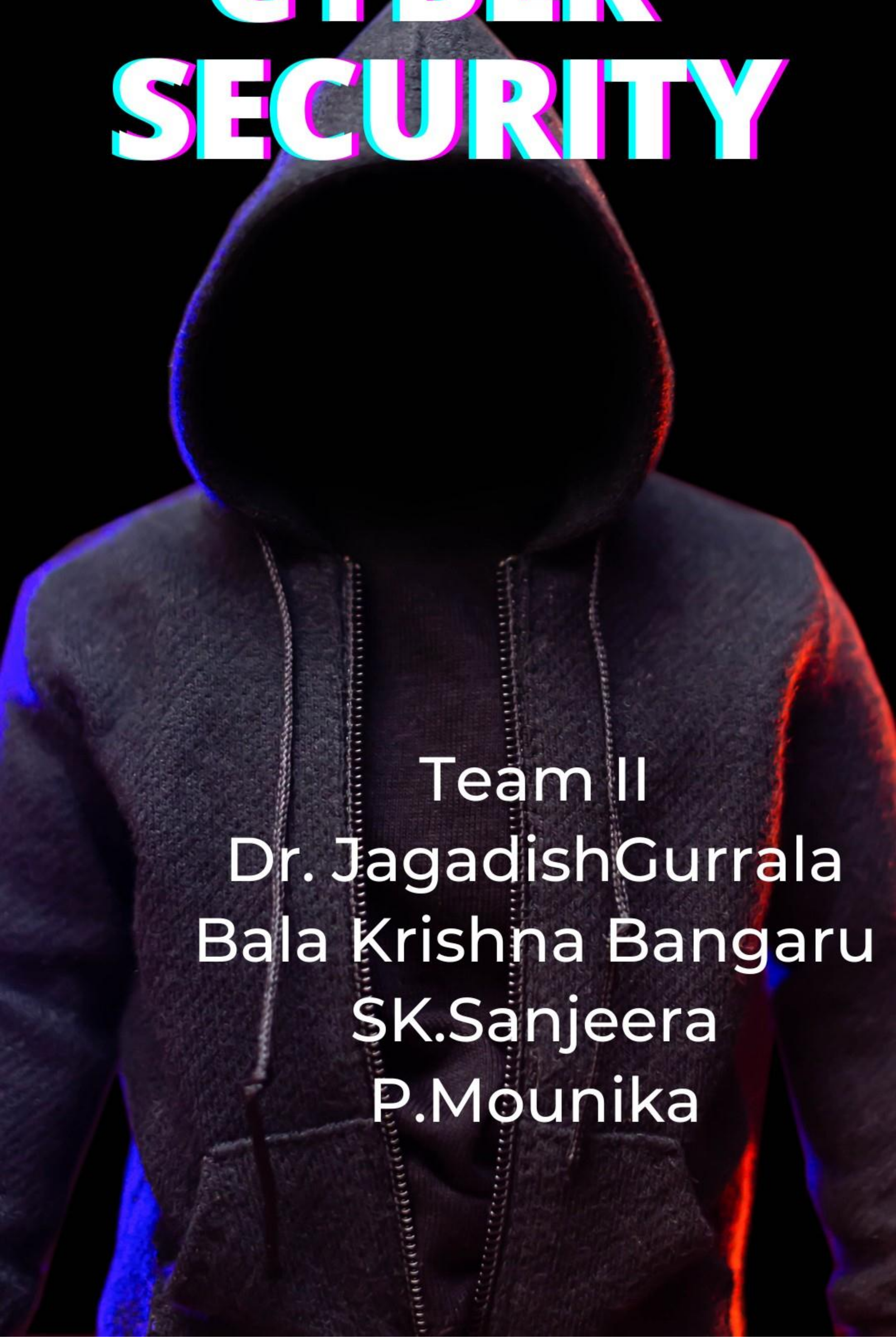
CYBER SECURITY



Team II

Dr. JagadishGurrala

Bala Krishna Bangaru

SK.Sanjeera

P.Mounika

TEAM -II

A Trust Defender

Part I-Executive summary

Overview:

Implementing cybersecurity in an organization involves a comprehensive and proactive approach to protect its digital assets, data, and infrastructure from cyber threats. The steps to implement cybersecurity effectively at every organization include:

- Develop a clear and well-defined cybersecurity policy and strategy that aligns with the organization's business objectives and risk tolerance.
- Conduct a thorough risk assessment to identify potential cybersecurity threats and vulnerabilities specific to the organization. Prioritize risks based on their potential impact and likelihood of occurrence. Implement risk mitigation measures and create a risk management plan to address identified vulnerabilities.
- Train all employees on cybersecurity best practices and the role they play in safeguarding the organization's information. Educate them about phishing, social engineering, password hygiene, and other common attack vectors to promote a security-conscious culture.
- Implement strong access control measures to ensure that only authorized personnel can access sensitive data and critical systems. Utilize multi-factor authentication (MFA) for an extra layer of security.
- Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gatewaysto monitor and control network traffic.

- Install antivirus software, endpoint protection tools, and host-based firewalls on all devices to defend against malware and other threats at the device level.
- Install antivirus software endpoint protection tools, and host-based firewalls on all devices to defend against malware and other threats at the device level.
- Encrypt sensitive data both at least and in transit to prevent unauthorized access and ensuredata confidentiality.
- Establish a systematic process to apply security patches and updates promptly to all software, operating systems, and firmware to address known vulnerabilities.
- Develop a well-defined incident response plan (IRP) to handle cybersecurity incidents effectively. The plan should include clear guidelines on identifying, reporting, containing, eradicating, and recovering from security incidents.
- Conduct regular internal and external security audits and assessments to evaluate the organization's security posture and identify potential weaknesses gaps.
- Monitoring and Logging: Implement centralized logging and real-time monitoring of network and system activities to detect and respond to suspicious activities promptly.
- Establish clear channels for reporting security incidents and communicating with stakeholders, including employees, customers, partners, and regulatory authorities.

IP address of irctc.com 103.116.163.23

2. Team Members Involved in vulnerability Assessment:

S. No	Name	Designation	Mobile Number
1	Dr. Jagadish Gurrala	Associate Professor	9441345914 gjagadish@kluniversity.in
2	Mr. Balakrishna Bangaru	Assistant Professor	8522879369 b.balakrishna@kluniversity.in
3	Ms.SK.Sanjeera	Assistant Professor	7893750475 shaiksanjeera@kluniversity.in
4	Mrs.P.Mounika	Assistant Professor	pmounika@kluniversity.in

3. List of Vulnerable Parameter, location discovered:

S. No	Name of the Vulnerability	Reference CWE
1	Broken Access Control	**CWE-284: Improper Access Control**
2	Cryptographic Failures	**CWE-326: Inadequate Encryption Strength**
3	Injection	**CWE-94: Improper Control of Generation of Code ('Code Injection')**
4	Insecure Design	**CWE-657: Violation of Secure Design Principles**

5	Security Misconfiguration	**CWE-942: Permissive Cross-domain Policy with Untrusted Domains**
6	Vulnerable and Outdated Components	**CWE-1104: Use of Unmaintained Third-Party Components**
7	Identification and Authentication Failures	**CWE-287: Improper Authentication**
8	Software and Data Integrity Failures	**CWE-502: Deserialization of Untrusted Data**
9	Security Logging and Monitoring Failures	**CWE-778: Insufficient Logging**
10	Server-Side Request Forgery	**CWE-352: Cross-Site Request Forgery (CSRF)**