Hack the University: Introducing Generic University

Katie Paxton-Fear
Department of Computing and Maths
Manchester Metropolitan University
Manchester, United Kingdom
k.paxton-fear@mmu.ac.uk

***Abstract*—CTF (Capture the Flag) challenges are often used to allow students to have a hands-on experience with security concepts, inviting them to hack into an intentionally vulnerable website, software, or server, find a hidden flag and submit these for rewards such as points or prizes. These challenges enable students to practice their skills in a safe environment where they will not impact the availability, confidentiality or integrity of real systems and their data. However often these challenges use out of date methods and techniques, in many situations this enables for an easier and more well documented challenge as students may be able to complete additional research. Often this is not well justified though and seems to arise as creators of CTF challenges are not intimately familiar with modern software stacks from a developer point of view. Generic University is an intentionally vulnerable API built with Laravel which presents a modern RESTful API using more modern software tools such as Object Relational Mapping (ORM), a Model View Controller (MVC) architecture, routing and templating. This is important as these new design patterns resolve security issues, such as ORM systems replacing traditional database queries reducing the scope for a SQL injection attack, or routing replacing typical file structure limiting the scope for a file inclusion vulnerability. Instead, these modern technology stacks often introduce new vulnerabilities such as access control issues, broken 3rd party authentication, or mass assignment issues. Generic University attempts to fill this gap by mapping security issues to the OWASP API Top 10 rather than relying on traditional security challenges. This demo will present Generic University and offer participants the opportunity to try web application security and hack into a 'University'.**

Keywords—Capture the Flag, Web Security, API Security, Secure Software Development, Offensive Security, Application Security