SANJIVANI RURAL EDUCATION SOCIETY'S

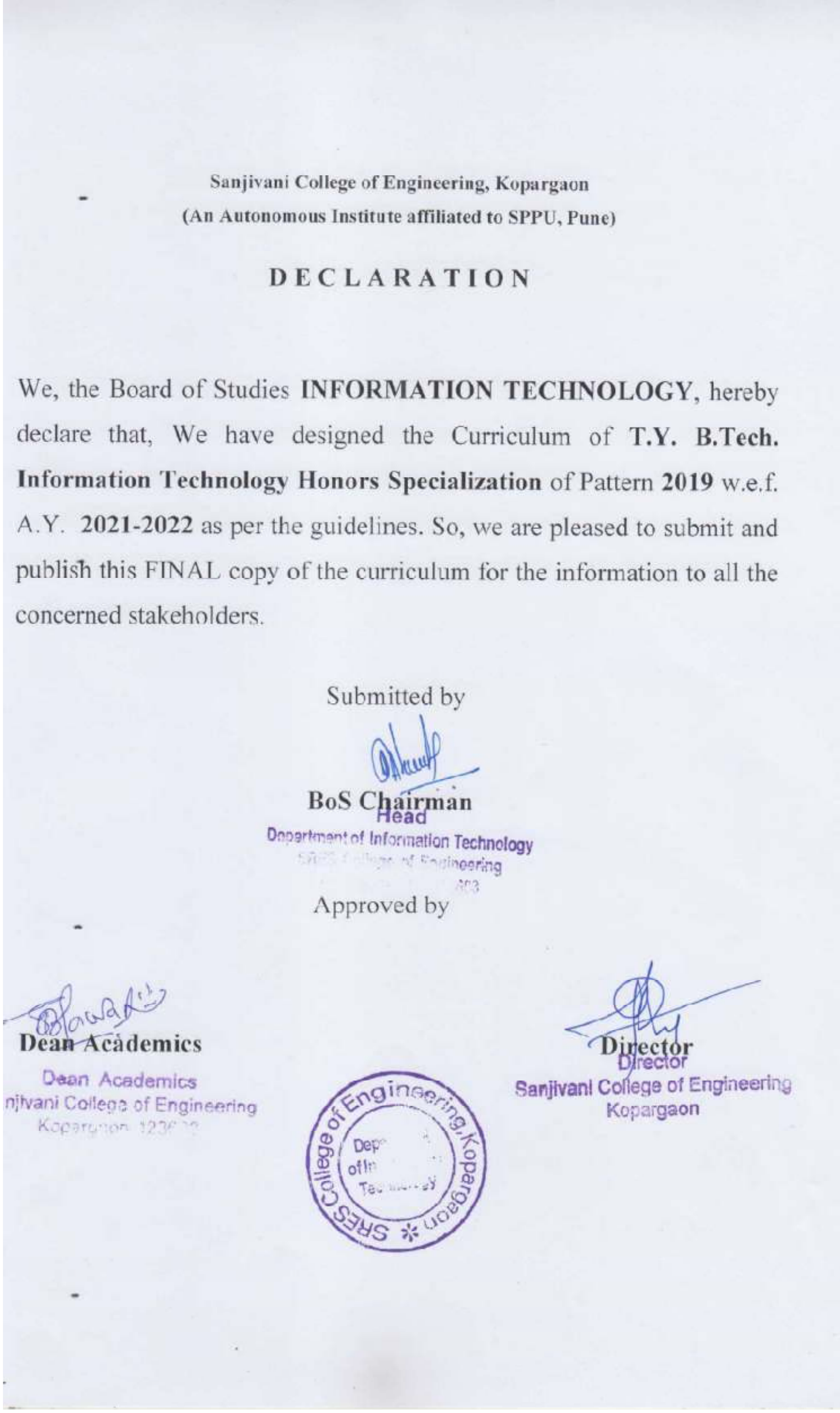
SANJIVANI COLLEGE OF ENGINEERING KOPARGAON

