT&T 等	和利时、浙大中控、四方继保、南京自动化、三维力控、北京亚控；绿盟、启明星辰、天融信、中科网威匡恩网络等

来源：中国信息通信研究院





紧跟国内外学术界进展

了解国内外工业界情况

加强代入感 让知识可见

加深对课堂讲授内容的理解

课程大纲

- **第一部分：基础知识**
- **介绍Web安全定义与内涵，国内外现状与趋势、近年来重大网络安全事件等；介绍本课程所需掌握的基础知识，包括HTTP/HTTPS协议、Web前后端编程语言、浏览器安全特性等。**
- 1.1 绪论
- 1.2 Web的简明历史
- 1.3 同源策略
- 1.4 HTTP与Cookie

课程大纲

- **第二部分：Web客户端安全**
- **详细讲解XSS跨站、跨站点请求伪造、点击劫持等前端安全。**
- 2.1 OWASP Top Ten
- 2.2 XSS与CSRF
- 2.3 ClickJacking
- 2.4 浏览器与扩展安全
- 2.5 案例分析

课程大纲

- **第三部分：Web服务器端安全**
- **详细讲解SQL注入、文件上传、文件包含、身份认证与访问控制、Web服务器配置等后端安全。**
- 3.1 SQL注入
- 3.2 文件上传与文件包含
- 3.3 XXE与SSRF
- 3.4 身份认证与访问控制
- 3.5 案例分析

课程大纲

- **第四部分：Web安全实践**
- **实践是本课程的重要组成部分，采用课后大作业、课上研讨和Web渗透实战（CTF环境）等三种形式相结合的方法，加深对课堂讲授内容的理解，建立Web安全形象思维和意识。**
- 4.1 CTF之Web安全中期考核
- 4.2 CTF之Web安全期末考核
- 4.3优秀大作业课堂分享
- 4.4课程复习
- 4.5考前答疑

课程成绩

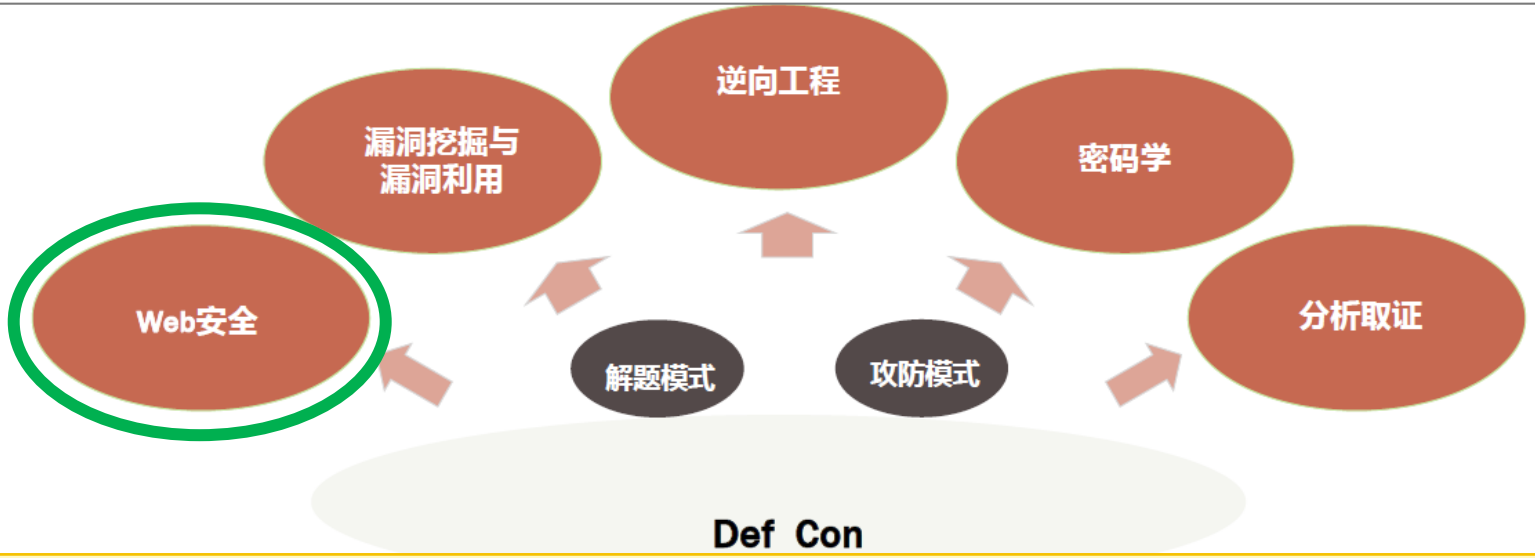
- CTF之Web安全中期考核：**10%**
- CTF之Web安全期末考核：**10%**
- 大作业：**30%**
- 期末考试：**50%**

课程成绩

CTF(Capture The Flag)

- CTF之Web安全中期考核：**10%**
- CTF之Web安全期末考核：**10%**

CTF(中文一般译作夺旗赛)，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会。



Web安全：通过浏览器访问题目服务器上的网站，寻找网站安全问题，利用网站的安全风险获取服务器的部分或全部权限，拿到Flag，提交到答题版上。

课程成绩

大作业

- **大作业：30%**
  - 大作业一个
  - 分组进行
  - 要求：认真思考，按时提交
  - 布置时间：待选课结束之后

课程成绩

期末考试

- **期末考试：50%**
  - 课堂开卷
  - 课堂讲述的重点内容

授课团队

刘奇旭　　博士、研究员、博士生导师　　课程首席教授

- 中国科学院信息工程研究所研究员、第六研究室G5群组(Web安全与溯源取证研究群组)组长，中国科学院大学岗位教授。中国科学院青年创新促进会会员，中国科学院朱李月华优秀教师。围绕网络攻防技术开展研究，曾获省部级科技进步一等奖1项。国家关键信息基础设施网络攻防实战演习裁判，“天府杯”国际网络安全大赛裁判，全国高校网安联赛(X-NUCA)技术委员会委员。任《Web安全技术》和《Web追踪前沿》课程首席教授。以培养攻防兼备实战型人才为目标，指导的学生获得多个实战类攻防演练大赛一等奖。

刘潮歌　　博士、副研究员、硕士生导师　　课程主讲教师

- 中国科学院信息工程研究所副研究员。2016~2018年任《Web安全技术》课程主讲教师；主要从事恶意代码原理、网络攻击追踪溯源和Web安全方向的研究工作，主持国家自然科学基金1项，参与科技部863课题/重点研发计划、国家自然科学基金、军队基础加强计划多项，在等国内外重要会议或期刊上发表论文20余篇。注重安全理论与攻防实践的结合，多次一线参与处置网络安全突发事件以及网络安全专项任务。

陈艳辉　　博士研究生　　教师助教

杨毅宇　　博士研究生　　学生助教

李寅　　硕士研究生　　学生助教

[2021秋]Web Security

群号：901651609

扫一扫二维码，加入群聊。

QQ

谢谢大家

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室

中国科学院大学
University of Chinese Academy of Sciences