# EDUCATION

**Kakatiya University 2017**

* BSC
* Grade: 8.33 GPA with Distinction marks

# EXPERIENCE

**Anil Arelli**



24.06.1997

8186817402

[anilarelli123@gmail.com](mailto:anilarelli123@gmail.com) Gujrat

* **Languages:**

Telugu,English,Hindi

**Penetration tester Intern (Swift Safe) 06/2017~12/2017**

* + Perform web application assessments/audits
  + Validate the vulnerabilities found by the different automated tools
  + Prepare documentation of the identified vulnerabilities.

**Mss Engineer (Indusface) 03/2018~01/2020**

* + Conduct vulnerability assessments, penetration testing.
  + Give proof of concepts for identified vulnerabilities.
  + Maintain confidentiality, integrity via vulnerability scanningand testing for OWASP Top Ten.
  + Prepare documentation of the identifiedvulnerabilities
  + Handle the client calls to explain the severity of the vulnerability and mitigation steps.
  + Infrastructure monitoring of automated scans.
  + DDoS and other attacks violation analysis.
  + Working on web-application-firewall based on Mod-Sec.
  + Creating & deploying the rules with PCRE based on Mod-Security to strengthen the website security.
  + mitigate WAF false-positive.

## Application security engineer (Eclinicalworks) 02/2020 ~current

* Work closely with Development, RM and Infrastructure teams to analyze, diagnose, debug and rectify security flaws.
* Security in SDLC (Application Security).
* Conduct secure source-code review using automated and manual approaches.
* Conduct vulnerability assessment and penetration testing and configuration review for web applications.
* provide remediation solution of vulnerabilities.
* FS and DS security review.

**PROJECTS**

* Security Assessment of Internet and Core Banking Application

|  |  |
| --- | --- |
| Client | * Large private banks of India |
| Project description | * The scope included the vulnerability assessment & penetration testing of different private banks of India. * Created different black box & white box test cases to search for possible security flaw. * Targeted to find more business logic vulnerabilities like captcha bypass, CSRF, privilege escalation, SQL injectionetc. * Provided comprehensive report on findings & action items   to fix identified vulnerabilities |

* Security Assessment of E-Commerce Applications

|  |  |
| --- | --- |
| Client | * E-Commerce organizations & online shopping portals |
| Project description | * The scope included the vulnerability assessment & penetration testing of different E-commerce applications& online shopping portals * Reported vulnerabilities like payment manipulation, Cross-site Scripting, Session Hijacking, Clickjacking etc. * Provided comprehensive report on findings * Handled client calls to make them understand the impact of the vulnerabilities & possible mitigation steps. |

* Security Assessment of Intranet Web Application

|  |  |
| --- | --- |
| Client | * Intranet/UAT applications |
| Project description | * The scope included the vulnerability assessment & penetration testing of different intranetapplications. * Reported vulnerabilities like payment manipulation,XSS, Session Hijacking etc. * Reported network/SSL related issues like SSL misconfiguration, weak-cipher suites used, unknown service running on various ports etc using tools like NMAP & Nessus. * Reported security misconfigurations likeopen-ports, application is reveling sensitive informationetc. * Reported issues of insufficient logging mechanism. * Provided comprehensive report on findings & action items to fix identified vulnerabilities |

# Technical Skills



* Excellent knowledge in application vulnerability assessments, manually and with the help of automated scanning tools
* Experience in conducting vulnerability assessments of different types of servers, manually and with the help of scanning tools
* Analyze different Web security threats
* Good in different security analysis tools like Burp Suite, Fiddler, Acunetix,subdomain enumaration tools, ffuf, Metasploit, Wireshark, Nessus, NMAP and various other bash and python scripts.
* Working knowledge on ELK Stack
* Knowledge on web application firewall
* Working knowledge of Mod-Security
* Amazon web service

# EVALUATION

* Good communication, presentation and interpersonal skills
* Complete dedication towards work, willingness to learn and explore new technologies on quickpace
* Comprehensive and analytical thinking capability, efficient time management
* Self-motivated. adaptive and Enthusiastic
* Open minded, team player, straight forward and flexible to adapt any newenvironment
* Excellent & fast learning capabilities

# Training & Certification

* CEH (EC-COUNCIL CERTIFIED ETHICAL HACKER) Certification
* Preparing for OSCP(offensive security Certified Professional)