Ashutosh Barot

Cyber Security Engineer, Deloitte

https://ashutoshbarot.com
ashutoshh@protonmail.com
https://linktr.ee/ashutosh_barot

https://in.linkedin.com/in/ashutoshbarot
@ashu_barot , @wahh_fans, @join_cwm

Blog: https://cyberworldmirror.com
HackerOne : https://hackerone.com/ashutosh7

Identified security vulnerabilities preventing leak of personal information for over 100 million individuals.

Skills:

- **Application Security:** Experienced in finding security issues in Web Apps, Mobile Apps, AI based Chatbots, Facebook Applications, APIs. Currently holding *2nd rank on Coinbase 's public bug bounty program on Hackerone .*
- **Vulnerability Management and Penetration Testing** - Proficient in finding and exploiting vulnerabilities in an organization's IT infrastructure including Web Applications, Servers, Cloud etc. Also performed vulnerability assessments using Nessus, Qualys guard scanner, Nexpose.
- **Cloud Security Assessment:** Experienced in managing and securing cloud infrastructure and performing Vulnerability Assessments in VPC network and cloud-based Web, Mobile applications.
- Open-Source Intelligence: Proficient in discovering business-critical information about organizations, such as leaked credit card details and credentials, by monitoring specific forums and chat rooms in the Darknet.
- Computer Forensics: Proficient in Data Carving, Network Traffic Analysis, Memory Forensics, Familiar with tools like Wireshark, TCP Dump, Network Miner, Autopsy, Volatility, and many more.
- Endpoint Protection/Secure Configuration Review: Performed configuration reviews for Linux, Windows, Servers, Databases, Firewalls, Web Application Firewalls and Endpoints.
- Java, C#, Python, HTML, CSS, PHP, Powershell, Bash scripting as well as basic knowledge of DBMS and Computer Networks, Amazon Web Services
- Soft Skills **-** Extremely Trustworthy**,** Curious**,** Quick learner, Detail-oriented

Notable Findings:

- *"Personal info of Akasa Air's passengers leaked, airline informs CERT-In"*
- *"India shipping logistics giant Shipyaari exposed customer data"*
- *"Critical Flaw Reported In phpMyAdmin Lets Attackers Damage Databases"*

Work Experience and Projects:

- **Deputy Manager at Deloitte Asia Pacific**
  (Jun 2017 - Present, Promoted in June 2019 and June 2022)

  - Prevented multiple large-scale data breaches by reporting misconfigured Databases, S3 buckets, IDORs and other vulnerabilities to multiple organizations.
  - Enhanced the organization's detection capabilities with comprehensive adversary simulation, purple teaming, and automated these tasks by creating YAML files, scripts for Atomic Red Team framework.
  - Worked with clients in the Finance, Insurance, Power and Utilities Sector and handled engagements involving finding, prioritising, and fixing vulnerabilities considering business impact and risk.
  - Performed extensive Security Assessments of Web Apps, Mobile Apps, APIs, AI based Chatbots, bots etc with Grey box, Black box and white box approach followed by confirmatory assessments and coordination with development teams for fixing the vulnerabilities.
  - Conducted black box security assessments utilizing various tools and custom wordlists to unveil the organizations' 'Shadow IT'.
  - Assisted clients in developing custom rules for Web Application Firewalls to facilitate virtual patching.

- Created Detailed Reports, explained findings, associated risk, and provided recommendations to developers, application owners and the Senior Management.

- **Contributor** – Exploit Prediction Scoring System (EPSS) (Jul 2022 – Present)
- Law Enforcement: Gujarat Police Department (Feb 2016 – May 2016) – Consultant/volunteer for investigations of cybercrimes at office of Inspector General of Police, Gandhinagar Range

  - Forensic Science Laboratory, Gujarat - Digital Forensics Trainee
- Created a Twitter bot 'Cyber Guru': www.twitter.com/cybersec_feed
  - The bot (@cybersec_feed) tweets about cyber security according to pre-set hashtags and keywords
  - Twitter Handle - Web Application Hacker's Handbook Fan Club: www.twitter.com/wahh_fans
  - **FinalURLs** - Created a python tool (using AI) that accepts short URLs and gives final urls after redirections
  - Reported many Facebook pages and profiles, Android apps on Playstore , twitter accounts that served disturbing and violent content or involved in frauds.

Achievements and Certificates:

- Featured in Coinbase security blog celebrating 10-year journey of their bug bounty program.
- Received a Bug Bounty from Google for identifying a security issue in Google Maps, and was awarded an 'Abuse Research Grant' of $1337 for uncovering abuse risks in Google Meet.
- CVE-2022-23746 - Credential stuffing,Password Spraying flaws in Checkpoint SSL Network Extender.
- Received $200 reward from Android Security Reward Program *(Google VRP)* for finding an issue in Android OS affecting a large number of android users.
- CVE 2017-1000499 - CSRF in PHPMyAdmin, featured in various InfoSec blogs such as The Hacker News, Net Sparker, etc. Submitted an exploit on exploit.db for CVE 2017-1000499.
- CVE-2019-5638 , CVE-2019-5640 - Found multiple vulnerabilities in Rapid7 insightVM, Nexpose.
- CVE-2019-6120, CVE-2019-6121, CVE-2019-6122 - Found Multiple issues in NiceHash Miner, a prominent thick client application used by 1,00,000+ crypto miners for mining crypto currencies.
- CVE-2020-27585, CVE-2020-27586, CVE-2020-27587 - CVE IDs and reward for reporting multiple Vulnerabilities in QuickHeal Total Security v18.0
- Acknowledged by NASA, United Nations, United States Department of Defense, National Critical Information Infrastructure Protection Centre (NCIIPC) , CERT-IN- Government of India, Deloitte, FireEye (for finding security issue in FireEye HX) , Amazon, United Airlines, Verizon, IBM, Nokia, JPMorgan Chase, Harvard University, University of Cambridge, AVG Technologies, Amazon Web Services, Avira, Intel Corporation, TrendMicro etc. for reporting security issues in their web applications.
- Rewarded by Google, Twitter, Coinbase, United Airlines (total 2 Million miles), Symantec, Quick Heal, ING Bank, RedBus, NiceHash, MakeMyTrip, Go Airlines, BBC for finding and reporting security issues with their web applications.
- Certificate - *Operational Security (OPSEC) training* for Control Systems by Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), *U.S. Department of Homeland Security* (July-2014)
- Certified Ethical Hacker, CEH v10: Aug 2018 (Expired in Aug 2021)
- IELTS General Test Scores – Reading – 8.5, Listening – 8.0, Speaking, Writing – 7.5 | Overall - 8.0

Education:

- **Master of Technology in Cyber Security and Incident Response, 2017**
  National Forensic Sciences University **[NFSU]** [First Class with Distinction]
  Final Year Dissertation - 'Analysis of Ransomware Families and Incident Response'
- Bachelor of Engineering: Computer Engineering: 2015
  Ahmedabad Institute of Technology, Ahmedabad CGPA - 6.7

Hobbies, Interests:

Engaging in farming, tree-planting, yoga, reiki, practicing martial arts (Tae-kwon-do, Gōjū-ryū), trekking, meditation.