(An Autonomous Institute Affiliated to SPPU Pune)

DEPARTMENT OF INFORMATION TECHNOLOGY

COURSE CURRICULUM - 2019 PATTERN

THIRD YEAR B. TECH. HONORS SPECIALIZATIONS



Sanjivani College of Engineering, Kopargaon

(An Autonomous Institute affiliated to SPPU, Pune)

DECLARATION

We, the Board of Studies **INFORMATION TECHNOLOGY**, hereby declare that, We have designed the Curriculum of **T.Y. B.Tech. Information Technology Honors Specialization** of Pattern **2019** w.e.f. A.Y. **2021-2022** as per the guidelines. So, we are pleased to submit and publish this FINAL copy of the curriculum for the information to all the concerned stakeholders.

Submitted by

BoS Chairman

Head
Department of Information Technology
SRES College of Engineering
[illegible] 423603

Approved by

Dean Academics

Dean Academics
njivani College of Engineering
Kopargaon 4236[illegible]

SRES College of Engineering, Kopargaon
Dep[illegible]
of In[illegible]
Technology

Director

Director
Sanjivani College of Engineering
Kopargaon

LIST OF ABBREVIATIONS

Abbreviation	Full Form	Abbreviation	Full Form
ES	Engineering Science	HSMC	Humanity Science
PC	Professional Core	CA	Continuous Assessment
PE	Professional Elective	OR	End Semester Oral Examination
OE	Open Elective	PR	End Semester Practical Examination
ISE	In-Semester Evaluation	TW	Continuous Term work Evaluation
ESE	End-Semester Evaluation	BSC	Basic Science Course
PRJ	Project	MC	Mandatory Course
HSIT	Honors Specialization Course in Information Technology		

Aboutoffered Specializations

CYBER SECURITY

Short Description:

The Cyber security Specialization covers the fundamental concepts underlying the construction of secure systems, from the hardware to the software to the human-computer interface, with the use of cryptography to secure interactions. These concepts are illustrated with examples drawn from modern practice and augmented with hands-on exercises involving relevant tools and techniques. Successful participants will develop a way of thinking that is security-oriented, a better understanding of how to think about adversaries, and how to build systems that defend against them.

The student will learn about the different phases of penetration testing, how to gather data for your penetration test, and popular penetration testing tools. Furthermore, the student will learn the phases of incident response, important documentation to collect, and the components of an incident response policy and team. Finally, you will learn key steps in the forensic process and important data to collect. This honor course also gives a student the first look at scripting and the importance of a system analyst. This honor course is intended for anyone who wants to gain a basic understanding of Cyber security to acquire the skills to work in the Cyber security field as a Cyber security Analyst.

Expected Outcome:

The basic concept of Cyber Security, Web Security Tools Laboratory Network and system administration fundamentals Information assurance fundamentals such as confidentiality, integrity, and availability, etc. Understand various digital forensics techniques and their usage for the incident response. Applications and implementation strategies with Blockchain using smart contract understand the components of Risk, risk management framework.

INTERNET OF THINGS

Short Description:

Internet of Things(IoT) is a network of physical objects or people called "things" that are embedded with software, electronics, network, and sensors that allows these objects to collect and exchange data. The goal of IoT is to extend to internet connectivity from standard devices like computer, mobile, tablet to relatively dumb devices like a toaster.

IoT makes virtually everything "smart," by improving aspects of our life with the power of data collection, AI algorithm, and networks. The thing in IoT can also be a person with a diabetes monitor implant, an animal with tracking devices, etc.

Expected Outcome:

At the end of this major specialization the engineering graduate shall demonstrate their ability to make use the emerging technology of Internet of Things in the diversified areas like agriculture, smart cities, industries, etc. The graduates shall be able to develop IoT system to be embedded in the existing system where a smart solution to the given problem is to be provided.

