Dhaval Kapil

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

EDUCATION

IIT ROORKEE

B. Tech. in Computer Science
July 2013 - May 2017
Cum. CGPA: 8.753

LINKS

Website: **dhavalkapil.com**
Github: **dhavalkapil**
LinkedIn: **dhavalkapil**
Twitter: **@dhaval_kapil**

SKILLS

LANGUAGES

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

TECHNOLOGIES

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

ACTIVITIES

GITHUB OSS

- luaver - Developed the Lua Version Manager to manage and switch easily between different versions of Lua, LuaJIT and Luarocks.
- image-uploader - Developed a simple, elegant and extremely secure library for uploading images on a web server.
- 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
- Gave a talk + live demo for bypassing ASLR protection and injecting shellcode
- Managed working of the group SDSLabs as the Joint Secretary

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.

PROJECTS

ICMPTUNNEL Aug 2015

Transparently tunnel your IP traffic through ICMP echo and reply packets. Prototype to bypass firewalls and captive portals. Exploited RFC 792's allowance of ICMP packets of arbitrary data length. Covered by PenTest Magazine. Most used ICMP tunnel - 2000 stars on Github

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.

HEAP EXPLOITATION April 2017 - June 2017

Wrote a short book for people who want to understand the internals of 'heap memory', particularly the implementation of glibc's 'malloc' and 'free' procedures, and the relavent exploits.

LIBDHEAP June 2017

Developed a shared (dynamic) library that can be transparently injected into different processes to detect memory corruption in glibc heap such as double frees, invalid malloc and heap buffer overruns.

ACHIEVEMENTS

2017 Credited by Google for CVE-2017-5045
2016 Winner of CSAW CTF India hosted by New York University
2016 All India 2nd rank in Microsoft Build The Shield Contest
2015 Runners up in Microsoft Code.Fun.Do hackathon
2013 All India Rank 114 in JEE Mains and 379 in JEE Advance