NUS and SMU Empower Students and Staff to Hack for Good

HackerOne, the world's trusted hacker-powered security platform, has announced the successful conclusion of the inaugural Inter-University (InterUni) Bug Bounty Challenge, jointly organised by the National University of Singapore (NUS) and Singapore Management University (SMU) in partnership with HackerOne. Bug bounty programmes incentivise ethical hackers to look for software vulnerabilities or 'bugs' in exchange for monetary rewards or 'bounties.'

NUS was the first university in Singapore to launch a bug bounty challenge in 2019 to actively incentivise its own students to hone their hacking skills and contribute to the defence of university infrastructure. Building upon the success of last year's challenge, NUS expanded participation to SMU with the goal of sharing knowledge, synergising resources, and working towards cyber resilience together. The InterUni Bug Bounty Challenge, led by NUS and SMU, is a significant step towards cybersecurity collaboration and progress within the educational ecosystem.

"Results of the InterUni Bug Bounty Challenge 2020 have again exceeded expectations," said Tommy Hor, Chief Information Technology Officer at NUS. "Extending the participation to other universities was a natural progression of our aim to continue driving cybersecurity innovation within the local higher education community. We were able to build upon last year's Challenge and make this an inclusive exercise for students and faculty at both universities."

The three-week InterUni hacking challenge was held from 12 August 2020 to 2 September 2020. More than 200 participated, testing a total of 18 critical systems and digital assets, three of which are mobile based. Overall, 33 valid vulnerabilities were safely reported by participants, earning US$13,700 for their findings, nearly triple the amount earned in NUS' initial bug bounty challenge last year. Participating students were also eligible to earn extra academic credits for select course modules on the completion of the training sessions.

"There is no better way for students to learn than to find security bugs in the real world," said Lau Kai Cheong, Chief Information Officer at SMU. "The Challenge allowed us to extend security testing to include those who use our technology most. Providing this opportunity for our students and faculty to build practical cybersecurity skills also helped us reduce real organisational risk."

This is the third time HackerOne has partnered with a major university to empower students to secure their school. In 2017, the University of Berkeley in the U.S. enrolled in an experimental "cyberwar" course powered by HackerOne. To train future cybersecurity leaders, the broader security community has to invest in education. HackerOne is proud to be a part of such efforts, empowering the world to build a safer internet.

"This challenge undoubtedly helped me build up my cybersecurity skills and put them to good use on real world systems," said Ngo Wei Lin, Year 3 student at the NUS School of Computing who emerged as top winner of the InterUni Bug Bounty Challenge 2020. "It was commendable that the University made available real-life systems for this programme. I won big not because of the cash award but the invaluable real-life experience I have gained."

The partnership between NUS and SMU has brought proactive security to new heights, increasing the team of defenders and expanding the opportunities for learning. Despite the pandemic, students were able to learn more than in previous years, showing that collaboration is a competitive advantage against attackers. NUS and SMU plan to make the InterUni Bug Bounty Challenge an annual event.