COURSE STRUCTURE- 2019 PATTERN
THIRD YEAR B. TECH.INFORMATION TECHNOLOGY

SEMESTER- V

HONORS SPECIALIZATION IN CYBER SECURITY

Course		Course Title	Teaching Scheme Hours/ Week			Credits	Evaluation Scheme-Marks						
Cat.	Code						Theory			OR	PR	TW	Total
			L	T	P		ISE	ESE	CIA				
HSIT	IT8101	Foundation For Cyber Security	4	-	-	4	30	50	20	-	-	-	100
		Total	4	-	-	4	30	50	20	-	-	-	100

HONORS SPECIALIZATION IN INTERNET OF THINGS

Course		Course Title	Teaching Scheme Hours/ Week			Credits	Evaluation Scheme-Marks						
Cat.	Code						Theory			OR	PR	TW	Total
			L	T	P		ISE	ESE	CIA				
HSIT	IT8201	Foundations of Internet of Things	4	-	-	4	30	50	20	-	-	-	100
		Total	4	-	-	4	30	50	20	-	-	-	100

SEMESTER- VI

HONORS SPECIALIZATION IN CYBER SECURITY

Course		Course Title	Teaching Scheme Hours/ Week			Credits	Evaluation Scheme-Marks						
Cat.	Code						Theory			OR	PR	TW	Total
			L	T	P		ISE	ESE	CIA				
HSIT	IT8102	Web Security	4	-	-	4	30	50	20	-	-	-	100
HSIT	IT8103	Web Security Tools Laboratory	-	-	2	1	-	-	-	-	-	50	50
		Total	4	-	2	5	30	50	20	-	-	50	150

HONORS SPECIALIZATION IN INTERNET OF THINGS

Course		Course Title	Teaching Scheme Hours/ Week			Credits	Evaluation Scheme-Marks						
Cat.	Code						Theory			OR	PR	TW	Total
			L	T	P		ISE	ESE	CIA				
HSIT	IT8202	Big Data Analytics for IoT	4	-	-	4	30	50	20	-	-	-	100
HSIT	IT8203	Big Data Analytics for IoT Laboratory	-	-	2	1	-	-	-	-	-	50	50
		Total	4	-	2	5	30	50	20	-	-	50	150

IT8101: Foundation For Cyber Security
(Honors Specialization Course in Cyber Security)

Teaching Scheme	**Examination Scheme**	
Lectures: 4 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 4	**Total:**	**100 Marks**
Prerequisite Course:		

Course Objectives

1. To outline the key components and principles of security.
2. To explore the security attacks and management roles.
3. To apply the cyber security policies and procedures for organizations.
4. To practice the security tools and hardening techniques.
5. To employ the Penetration Testing and explore the Next Generation Security.

Course Outcomes (COs):

After successful completion of the course, student will be able to

	Course Outcome (s)	**Bloom's Taxonomy**	
		Level	**Descriptor**
CO1	**Select** & describe appropriate cryptographic algorithm and its application.	**4**	**Analyze**
CO2	**Apply** the cyber security policies and procedures for organizations	**3**	**Apply**
CO3	**Apply** the security tools and hardening techniques	**3**	**Apply**
CO4	**Examine** security attacks and management roles.	**4**	**Analyze**
CO5	**Select** Penetration Testing and explore the Next Generation Security.	**5**	**Apply**
CO6	**Compare** and identify the best technological solution for cyber security	**4**	**Analyze**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	-	1	1	1	-	-	-	1	3	-	3	-	3	-
CO2	2	-	-	1	-	-	-	-	-	2	-	2	-	3	-
CO3	1	1	3	3	2	3	1	1	3	-	-	1	-	3	-
CO4	-	3	-	3	-	-	2	-	-	1	-	2	-	3	-
CO5	-	2	-	3	-	-	-	-	-	3	2	2	-	3	-
CO6	2	-	3	1	3	2	-	1	3	-	-	1	-	3	-

