OWASP Cambridge Spring Chapter Meeting -Tuesday 17th April 2018

Tuesday 17th April 2018 17:30 – 20:30, Lord Ashcroft Building (LAB002/LAB006), Anglia Ruskin University, Cambridge.

Hosted by the Cyber Security Networking & Big Data Research Group, Anglia Ruskin University, and OWASP (Open Web Application Security Project) Cambridge Chapter

This evening is part of a series of evening events on raising awareness for local businesses & organisations on the issues of cyber security and cybercrime, what regulations and legislation do organisations need to be aware to protect themselves and what is considered best practice in these challenging times.

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 **Cyber Security, Networking & Big Data** (**CSNBD**) Research Group at Anglia Ruskin University has close working strategic relationships with industry, professional bodies, law enforcement, government agencies and academia in the delivery of operationally focused applied information and application security research. We have strong international links with professional organisations such as OWASP, BCS, ISC2, IISP & the UK Cyber Security Forum amongst others. The primary aims of CSNRG are to help the UK and partner nations to tackle cybercrime, be more resilient to cyber attacks and educate its users for a more secure cyberspace and operational business environment. These will be achieved through the investigation of threats posed to information systems and understanding the impact of attacks and creation of cyber-based warning systems which gathering threat intelligence, automate threat detection, alert users and neutralising attacks. For network security we are researching securing the next generation of software defined infrastructures from the application API and control/data plane attacks. Other key work includes Computer forensic analysis, digital evidence crime scenes and evidence visualisation as well as Cyber educational approaches such as developing Capture the Flag (CTF) resources and application security programs.

Speaker Biographies & Abstracts

Guest Speaker: Jonathon Brookfield –Security Research Group Director, Blackberry

Bio:

Jonathon Brookfield leads the Security Research Group at BlackBerry. He has been working in product security for over 12 years, with the last 6 years at BlackBerry. At BlackBerry he has been involved in improving the security of a range of products including BlackBerry OS, BlackBerry 10 and most recently the PRIV on the device side and BlackBerry ID and Enterprise Identity by BlackBerry on the services side.

Abstract: *"Security OAuth 2.0"*

Enterprise authentication and single sign-on is a frequently overlooked subject by developers and security testers and is often relegated to something that "just works" or stands in the way of accessing the application being assessed. As such, the finer details are frequently ignored or left to third-party libraries to implement. This talk aims to help penetration testers and developers understand OAuth 2.0 protocol, detailing its components, configurations and modes of operation. Common implementation pitfalls will be explored from first-hand experience of securing OAuth in the enterprise, and an example will be demonstrated of how a mistake in the implementation can lead to a compromise of applications relying on OAuth for authorisation.

Guest Speaker: Marc Wickenden, CEO, 4Armed.

Bio:

Marc cut his teeth looking after applications and infrastructure for various online financial services companies before venturing into consultancy and ultimately founding 4ARMED, a company focused on appsec and cloud computing. He part Dev, part Sec, part Ops (the cool kids call this DevSecOps I think) and his latest squeeze is all things Docker and Kubernetes.

Abstract: *"XXE - The Bug That Bit Me"*

XXE and me have history. It taught me a valuable lesson and we've been friends ever since. It's prolific yet still relatively unknown outside security testing circles.

It was a new addition to the OWASP Top Ten in 2017 and is unique compared to the other entries. In this talk I'll explain why, provide live demonstrations of how to find and exploit it based on real world examples I've found, show what it's impact can be and ultimately give you some tips to avoid it.

Provisional Agenda

17:30 – 18:15 Registration & Refreshments (LAB006)

18:15 – 18:30 Welcome from the OWASP Cambridge Chapter Leader, Adrian Winckles, Director of Cyber Security & Networking Research Group, Anglia Ruskin University – Overview of OWASP AppSec 2018 – London July 2nd – 6th & OWASP Open Security Summit 4th – 8th June 2018.

18:30 – 19:15 "*Security OAuth 2.0*" - Jonathon Brookfield –Security Research Group Director, Blackberry

19:15 – 20:00 "*XXE - The Bug That Bit Me.*"- Marc Wickenden, CEO, 4Armed.

20:00 – 20:15 Q & A & Close

Registration

To register for this free event, please register online at

https://www.eventbrite.com/e/owasp-cambridge-spring-chapter-meeting-tuesday-17th-april-2018-tickets-44728540268

The event will be held in the Lord Ashcroft Building, Room LAB002 (Breakout Room LAB006 for networking & refreshments).

Please enter through the Helmore Building and ask at reception.

Anglia Ruskin University
Cambridge Campus
East Road
Cambridge
CB1 1PT

Please note that there is no parking on campus. Get further information on travelling to the university.

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