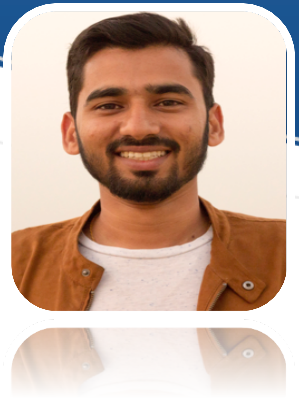
Anand Prakash
(Appsecure)

Anand Prakash is a prolific security researcher who is famous for finding bugs in some of the world's most popular apps and websites. He thrives off of "bugs bounties"— large cash prizes he earns from companies in exchange for successfully hacking their systems and showing them their security flaws. Anand is supremely good at what he does, having discovered vulnerabilities at companies like Facebook, Twitter, and Uber. For the past 5 years, Facebook's has ranked Anand as one of their top bounty hunters. And on Twitter's bounty program, he's ranked #3 world-wide. Anand's reputation as a hacker has led to him being featured in last year's Forbes "30 under 30" for enterprise technology in Asia. And a major Indian news website declared Anand "one of India's best known white hat hackers."



Sai Krishna Kothapalli
(IIT Guwahati)

Sai Krishna Kothapalli is a final Year Computer Science and Engineering Undergrad, IIT Guwahati, Bug Bounty Hunter, and Security Researcher. He has found some serious bugs in some popular web applications including a few in the Indian government sector. He is also one of the students at IITG who campaigned for the campus bug bounty program and helped getting it organized and started.

C3i Center, IIT Kanpur

https://security.cse.iitk.ac.in/

An evening with WHITE HAT Hackers on Bounty Hunting

Organized By:
Interdisciplinary Centre for Cyber Security and Cyber Defence of Critical Infrastructures

March 21st 2018

5:30 PM to 8:30 PM
Venue: L-19

The Good, the bad and the Ugly – White Hat, Grey Hat, and the Black Hat hacking

Panelists: Anand Prakash, Sai Krishna Kothapalli **Moderator**: Sandeep K. Shukla

In this panel discussion we will discuss the on-going race between the black hat hackers to exploit information and critical systems while the white hat hackers try to save the day with their repertoire of tools and techniques. Unfortunately, this war is often tilted as black hat hackers are often parts of crime syndicates, and worse yet – recruited by the cyber army and espionage functionaries of various governments. Then how are the white hat hackers to save the systems by finding the vulnerabilities faster than the black hats. Black hats are also organized in chat rooms and forums in the under bellies of the dark web. Are the white hat hackers organized in the same way?

"Talk 1: Story of a White Hat Hacker: How I saved a billion user accounts?"

Speaker: Anand Prakash

Abstract: Bugs Bounty programs worldwide have taken off because most customer facing websites and web applications are increasingly under attack by hackers. Large companies such as Facebook, twitter, google, Microsoft, as well as mobile apps-based companies such as Uber cannot fully guarantee that the web applications and mobile applications their engineers produce are free of security vulnerabilities. Therefore, they all have announced large monetary reward programs for ethical exploits, and based on the criticality level of the discovery – they reward the bounty hunting hacker handsomely. As an ethical hacker, and bounty hunter, I have found many vulnerabilities in these popular sites that could have been disastrous if exploited by a black hat hacker. The race is on between black hat hackers who use very sophisticated tools, and experience -- sometimes employed by organized crime syndicates as well as rogue states, and white hat ethical hackers who also use their experience and tools to find the vulnerabilities to help the companies. In this talk, I will discuss my own experience in saving billion user accounts, and more stories from the trench of this ongoing duel of minds between white hat and black hat hackers.

"Talk 2: Landscape of bug bounty programs"

Speaker: Sai Krishna Kothapalli

Abstract: In the ever-advancing Digital Age, India has placed so much effort in digitizing all walks of life, but are we IITG has taken the first step in this direction by

taking enough care to protect our data? being the only educational institution in Asia to launch its own responsible disclosure policy (bug bounty program). This talk lays out the challenges faced, and the response received by implementing this for IITG and highlights what other institutes and government organizations can learn from them. It also emphasizes the necessity and benefits of a responsible disclosure policy in government organizations. It winds up by focusing on some country-specific case studies where things went downhill and find out what could have been done to avert whatever had happened.