Course Contents			
Unit-I	**USABLE SECURITY**	**No. of Hours**	**COs**
	Fundamentals of Human-Computer Interaction: users, usability, tasks, and cognitive models, Design: design methodology, prototyping, cyber security case study, Evaluation: usability studies, A/B testing, quantitative and qualitative evaluation, cyber security case study, Strategies for Secure Interaction Design: authority, guidelines for interface design.	08	CO1
Unit-II	**SOFTWARE SECURITY**	**No.of Hours**	**COs**
	Introducing Computer Security What is software security? Low level security: Attacks and exploits, Defending against low-level exploits, Web security: Attacks and defences, Designing and Building Secure Software.	08	CO2
Unit-III	**CRYPTOGRAPHY**	**No. of Hours**	**COs**
	Introduction to Classical Cryptography, Computational Secrecy and Principles of Modern Cryptography, Private-Key Encryption, Message Authentication Codes.	08	CO3
Unit-IV	**HARDWARE SECURITY**	**No. of Hours**	**COs**
	Introduction Digital System Specification, Digital System Implementation, Function Simplification and Don't Care Conditions, Sequential System Specification, Sequential System Implementation, Vulnerabilities in Digital Logic Design.	08	CO4
Unit-V	**DESIGN INTELLECTUAL PROPERTY PROTECTION**	**No. of Hours**	**COs**
	Design Intellectual Property Protection Introduction to IP Protection, Watermarking Basic, Good Watermarks, Fingerprinting, Hardware Metering.	08	CO4
Unit-VI	**PHYSICAL ATTACKS AND MODULAREXPONENTIATION**	**No. of Hours**	**COs**
	Physical Attacks (PA) Basics, Physical Attacks and Counter measures, Building Secure Systems Modular Exponentiation (ME) Basics ,ME in Cryptography, ME Implementation and Vulnerability, Montgomery Reduction.	08	CO6

Text Books:

1. Lawrence C. Miller, “Cybersecurity for Dummies”, Palo Alto Networks, John Wiley & Sons. Inc.,2ndEdition, 2016.
2. William Stallings, “Effective Cybersecurity: A Guide to Using Best Practices and Standards”, Addison - Wesley Professional Publishers, 1stEdition, 2018.

Reference Books:

1. RaefMeeuwisse,“Cybersecurity for Beginners”, Cyber Simplicity Publications, 2nd Edition, 2017.
2. Mehdi Khosrow-Pour, DBA, Information Resources Management Association, USA, “Cybersecurity and threats: concepts, methodologies, tools, and applications”, IGI Global, Vol. 1, 2018.

3. Tanenbaum, A., “Modern Operating Systems”, Prentice-Hall of India.

IT8201: Foundations of Internet of Things (Honors Specialization Course in Internet of Things)

Teaching Scheme	Examination Scheme	
Lectures: 4 Hrs./Week	**Continuous Assessment:**	**20 Marks**
	In-Sem Exam:	**30 Marks**
	End-Sem Exam:	**50 Marks**
Credits: 4	**Total:**	**100 Marks**

Prerequisite Course: Microprocessors and Microcontrollers

Course Objectives

1. To understanduse of sensors and signal conditioning in IoT.
2. To understand use of various actuators in IoT.
3. To understand use of exemplary devices in IoT.
4. To analyze security challenges in IoT.
5. To make use IoT in various application.
6. To create prototype of an IoT System.

Course Outcomes (COs):

After successful completion of the course, student will be able to

Course Outcome (s)		Bloom’s Taxonomy	
		Level	**Descriptor**
CO1	**Demonstrate** use ofsensors and signal conditioning used in IoT.	**3**	**Apply**
CO2	**Demonstrate** use of various actuators IoT.	**3**	**Apply**
CO3	**Demonstrate** use of exemplary devices in IoT.	**3**	**Apply**
CO4	**Analyze** security challenges in IoT.	**4**	**Analyze**
CO5	**Use** IoT in various applications.	**3**	**Apply**
CO6	**Create** prototype for an IoT System	**6**	**Create**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	-	-	-	-	-	-	-	-	-	-	-	-	3	-
CO2	3	2	-	2	1	-	-	-	-	-	-	-	-	3	-
CO3	3	-	1	2	2	-	-	-	-	-	-	-	-	3	-
CO4	-	3	2	3	3	3	-	-	2	1	-	-	-	3	1
CO5	-	2	3	2	3	2	2	-	3	2	1	-	-	3	2
CO6	-	3	3	2	3	2	2	-	3	2	2	1	-	3	3

