IN AT THE DEEP END - CYBER

SECURITY UNIVERSITY CHALLENGES THE OWASP WAY

By Adrian Winckles, Anglia Ruskin University

For students who are studying information security related undergraduate or postgraduate courses there is often a dichotomy between the theory of their studies and the practical implementation of the knowledge and skills derived from those studies. In an ever competitive employment marketplace, it is no longer enough to be able to say “I’ve a 2:1 or 1st class honours degree, employ me”, the potential employer is looking for additional “value added” experiences that differentiate the candidates.

Major employers in the Information Security industry such as GCHQ and NCA use competitions such as the UK Cyber Security Challenge (http://cybersecuritychallenge.org.uk/) to provide this added valued in addition to the standard CV and interview process by seeing how individuals tackle specific “real world” security related problems, methodologies employed and factors such as teamwork considered. Increasingly within higher education courses (information security being no exception) there is both a need to build a sense of community with the student cohort by offering the engagement with extracurricular activities and meeting the aspirations for increasing the student’s employability prospects. These are also key indicators for student satisfaction with the NSS (National Student Satisfaction Survey).

Anyone who’s serious about giving students real life experience and encouraging engagement in the Cyber Security industry should be thinking along the lines of forming cohort teams to take part in industry supported/sponsored “hacking” competitions and “capture the flag” (CTF) events. These types of activities are often affiliated with larger security related conference such as those offered by OWASP, Blackhat, 44Con etc. One of the key objectives of such competitions is to directly engage university students studying information security related courses and give them hands-on challenges to push them beyond their initial studies. It also allows talent scouting to bring young talented cyber experts into the security community.

So how does one go about preparing for a team for one of these competitions?

Following on from a very successful OWASP AppSec Europe 2014 conference and University Challenge delivered at Anglia Ruskin University, Cambridge, we wanted to continue the momentum and engage our students with the next University Challenge @ OWASP AppSec Europe 2015 Conference in Amsterdam, RAI between 19th-22nd May. We offered the opportunity to our BSc(Hons) Information Security & Forensic Computing, BSc(Hons) Computer Science and MSc Information & Communication Technologies students for volunteers to engage in a 4 month program of 3-4 hours a week to undertake additional tuition and practice in application penetration testing and ethical hacking techniques prior to the competition in Amsterdam.

The methodology we adopted was:

• Starting with fundamentals we looked at the basics the of web application communication process and how a local proxy (Burp Suite (https://portswigger.net/burp/) or OWASP ZAP (https://www.owasp.org/index.php/OWASP\_Zed\_Attack\_Proxy\_Project)) could be used to intercept and potentially modify web application traffic.

• Students were (re)introduced to the OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project) as an underpinning set of vulnerabilities they needed to know the implications of, how they might be exploited and ultimately how they could be mitigated against

• In terms of a safe and trusted “testbed” students were encouraged to develop a virtualised sandboxed environment using VMware Workstation/VirtualBox or equivalent with virtual machines running vulnerable web applications and penetration testing frameworks.

• For the vulnerable web applications, we used the OWASP Broken Web Applications (BWA) (https://www.owasp.org/index.php/OWASP\_Broken\_Web\_Applications\_Project) VM as it contained both industry designed deliberately broken remaining web applications as well as examples or real world broken applications.

• For an attack framework, students could use the generic Kali distribution (https://www.kali.org/) or the more Web Application specific Samurai WTF Framework (http://samurai.inguardians.com/). The recent good news is that the latest version of Kali has more Web application specific tools such as BeEF (<http://beefproject.com/>).

• The first vulnerable Web Application we used was the OWASP Webgoat (https://www.owasp.org/index.php/Category:OWASP\_WebGoat\_Project)project contained within the BWA project. Webgoat’s strength is its simplicity in how the vulnerabilities can be demonstrated and the hints/tips to support novice penetration testers.

• Once vulnerabilities were found students were encouraged to study the related OWASP cheat sheets (https://www.owasp.org/index.php/OWASP\_Cheat\_Sheet\_Series) to reinforce how the vulnerabilities can be mitigated.

• Once the students are comfortable with the web application basics and the OWASP Top 10 students were introduced into more challenging scenarios offered by additional OWASP projects like Hackademic (https://www.owasp.org/index.php/OWASP\_Hackademic\_

Challenges\_Project) and Security Shepherd (https://www.owasp.org/index.php/OWASP\_Security\_Shepherd). Additional challenges can be written and added to these educational frameworks to further teach students abilities.

• The actual University Challenge uses challenges written by Hacking Lab (https://www.owasp.org/index.php/OWASP\_Hacking\_Lab) and potential contestants are encouraged to register to attempt similar challenges within the sites open areas.

• As the last piece of the puzzle to really stretch students abilities and get those extra lines on their CV, we encourage our students to seek opportunities to be able to legitimately test and audit web application security as additional experience. The key industry practice that lets this happen is the myriad of “Bug Bounty” program’s which encourage the “white hat” testing and reporting of vulnerabilities found on organisations registered under these program’s. Key to these programs is registering as a “tester” and thus have approval to begin testing. The beauty of “bug bounty” program is they often financially reward testers by the severity of the bugs found. Even if organisations haven’t signed up to a bug bounty program, it is worth checking if they have a mechanism for reporting issues (usually an anonymised form or a specific email address) via a “whistle blowing” mechanism.

The important practice for students is ensuring ethical behaviour, documenting findings as issues on Github or other mechanism and reporting the vulnerabilities to the organisation owning/operating the application. Students are strongly discouraged from purely just releasing the information on internet forums or social media and reminded this is unethical behaviour.

During the University Challenge, teams solved mission style security challenges using the Hacking-Lab framework. Student teams compete solving hacking challenges and defending insecure applications. There were 11 teams and 80 contestants fighting in a jeopardy style Capture Flag (CTF) hacking competition for two days. We were competing against teams from Germany, Austria, Greece, Netherlands and Switzerland. On the home front we were also competing against a team from Bournemouth University and came a well-earned 6th place out of the 11 taking part.

“Our team did exceptionally well against some very experienced teams who regularly take part in these types of events and the additional time and commitment they put in over the last months definitely paid off.

This type of event engages our students with the cyber security industry, showcasing and enhancing the skills that potential employers will be looking for. By taking part in the overall conference with over 500+ attendees exposes our students to CISO’s/executives from Fortune 500 companies, thought leaders, penetration testers security architects and developers to share cutting edge ideas, initiatives and technology advancements in application security.”