Keerthi Bandaru

7396220106|keerthibandaru900 @gmail.com
Naukri: Profile | Mynaukri

Objective

Seeking a position in an organization, which will challenge my abilities and provide me with an opportunity to utilize my strength and decision-making skills in a professional and a learning environment. To extract the knowledge and impart learning wherever I work to progress in my chosen career path.

Profile:

Having professional experience of Software Engineer with 2+ years of experience in HCL TECHNOLOGIES. Worked on Application security testing, Vulnerability Analysis of a web application, Vulnerability Assessment and Penetration Testing (Both automation and manual).

Technical Skills:

Languages : Python, java(foundation).
Tools: OWASP ZAP (Scanning) , Burpsuite (Scanning and testing) ,Wappalyzer, sqlmap , SonarQube ,CheckMarxs (SAST) , Nmap ,Postman(API Testing).
Linux : Kali Linux, Parrot Linux .
Professional Skills: Vulnerability Analyst , Web Application Security Testing, API Testing.

Certifications:

Certified Ethical Hacker(CEH) v11 EC Council

Courses:

Vulnerability Management
Web Hacking and Penetration Testing

Professional Experience :

Hands-on experience in web application security assessment and exploitation.

- Performed security testing to identify vulnerabilities in cloud and on-premise applications.
- Familiar with security standards like OWASP TOP 10 vulnerabilities.
- Worked on Burpsuite, sqlmap and Kali Linux tools.
- Understand the application flow and design the proper test cases to identify the Vulnerabilities.
- Performed Vulnerability Assessment and Penetration Testing(VA/PT) by manual and automated ways on web applications.
- Interact with customers in a collaborative, consultative manner to deliver results, remediation recommendations on findings.
- Hands-on experience in doing web application VAPT and exploitation.

- Experience in conducting source code review using CheckMarxs , SonarQube.
- Able to conduct scan against latest CVE's and their exploitation in a product .
- Keep oneself updated on the latest IT Security news, exploits, hacks.
- Should be able to create report and present dashboard to the client.

Project Summary:

Worked as a **Web Application Security Tester** (VA/PT)

- Applications which are to be tested will be assigned.
- Start gathering information about the application by ensuring you get all the end user access from the application owner.
- Understanding all the web components , web technologies , frameworks used and checking their configurations and versions which are vulnerable.
- Save each and every result of analysis and start scanning the application using OWASP ZAP and Burpsuite.
- Testing Each and Every vulnerability manually using Burpsuite to conclude the true positives and false positives from the scanned report of vulnerabilities.
- If any application contains API's – testing using postman and burpsuite.
- Document each and every result and analysis of true positive vulnerability and prepare a dashboard to make sure a proper understanding to the client.

Roles & Responsibilities:

- Applications which are to be tested will be assigned.
- Responsible to gather all the information regarding the application to ensure end to end security testing.
- Understanding all the web components , web technologies , frameworks used and checking their configurations and versions which are vulnerable.
- Scanning and testing vulnerabilities using OWASP ZAP , burpsuite tools against latest CVE's .
- Able to understand each and every vulnerability and test them and recommend the remediation tips to the developers.
- Document each and every result and analysis of true positive vulnerability and prepare a dashboard to make sure a proper understanding to the client.