Course Contents			
Unit-I	**IOT SENSORS AND SIGNAL CONDITIONG**	**No. of Hours**	**COs**
	Overview of IoT. IoT Sensors and transducers: specifications, classifications, principle of operation and applications. Signal Conditioning: operations - amplification/attenuation, filtering, protection, conversion (DAC/ADC), linearization.	08	CO1
Unit-II	**ACTUATORS IN IOT**	**No.of Hours**	**COs**
	Role of actuators, types: electrical, electromechanical, electromagnetic, hydraulic, pneumatic, smart material actuators, micro and nano-actuators.	08	CO2
Unit-III	**IOT EXEMPLARY DEVICE – RASPBERRY PI**	**No. of Hours**	**COs**
	Raspberry Pi: features, Architecture, Raspbian, Raspberry pi GPIO: serial, SPI, Interfacing with Raspberry pi.	08	CO3
Unit-IV	**SECURITY AND SAFETY**	**No. of Hours**	**COs**
	Introduction, Systems Security, Network Security, Generic Application Security, Application Process Security and Safety, Reliable-and-Secure-by-Design IoT Applications, Run-Time Monitoring, Privacy and Dependability.	08	CO4
Unit-V	**IOT APPLICATIONS**	**No. of Hours**	**COs**
	IoT Applications — Value Creation for Industry, Value Creation and Challenges, The Smart FactoryInitiative, Cost-effective Process Integration of IoT Devices, IoT for Retailing Industry.	08	CO5
Unit-VI	**CASE STUDIES**	**No. of Hours**	**COs**
	Latest Case Studies at least one on Smart City, Agriculture and Farming, Healthcare, Automobile, Home Automation, Energy.	08	CO6

Text Books:

1. OvidiuVermesan, Peter Friess, “Internet of Things: Converging Technologies for SmartEnvironments and Integrated Ecosystems”, River Publishers, 2013.
2. Adrian McEwen,HakimCassimally “Designing the Internet of Things”, John Wiley & Sons, 2014.
3. Joe Biron and Jonathan Follett “Foundational Elements of an IoT Solution: The Edge, TheCloud, and Application Development”, 1st Edition. Cisco Press, 2017.
4. R. Bishop, “The Mechatronics Handbook”, CRC Press, 2002.

Reference Books:

1. Qusay F. Hassan, “Internet of Things A to Z: Technologies and Applications”, John Wiley & Sons, 2018.
2. Alessandro Bassi, Martin Bauer, “Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model”, Springer, 2013.
3. Sean McManus, Mike Cook “Raspbery pi for Dummeis”, Wiley, 2013.
4. Dimitrios Serpanos, Marilyn Wolf, “Internet-of-Things (IoT) Systems Architectures, Algorithms, Methodologies”, Springer.

IT8102 : Web Security

Teaching Scheme	Examination Scheme	
Lectures: 3 Hrs./Week	Term Work:	NA
	Oral :	NA
	Practical:	NA
Credits: 3	Total:	100 Marks

Course Objectives

1) To study and practice fundamental techniques in developing secure web based applications.
2) To identify the vulnerabilities of web based applications and to protect those applications from attacks.
3) To impart familiarity with the security techniques that provides web security.
4) To find vulnerabilities of web based applications and various attacks.
5) To identify wide range of web security vulnerabilities and issues.
6) To learn fundamentals and advanced concept of session management and SQL injection.

