Semester 1

SELF DRIVEN ACTIVITY

Quarter 2

Activity Name	**Bootcamp On Demystifying Android App Security**
Date of Activity	01-December-2024 to 06-December-2024
Mode of Conduct	Physical
Time	Five Day
Mandatory/Elective	Mandatory
Participants *(Online /offline)*	• Students: Attending all 5th Sem Students from CSE Department, • Staff's from core branches
Resource Person	Mr. Sunil K P
Description	Organize Five Day activity on "Bootcamp on Demystifying Android App Security" The activity should focus on following: • This 5-daysWorkshop is designed to immerse students in the world of demystifying Android app security is to provide a clear understanding of the essential measures that protect apps and user data from malicious threats • It aims to highlight the importance of **app signing** and **integrity checks**, ensuring that the app is authentic and unmodified. Key security practices such as **data encryption** for both storage and transmission, **secure API communication**, and the use of **runtime permissions** are emphasized to safeguard sensitive information. • By focusing on a secure **Software Development Lifecycle (SDLC)**, the goal is to promote the early identification and mitigation of security risks. Ultimately, the aim is to equip both developers and users with the knowledge to create, deploy, and use Android apps in a secure manner, fostering trust and minimizing exposure to potential attacks. • Establishment of Security Analysis Environment and Secure Coding Practices. • APK Analysis Skills • Enhanced Security Awareness Android app security is crucial due to the widespread use of Android devices,

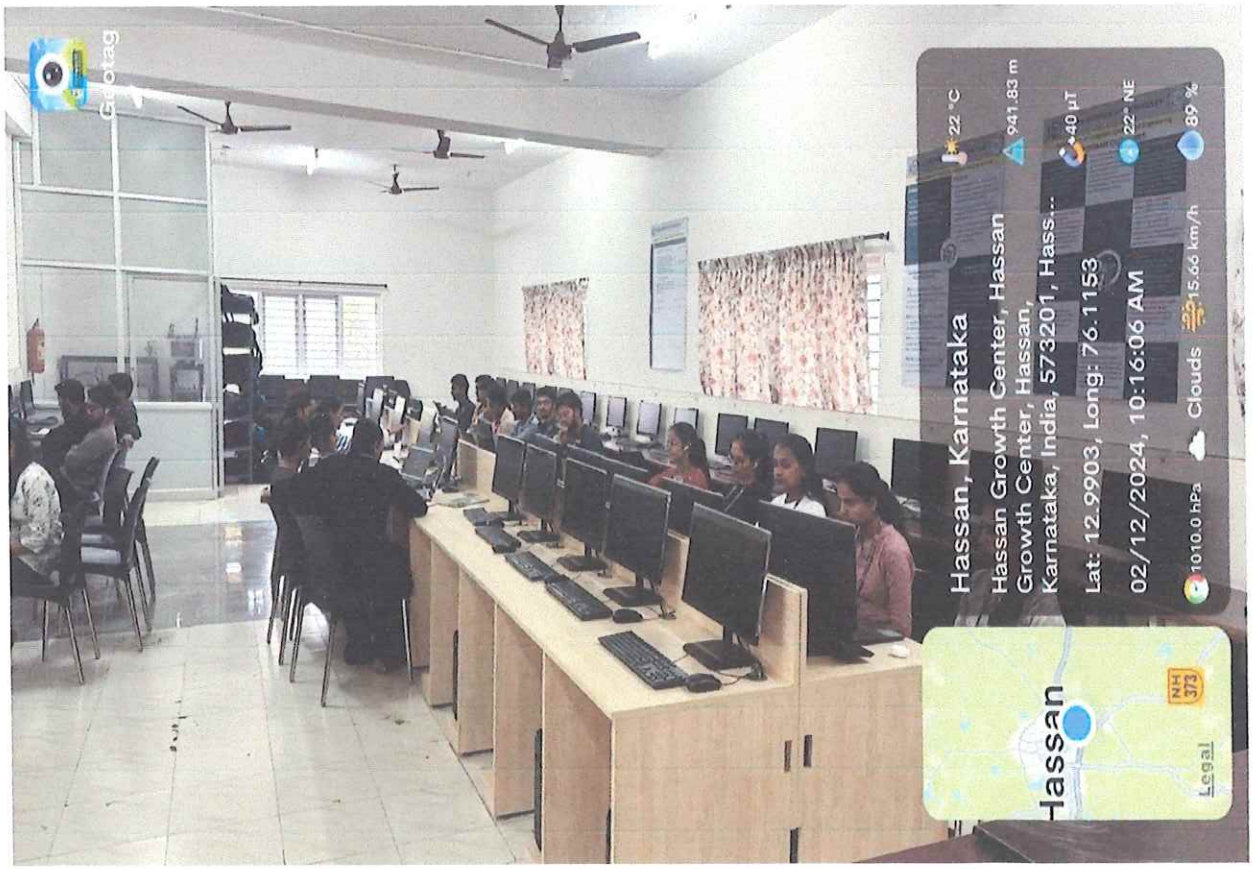
	which exposes them to various vulnerabilities. At the heart of app security is app signing, where developers use cryptographic keys to ensure that apps haven't been tampered with. Apps must also use encryption—both for data in transit (via HTTPS) and at rest (through storage encryption or the Android Keystore)—to safeguard sensitive information. Permissions play a key role, as apps request explicit access to certain device features, and users must carefully manage these to limit data exposure. To prevent reverse engineering, code obfuscation tools like ProGuard and R8 are employed to obscure app logic. Secure communication with backend services is vital, often achieved through OAuth2 and JWT for authentication. Additional measures include detecting rooted devices and using app sandboxing to isolate apps from each other. A secure Software Development Lifecycle (SDLC), involving regular code reviews, penetration testing, and timely updates, ensures that vulnerabilities are addressed early.
	Day1-Session1 (9.00 am to5.00pm): Introduction to Android Apps Android apps are software applications specifically designed and developed to run on devices powered by the Android operating system, which is the most widely used mobile OS in the world. Android, an open-source platform developed by Google, powers smartphones, tablets, smartwatches, televisions, and even some wearables and automobiles. **Day 2-Session 2 (9.00 am to 5.00pm): security threats and vulnerabilities** The latest mobile application security threats and vulnerabilities are increasingly sophisticated, posing significant risks to both users and developers. **Day 3-Session 3(9.00amto05.00 pm): Static analysis of Android applications** Static analysis of Android applications is a security testing technique that involves

