課程名稱 Course Title	(中文) 軟體安全 (英文) Software Security		
授課教師 Instructor	Fang Yu	開課單位 Departments	MIS
學分數 Credit(s)	3	修課對象 Target Students	Graduate Students
課程目標 Course Objectives	Software security is becoming more important at an exponential rate since the continual increase in cyber/computer crimes. Over the last few years the necessity for software security has grown rapidly as web sites have been defaced, credit card information has been stolen, publicly available hacking tools have become more sophisticated and viruses and worms cause more damage than ever before. We will discuss modern software security issues in this course with an emphasis on how to secure programs with static source code analysis. Students will learn how to apply advance static analysis techniques and tools to develop more secure and more reliable software. Students will also have chance to polish their presentation skills by presenting selected security papers. At the end of this course, students shall have a clear view of software security and static analysis, and shall be familiar with common vulnerabilities and exploits, such as Cross Site Scripting and SQL Injections in Web applications, and integer and buffer overflows in legacy systems. Students shall also know how to detect, prevent and remove these software flaws in the systems/applications via static analysis.		
課程大綱 Course Description	1. Introduction to Software Security and Static Analysis (2~3 weeks) 1.1 The Software Security Problems 1.2 Code Review 2. Static Analysis Techniques (5 weeks) 2.1 Type Checking/Taint Analysis 2.2 Integer Analysis 2.3 String/Size Analysis 3. Pervasive Problems (5 weeks) 3.1 Handling Inputs 3.2 Buffer Overflows 3.3 Web Application Vulnerabilities 3.4 XML and Web Services 3.5 Privacy and Secrets 4. Static Analysis in Practice: (4 weeks) Source Code Analysis Exercises for Jave, C and PHP		
上課進度 Weekly Course Schedule	Part I: Introduction to Software Security and Static Analysis 2/22 The Software Security Problems 3/1 Static Analysis and Code Review		

	Part II: Static Analysis Techniques 3/8 Type Checking/Taint Analysis 3/15 Integer/Size Analysis 3/22 Grammar-based String Analysis 3/29 Automata-based String Analysis Part III: Pervasive Problems 4/12 Handling Inputs/Exceptions 4/19 Buffer Overflows 4/26 Cross Site Scripting Vulnerabilities 5/3 Injection Flaws 5/10 Other Web Application Vulnerabilities 5/17 XML and Web Services Part IV: Static Analysis in Practice 5/24 Source Code Analysis Exercises for Java 5/31 Source Code Analysis Exercises for PHP 6/7 Term paper presentation and discussion (I) 6/14 Term paper presentation and discussion (II)
教學方式 Instructional Method	Lecture (70%) and Paper Presentation/Discussion (30%)
課程要求 Course Requirements	
評量方式 Evaluation	Quiz 20% Participation 10% Paper Presentation 30% Term paper 40%
教材及參考書目 Textbooks & Suggested Materials	Textbook: Secure Programming with Static Analysis. By Brain Chess and Jacob West, Addison-Wesley Professional, 2007 Reference book: The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws. By Dafydd Stuttard and Marcus Pinto, Wiley Publishing, Inc, 2007 Some String Analysis Tools: - [Stranger] http://www.cs.ucsb.edu/~vlab/stranger - [JSA] http://www.brics.dk/JSA/ Selected Papers (Subject to Change): - Prateek Saxena, Devdatta Akhawe, Steve Hanna, Feng Mao, Stephen McCamant, Dawn Song. "A Symbolic Execution Framework for JavaScript."

	In *Proc. of the 31st IEEE Symposium on Security & Privacy (Oakland 2010)* - Fang Yu, Muath Alkhalaf, Tevfik Bultan. "Stranger: An Automata-based String Analysis Tool for PHP." Tool paper. In the Proceedings of the 16th International Conference on Tools and Algorithms for the Construction and Analysis of Systems *(TACAS 2010)* - Prateek Saxena, Steve Hanna, Pongsin Poosankam, Dawn Song. "FLAX: Systematic Discovery of Client-side Validation Vulnerabilities in Rich Web Applications." In *Proc. of the 17th Network and Distributed System Security Symposium (NDSS 2010)* - Gary Wassermann and Zhendong Su. "Static Detection of Cross-site Scripting Vulnerabilities." In Proc. of the 30th International Conference on Software Engineering *(ICSE 2008)* - Yichen Xie and Alex Aiken. "Static Detection of Security Vulnerabilities in Scripting Languages." In Proc. of the 15th USENIX Security Symposium *(USENIX 2006)* - William GJ Halfond, Alessandro Orso, and Panagiotis Manolios. "Using positive tainting and syntax-aware evaluation to counter SQL injection attacks." In Proc. of the 14th ACM SIGSOFT international symposium on Foundations of software engineering *(FSE 2006)*
課程相關連結網址 **Course Website**	- Class web site: http://www3.nccu.edu.tw/~yuf/course - OWASP: http://www.owasp.org/ - CVE: http://cve.mitre.org/
備註 **Remarks**	