Course Outcomes (COs):

After successful completion of the course, student will be able to

	Course Outcome (s)	Bloom's Taxonomy	
		Level	Descriptor
CO1	**Understand** security-related issues in Web-based systems and applications.	**2**	**Understand**
CO2	To **Understand** the fundamental mechanisms of securing a Web-based system.	**2**	**Understand**
CO3	To be able to **Implement** security mechanisms to secure a Web-based application.	**3**	**Apply**
CO4	To be able to **Evaluate** a Web-based system with respect to its security requirements	**5**	**Evaluate**
CO5	To **Analyze** the various categories of threats, vulnerabilities, countermeasures in the area of Web security.	**4**	**Analyze**
CO6	To **Describe** the inner-workings of today's real time Web application security.	**2**	**Understand**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO2	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO3	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO4	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO5	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO6	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1

(Specify Values As: 3: High Level, 2: Medium Level, 1: Low Level For Mapping of COs to POs)

Course Contents			
Unit-I	**INTRODUCTION**	**No. of Hours**	**COs**
	Introduction - Evolution of Web Applications – Web Application Security - Core Defence Mechanisms - Handling User Access - Handling User Input- Handling Attackers Security and its building blocks, Security related definition and its categories. XSS, XSS attacks, types of XSS, XSS mitigation and prevention.	06	CO1 CO2
Unit-II	**WEB APPLICATION TECHNOLOGIES**	**No.of Hours**	**COs**
	Web Functionality Encoding Schemes Mapping the Application, Sanitizing user input, validating input, client side encoding, blacklisting and whitelisting input, Rules for the browser, Default directives and wildcards, The nonce attribute and the script hash.	06	CO1 CO2
Unit-III	**CREDENTIALS MANAGEMENT**	**No.of Hours**	**COs**
	Authentication Fundamentals- Two Factor and Three Factor Authentication - Password Based, Built-in HTTP, Single Sign-on Custom Authentication- Secured Password Based Authentication: Attacks against Password, Importance of Password Complexity, Broken authentication and session management, Password: strength, transit and storage, login authentication, hashing, Password: recovery.	06	CO3 CO4
Unit-IV	**SESSION MANAGEMENT**	**No.of Hours**	**COs**
	What is session, Need for Session Management Weaknesses in Session Token Generation Weaknesses in Session Token Handling Securing Session Management, Anatomy of session attacks, session hijacking, session without cookies, session ids using hidden form fields and cookies, session hijacking using session fixation, session hijacking counter measures, session hijacking: sedejacking, XSS, malware.	06	CO3 CO4
Unit-V	**SQL INJECTION**	**No.of Hours**	**COs**
	SQLi working, Anatomy of a SQLi attack - unsanitized input and server errors, Anatomy of a SQLi attack - table names and column names, Anatomy of a SQLi attack - getting valid credentials for the site, Types of SQL injection, SQLi mitigation - parameterized queries and stored procedures, SQLi mitigation- Escaping user input, least privilege, whitelist validation.	06	CO4 CO5 CO6
Unit-VI	**WEB APPLICATION VULNERABILITY**	**No.of Hours**	**COs**
	Understanding Vulnerabilities in Traditional Client Server Application and Web Applications, Cross Domain Attack: XSRF (Cross-Site Request Forgery), XSRF with GET and POST parameters, XSRF mitigation - The referer, origin header and the challenge response, XSRF mitigation.	06	CO5 CO6

Text Books:

1. B. Sullivan, V. Liu, and M. Howard, “Web Application Security, A B Guide”, New York: McGraw-Hill. (ISBN No.: 978-0-07-177616-5).
2. D. Stuttard and M. Pinto, “The Web Application Hackers Handbook: Finding and Exploiting Security Flaws”, 2nd Edition, Indianapolis, IN: Wiley, John Sons, 2011 (ISBN No. : 978-1-118-02647-2).

