

**UC Tech Awards 2023 Candidate**

**Category: IT Security**
**Project/Team name:** Web Application Security Student Offensive Testing Program (3)
**Number of people:** 3
**Location:** UC Berkeley

1. **Person submitting the application/nomination**
	1. Allison Henry
	2. **Email address: akhenry@berkeley.edu**
	3. **The name of your organization:** (i.e. UCLA): UC Berkeley
2. **Award category** IT Security
3. **Name of person, name of the team, or name of the project to receive the award** Web Application Security: Building an Offensive Testing Program with Cybersecurity Grad Students
4. **All project team members - if applicable**
	1. Lisa Ho, Academic Director, Master of Information and Cybersecurity, School of Information
	2. Jennia Hizver, Lecturer, School of Information
	3. Josh Kwan, Security Analyst, Information Security Office, Berkeley IT
5. **Which location was affected by the work?** (the name(s) of the organization affected): UC Berkeley
6. **Summary** According to the 2022 Verizon Data Breach Investigations Report, 40% of all data breaches involved a web application attack. At the same time, hands-on web application security testing is resource intensive and out of reach for many institutions on tight budgets, leaving many critical applications vulnerable to attack.

Through a partnership between the Information Security Office (ISO) and the School of Information's Master of Information and Cybersecurity (MICS) Program, UC Beekeley developed a truly innovative solution to this challenge - to provide offensive web application security testing services for campus business applications using graduate students as part of their of instructor-led coursework.

1. **Narrative**

**Web Application Security: Building an Offensive Testing Program with Cybersecurity Grad Students**

According to the 2022 Verizon Data Breach Investigations Report, 40% of all data breaches involved a web application attack. At the same time, hands-on web application security testing is resource intensive and out of reach for many institutions on tight budgets, leaving many critical applications vulnerable to attack.

Through a partnership between the Information Security Office (ISO) and the School of Information's Master of Information and Cybersecurity (MICS) Program, UC Beekeley developed a truly innovative solution to this challenge - to provide offensive web application security testing services for campus business applications using graduate students as part their of instructor-led coursework.

Through their coursework in the MICS Web Application Security course, MICS students learn about tools and techniques for web application security testing. After 7 weeks they are authorized to launch attacks against real world campus web applications, nominated by IT administrators selected by ISO based on risk profile. At the conclusion of the program, the students provide a detailed report on their findings, prioritized by risk. ISO tracks remediation with the IT administrators to ensure campus web applications are secured against any discovered vulnerabilities. In addition to the learning experience, students receive a letter of recognition signed by the CISO, which they can use to augment their CV as they move into the information security workforce. This invaluable learning strategy prepares them for rising in their cybersecurity careers, while improving resilience of campus applications to cyberattacks by providing actionable reports to our application developers.

The program started in 2022 and has been running for three semesters. During this time, 9 campus business applications were tested, and the student teams discovered 102 flaws: 18 High Risk 18, 50 Medium Risk 50, and 34 Low Risk.

For cost-effectiveness, “Web app penetration testing costs can vary from $15,000 to over $100,000 for a single pen test.” ([Source: NetworkAssured.com’s Web App Penetration Testing Costs](https://networkassured.com/security/web-application-penetration-testing-cost/)). Campus program tests 9+ apps/year, with a cost to the ISO of  ~$7,232 total ($452/year for 16 VMs). Software licenses are donated through a partnership with Portswigger.

Reflecting on his experience, student Jacob Glad commented: “This course was my first real deep dive into web application security testing. The real hands-on experience […] really helped grow my understanding of web application security. I have since used the practices I learned in this course to train others in my professional circle, and I’ve used the principles taught to argue for increased testing coverage of systems that I work with. All said, this is one of the most immediately applicable and useful courses I have taken in the MICS program.”

This innovative program leverages our greatest resource - smart, motivated students - to perform critical application security testing work on campus business applications at a far lower cost compared to contracting for external professional services. This program is particularly exciting because it supports the cybersecurity needs of our key campus business functions, while also contributing to our core mission of educating students with the knowledge and skills necessary to build successful careers in a field where new talent is desperately needed. Our goal is to demonstrate the value of our program with the hope that other campuses can benefit through development of similar partnerships with their academic communities.

See this news article for more information on the program and the value it brings to both the students and the institution: <https://www.ischool.berkeley.edu/news/2022/new-cybersecurity-class-works-information-security-office-prevent-uc-web-application-data>