Ashutosh Barot

Cyber Security Engineer, Deloitte

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

https://ashutoshbarot.com
ashutoshh@protonmail.com,

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

Found security issues that prevented leak of personal information belonging to 100 million+ people.

Skills:

- **Application Security:** Experienced in finding security issues in Web Apps, Mobile Apps, AI based Chatbots, Facebook Applications, APIs. Currently 3rd 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: Experienced in finding business critical information about organizations (such as leaked credit card details, credentials etc. by keeping an eye on specific forums, chat rooms in 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

Media Exposure:

- *"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 Jun 2019 and Jun 2022)

  - Prevented multiple large-scale data breaches by reporting misconfigured Databases, S3 buckets, IDORs and other vulnerabilities to multiple organizations.
  - 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.
  - Performed black box security assessments using multiple tools with custom wordlists to uncover the organizations' 'Shadow IT'.
  - Helped clients create custom rules for Web Application Firewall for 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

    Using this handle, I tweet interesting excerpts/Tips from Web Application Hacker's Handbook.

  - 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:

- Bug Bounty from Google for finding a security issue in Google Maps, also received 'Abuse Research Grant' of $1337 from Google for finding abuse risks in Google Meet. [Sep-2020]
- Received $200 reward from Android Security Reward Program (Google VRP) for finding an issue in Android OS affecting large number of android apps. [Feb – 2022]
- 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.
- Found multiple vulnerabilities in Rapid7 insightVM, Nexpose - CVE-2019-5638 and CVE-2019-5640
- Found Multiple issues in NiceHash Miner, a prominent thick client application used by 1,00,000+ crypto miners for mining crypto currencies. CVE-2019-6120, CVE-2019-6121, CVE-2019-6122
- Received 3 CVE IDs and reward for reporting multiple Vulnerabilities in QuickHeal Total Security v18.0 – CVE-2020-27585, CVE-2020-27586, CVE-2020-27587
- Acknowledged by United Nations, United States Department of Defense, National Critical Information Infrastructure Protection Centre - 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 8,65,000 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)
- Certificate in Cyber Security, Forensics & Cyber Laws: 2015 by IEEE
- 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's in Technology: Cyber Security and Incident Response: 2017**
  Institute of Forensic Science, Gujarat Forensic Sciences University 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:

Planting Trees, Yoga, Reiki, Martial Arts (Tae-kwon-do and karate), Trekking, Meditation