Reference Books:

1. Hanqing and L. Zhao, “Web Security: A Whitehat Perspective”, United Kingdom: Auerbach Publishers, (ISBN No.: 978-1-46-659261-2).
2. M. Shema and J. B. Alcover, “Hacking Web Apps: Detecting and Preventing Web Application Security Problems”, Washington, DC, United States: Syngress Publishing, (ISBN No. 978-1-59-749951-4)
3. Hanqing Wu, Liz Zhao “Web Security: A WhiteHat Perspective” CRC press.

Online Course :

Udemy:

1. Web Security: Common Vulnerability and their Mitigation.
2. Web Application Security.

Coursera:

1. Security for the Web.

IT8103 Web Security Tools Laboratory

Teaching Scheme	Examination Scheme	
Lectures: 2 Hrs./Week	**Term Work:**	**50 Marks**
	Oral :	NA
	Practical:	NA
Credits: 01	**Total:**	**50 Marks**

Prerequisite Course:

- Basic Security Tools

Course Objectives

1. To install different software and set up Operating System for Web Security.
2. To analyze different Vulnerabilities in a web application and networks.
3. To implement SQL injection to find Vulnerabilities.
4. To understand the basics of Cross site Scripting.
5. To identify wide range of web security vulnerabilities and issues.
6. To learn fundamentals and advanced concepts of session management and SQL injections.

Course Outcomes (COs):

After successful completion of the course, student will be able to

	Course Outcome (s)	Bloom's Taxonomy	
		Level	Descriptor
CO1	To **Understand** the fundamental mechanisms of securing a Web-based system.	2	**Understand**
CO2	**Analyze** different Vulnerabilities in a web application and networks.	4	**Analyze**
CO3	To be able to **Implement** security mechanisms to secure a Web-based application.	3	**Apply**
CO4	**Implement** SQL injection to find Vulnerabilities.	3	**Apply**
CO5	To **Analyze** the various categories of threats, vulnerabilities, countermeasures in the area of Web security.	4	**Analyze**
CO5	**Implement** Cross site Scripting.	3	**Apply**

Mapping of Course Outcomes to Program Outcomes (POs) & Program Specific Outcomes (PSOs):

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO2	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO3	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO4	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO5	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1
CO6	2	3	1	1	2	2	-	2	1	1	1	2	-	3	1

(Specify Values As: 3: High Level, 2: Medium Level, 1: Low Level For Mapping of COs to POs)

Suggested List of Assignments			
Sr. No.	**ASSIGNMENTS**	**No.of Hours**	**Cos**
1	Assignment on Crawling a website	2 Hrs.	CO1
2	Assignment on Vulnerability scanning	2 Hrs.	CO2
3	Assignment on Cookie Stealing with cross site scripting	2 Hrs.	CO3
4	Assignment on XSS and SQL injections	2 Hrs.	CO2,CO4
5	Assignment on SQL injection	2 Hrs.	CO4
6	Assignment on Password security	2 Hrs.	CO5
7	Assignment on Browser security	2 Hrs.	CO5
8	Assignment on Cross site scripting	2 Hrs.	CO6

Text Books:

1. B. Sullivan, V. Liu, and M. Howard, Web Application Security, A B Guide. New York: McGraw-Hill. (ISBN No.: 978-0-07-177616-5).
2 D. Stuttard and M. Pinto, The Web Application Hackers Handbook: Finding and Exploiting Security Flaws, 2nd ed. Indianapolis, IN: Wiley, John Sons, 2011. (ISBN No. : 978-1-118-02647-2)

Reference Books:

1. Hanqing and L. Zhao, “Web Security: A Whitehat Perspective”, United Kingdom: Auerbach Publishers, (ISBN No.: 978-1-46-659261-2).
2. M. Shema and J. B. Alcover, “Hacking Web Apps: Detecting and Preventing Web Application Security Problems”, Washington, DC, United States: Syngress Publishing, (ISBN No. 978-1-59-749951-4).
3. Hanqing Wu, Liz Zhao “Web Security: A WhiteHat Perspective”, CRC press.

Online Course :

Udemy:

1. Web Security: Common Vulnerability and their Mitigation.
2. Web Application Security.

Coursera:

1. Security for the Web.