OWASP EUROPEAN TOUR 2013 – Cambridge – 13th May 2013 Conference in Conjunction with Anglia Ruskin University – Department of Computing & Technology (Cambridge)

The OWASP European Tour objective is to raise awareness about application security in the European region, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

A series of activities such as free conferences, trainings sessions and awareness games will be provided by renowned professionals with the sole purpose of bringing high-quality content and a comprehensive breadth of security topics across the EU region .

Who Should Attend the European Tour?

- Application Developers
- Application Testers and Quality Assurance
- Application Project Management and Staff
- Chief Information Officers, Chief Information Security Officers, Chief Technology Officers, Deputies, Associates and Staff
- Chief Financial Officers, Auditors, and Staff Responsible for IT Security Oversight and Compliance
- Security Management and Staff
- Executives, Mangers, and Staff Responsible for IT Security Governance
- IT Professionals Interested in Improving IT Security
- Anyone interested in learning about or promoting Web Application Security

OWASP Europe TOUR, is an event across the European region that promotes awareness about application security, so that people and organizations can make informed decisions about true application security risks.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. Apart from OWASP's Top 10, most OWASP Projects are not widely used and understood. In most cases this is not due to lack of quality and usefulness of those Document & Tool projects, but due to a lack of understanding of where they fit in an Enterprise's security ecosystem or in the Web Application Development Life-cycle.

This event aims to change that by providing an insight into the issues of cybercrime, its impact and detection and a selection of mature and enterprise ready approaches together with practical examples of how to use them.

Background

OWASP (Open Web Application Security Project is a 501(c)(3) not-for-profit worldwide charitable organization focused on improving the security of application software. Their mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks.

The Department of Computing & Technology at Anglia Ruskin University is enhancing its curricula and capabilities in information security following its successful BSc(Hons) Information Security and Forensic Computing course.

Establishing a joint professional networking group with OWASP concentrating on aspects of computing and application security is a key part of this enhancement. A key aim the department is working towards is developing a MSc Information Security specialising in Application Security and as part of this activity looking to develop and a local Information Security Student Society.

Agenda

Time	Title	Speaker	Description
11:00	Registration & Refreshments (Outside LAB002)	-	-
11:45 (15 mins)	Introduction & Welcome	Adrian Winckles - OWASP Cambridge Chapter Leader & Senior Lecturer	Introduction to OWASP & Anglia Ruskin University Schedule for the Day
12:00 (45 mins)	Real Costs of Cybercrime	Ross Anderson (Cambridge University Computer Laboratory)	Following a systematic study of the costs of cybercrime, in response to a request from the UK Ministry of Defence following scepticism that previous studies had hyped the problem, each of the main

			categories of cybercrime we set out what is and is not known of the direct costs, indirect costs and defence costs {both to the UK and to the world as a whole. We distinguish carefully between traditional crimes that are now `cyber' because they are conducted online (such as tax and welfare fraud); transitional crimes whose modus operandi has changed substantially as a result of the move online (such as credit card fraud); new crimes that owe their existence to the Internet; and what we might call platform crimes such as the provision of botnets which facilitate other crimes rather than being used to extract money from victims directly.
12:45 (45 mins)	Three Legged Cybercrime Investigation and its Implications	DI Stewart Garrick (Metropolitan Police ECrime Unit)	DI Stewart Garrick has over 27 years experience in the Metropolitan Police Service, 22 years as a detective and 10 years as a Detective Inspector. His career has been spent primarily on major crime units engaged on both proactive and reactive investigations, including 5 years investigating murders, 3 years on the Homicide Task Force (a proactive unit targeting those who would commit murder) and 5 years managing covert operations against organised crime. In March 2011 he joined Scotland Yard's Police Central eCrime Unit. He has witnessed the PCeU's growth from 40 officers to over 100 and has managed several high profile investigations. He has recently taken charge of the unit's cadre of police and civilian forensic examiners who are integrated into the unit's dynamic investigative model. He has this year completed an MSc in Countering Organised Crime and Terrorism at UCL, with a dissertation examining the emergence of radicalising settings based on Situational Action Theory.
13:30 (45 mins)	OWASP Top 10 & Mobile Top 10	Justin Clarke - London OWASP Chapter Leader	The OWASP Mobile Security Project is a centralized resource intended to give developers and security teams the resources they need to build and

			maintain secure mobile applications. Through the project, our goal is to classify mobile security risks and provide developmental controls to reduce their impact or likelihood of exploitation. As part of the overall Mobile Project , the Top 10 Mobile Risks include M1: Insecure Data Storage M2: Weak Server Side Controls M3: Insufficient Transport Layer Protection M4: Client Side Injection M5: Poor Authorization and Authentication M6: Improper Session Handling M7: Security Decisions Via Untrusted Inputs M8: Side Channel Data Leakage M9: Broken Cryptography M10: Sensitive Information Disclosure
14:15 (45 mins)	Refreshments & Networking	LAB107	
15:00 (45 mins)	Everything We Know is Wrong	Eoin Kelly - OWASP Board Member	The premise behind this talk is to challenge both the technical controls we recommend to developers and also out actual approach to testing. This talk is sure to challenge the status quo of web security today. "Insanity is doing the same thing over and over and expecting different results." - Albert Einstein We continue to rely on a “pentest” to secure our applications. Why do we think it is acceptable to perform a time-limited test of an application to help ensure security when a determined attacker may spend 10-100 times longer attempting to find a suitable vulnerability? Our testing methodologies are non-consistent and rely on the individual and the tools they use. Currently we treat vulnerabilities like XSS and SQLI as different issues but

			the root causes it the same. – it's all code injection theory!! Why do we do this and make security bugs over complex? Why are we still happy with "Testing security out" rather than the more superior "building security in"?
15:45 (45 mins)	Tricolour Alphanumercial Spaghetti	Colin Watson - OWASP Project Leader	Do you know your "A, B, Cs" from your "1, 2, 3s"? Is "red" much worse than "orange", and why is "yellow" used instead of "green"? Just what is a "critical" vulnerability? Is "critical" the same as "very high"? How do PCI DSS "level 4 and 5" security scanning vulnerabilities relate to application weaknesses? Does a "tick" mean you passed? Are you using CWE and CVSS? Is a "medium" network vulnerability as dangerous as a "medium" application vulnerability? Can CWSS help? What is FIPS PUB 199? Does risk ranking equate to prioritisation? What is "one" vulnerability? Are you drowning in a mess of unrelated, classifications, terminology and abbreviations? If you are a security verifier and want to know more about ranking your findings more meaningfully, or receive test reports and want to better understand the results, or are just new to ranking weaknesses/vulnerabilities and want an overview, come along to this presentation. It will also explain why the unranked information-only ("grey" or "blue"?) findings might contain some of the best value information.
16:30 (45	tbc	Steven van der Baan - OWASP	

mins)		Cambridge Chapter Leader	

Registration

To register for this free event, please register online at

https://www.surveymonkey.com/s/OWASP-Tour-May2013

Please note there is no automatic notification or confirmation.

The meeting will be held in the Lord Ashcroft Building, Room LAB002 (Breakout Room LAB107 for networking & refreshments).

Please enter through the main entrance in the Helmore Building (East Road) and ask at reception.

Anglia Ruskin University
Cambridge Campus
East Road
Cambridge
CB1 1PT

Get further information on travelling to the university can be found at:

http://www.anglia.ac.uk/ruskin/en/home/your_university/anglia_ruskin_campuses/cambridge_campus/find_cambridge.html

Please note there is no parking at the University site. There are a number of pay and display car parks in the vicinity.