	inspecting the app's source code or compiled APK without executing it, to identify potential vulnerabilities. **Day4-Session 4 (9.00amto 5.00 pm):Dynamic analysis of Android applications** Dynamic analysis of Android applications involves running the app in a controlled environment to observe its behavior during execution, identifying vulnerabilities and security flaws that only manifest when the app is active. **Day5-Session 5 (9.00amto 5.00 pm):case studies** Security analysis of Android applications through case studies provides invaluable insights into common vulnerabilities and the effectiveness of mitigation strategies. One notable case is the Heartbleed vulnerability in Android apps, which affected many apps relying on OpenSSL for secure communication.
Program Outcome	• The outcomes of Demystifying Android App Security are centered on empowering developers and security professionals with a deeper understanding of how to build, deploy, and maintain secure Android applications. • By the end of the initiative, participants should be able to effectively apply security best practices such as app signing, data encryption, and secure API integration to ensure robust app protection. • Developers will gain the ability to identify and mitigate vulnerabilities related to insecure data storage, communication, and code obfuscation, thus reducing the risk of data breaches, reverse engineering, and unauthorized access. • The initiative also aims to foster a security-conscious development culture, enabling professionals to adopt proactive measures like root detection, secure session management, and thorough testing to safeguard apps against both known and emerging threats. • Ultimately, the outcome is a more informed and prepared developer community that is equipped to create Android apps that not only meet functional requirements but are also resilient to the increasingly sophisticated landscape of mobile security threats.


Geotag
BOOTCAMP
DEMYSTIFYING ANDROID APP SECURITY
Hassan, Karnataka
Hassan Growth Center, Hassan
Growth Center, Hassan,
Karnataka, India, 573201, Hass...
Lat: 12.9902, Long: 76.1152
02/12/2024, 10:21:07 AM
22 °C
942.11 m
39 µT
96° E
89 %
Clouds
15.66 km/h
1010.0 hPa
Hassan
NH 373
Legal


Geotag
BOOTCAMP
DEMYSTIFYING ANDROID APP SECURITY
Hassan, Karnataka
Hassan Growth Center, Hassan
Growth Center, Hassan,
Karnataka, India, 573201, Hass...
Lat: 12.9901, Long: 76.1152
02/12/2024, 10:14:43 AM
22 °C
941.95 m
38 µT
107° E
89 %
Clouds
15.66 km/h
1010.0 hPa
Hassan
NH 373
Legal

Department of Computer Science and Engineering



Dr. Arjun B C **HOD**	**Mr. Vishwanath B R** **Member Secretary**	**Dr. H N Prakash** **IIC President**	**Dr. Mahesh P K** **Principal** Principal Rajeev Institute of Technolog Hassan-573 201