

Dhaval Kapil

<https://dhavalkapil.com>
me@dhavalkapil.com

EDUCATION

IIT ROORKEE

B. TECH. IN COMPUTER SCIENCE

Expected June 2017

Cum. CGPA: 8.544

LINKS

Blog: dhavalkapil.com

Github: [dhavalkapil](#)

LinkedIn: [dhavalkapil](#)

Twitter: [@dhaval_kapil](#)

SKILLS

LANGUAGES

Java, C, C++, C#, Lua, PHP, Javascript, Python, Haskell, Shell, SQL

TECHNOLOGIES

git, linux, apache, Node.js, elasticsearch, django, memcache

ACTIVITIES

GITHUB OSS/PROJECTS

- icmptunnel - Developed an IP over ICMP tunnel to bypass firewalls, captive portals and secure communication. > 1800 stars. Covered by PenTest Magazine.
- luaver - Developed the Lua Version Manager to manage and switch easily between different versions of Lua, LuaJIT and Luarocks.
- dns-validator - Developed a tool to detect DNS poisoning attacks.

BACKDOOR CTF

- Created Backdoor, an always online wargame platform to host Capture the Flag Events. On an average > 200 submissions every week.
- Created the required jail for serving vulnerable challenges.
- Designed 25 challenges in the field of web penetration, cryptography and binary exploitation. Hosted many CTFs.

MISCELLANEOUS

- Co-founded InfosecIITR - the information security group of IIT Roorkee
- Managed working of the group SDS Labs as the Joint Secretary
- Pianist in IIT Roorkee's Music Section

EXPERIENCE

GOOGLE SUMMER OF CODE | SOFTWARE ENGINEERING INTERN

Summer 2015, 2016 | Remote

- Worked with LabLua, a research lab for the Lua Programming language, to develop a client for Elasticsearch in Lua from scratch
- Wrote unit, integration and stress tests

AMAZON | SOFTWARE ENGINEERING INTERN

May 2016 – July 2016 | Bangalore, India

- As part of AFT Receive, automated expiration date handling, thereby improving the efficiency and reducing the cost considerably
- Fixed severity level 2 bugs concerning DNS server issues
- Improved existing CacheClient to support caching arbitrary objects

RELIANCE JIO INFOCOMM LIMITED | PENETRATION TESTER & SOFTWARE ENGINEERING INTERN

May 2015 – June 2015 | Mumbai, India

- As part of the cloud team, pentested the cloud and reported various vulnerabilities
- Developed a network monitoring web application that reports the health of different vRouter/Agent in Open Contrail from scratch.

RESEARCH

IIT ROORKEE COMPUTER SCIENCE DEPARTMENT August 2016 – Present

Working with Dr. Manoj Mishra on securing the ARP protocol from Denial of Service and Man in the Middle attacks. Researching on hybrid approaches involving unicast messages, voting mechanisms and cryptographic primitives.

PERSONAL RESEARCH Septemeber 2016 - November 2016

Discovered a new class of vulnerabilities involving XSS Auditor/Filter with implications such as stealing OAuth Tokens, bypassing Same Origin Policy and disabling existing security protection in browsers. Reported zero-day vulnerabilities to Chromium team. Publication in progress.

SDSLABS, IIT ROORKEE Jan 2016 – May 2016

Developed a PHP library to upload images securely on a web server. Researched on various vulnerabilities related to file uploading and successfully added required protection.

RECENT TRENDS IN NETWORK SECURITY | IIT ROORKEE Dec 2015 - Feb 2016

Gave a talk + live demo for bypassing ASLR protection and injecting shellcode. My work was translated into Arabic and covered by iSecur1ty, an Arab Cyber Security company.

ACHIEVEMENTS

- 2016 Winner of CSAW CTF India hosted by New York University
- 2016 All India 2nd rank in Microsoft Build The Shield Contest
- 2016 Runners up in Microsoft Code.Fun.Do hackathon
- 2013 All India Rank 114 in JEE Mains and 379 in JEE Advance