Exploiting Cross-Site Scripting, Scanning for XSS flaws, Preventing and mitigating Cross-Site Scripting, **Cross-Site Request Forgery, Identification, and Exploitation :** Testing for CSRF flaws, Exploiting a CSRF flaw, Preventing CSRF, **Attacking Flaws in Cryptographic Implementations :** A cryptography primer, Secure communication over SSL/TLS, Identifying weak implementations of SSL/TLS, Custom encryption protocols, Common flaws in sensitive data storage and transmission, Preventing flaws in cryptographic implementations

(16 hours)

UNIT III

AJAX, HTML5, and Client-Side Attacks : Crawling AJAX applications, Analyzing the client-side code and storage, HTML5 for penetration testers, Bypassing client-side controls, Mitigating AJAX, HTML5, and client-side vulnerabilities, **Other Common Security Flaws in Web Applications :** Insecure direct object references, File inclusion vulnerabilities, HTTP parameter pollution, Information disclosure, Mitigation, **Using Automated Scanners on Web Applications :** Considerations before using an automated scanner, Web application vulnerability scanners in Kali Linux, Content Management Systems scanners, Fuzzing web applications, Post-scanning actions

(16 hours)

Text Books :

(1). "Web Penetration Testing with Kali Linux", Gilberto Najera-Gutierrez, Juned Ahmed Ansari, Packt Publishing, Third Edition, 2018

(2). "Kali Linux Revealed", Mastering the Penetration Testing Distribution, Raphaël Hertzog, Offsec Press, 2017

(3). " Learn Kali Linux 2019", Glen D. Singh, Packt Publishing, 2019

(4). " Quick Start Guide to Penetration Testing", Sagar Rahalkar, Apress, 2019

CSCH 503: Cybersecurity with Blockchain

CO1 : To understand the new form of disruptive technology which is coming up in the world wide economy, as a way to assure data security.

CO2: To offer an alternative form of DNS servers, based on blockchain with better security aspects.

CO3: To consider blockchain as a means to thwart cyberattacks like DDoS.

CO4: To look into the future perspective available for cybersecurity and blockchain.

UNIT I

Cyber Threat Landscape and Security Challenges : Current threat landscape, Defender perspectives, Live attack execution, Emerging security challenges, **Evolution of Security:** The security ecosystem, The zero-trust approach, The assume breach approach, Evolution at the foundation layer, **Introducing Blockchain and Ethereum :** Introduction to blockchain, Internet versus blockchain, How blockchain works, The building blocks of blockchain, Ethereum, Private vs Public Blockchain, Business adaptation

(16 hours)

UNIT II

Hyperledger, the Blockchain for Businesses : Technical requirements, Hyperledger overview, Blockchain-as-a-service (BaaS), Architecture and core components, Hyperledger Fabric model, Bitcoin versus Ethereum versus Hyperledger, Hyperledger Fabric capabilities, **Blockchain on the CIA Security Triad :** Understanding blockchain on confidentiality, Blockchain on integrity, Understanding blockchain on availability, **Deploying PKI-Based Identity with Blockchain :** PKI, Challenges of the existing PKI model, How blockchain can help, **Two-Factor Authentication with Blockchain:** Introduction to 2FA, Blockchain for 2FA

(16 hours)

UNIT III

Blockchain-Based DNS Security Platform : Understanding DNS components, DNS structure and hierarchy, DNS topology for large enterprises, Challenges with current DNS, Blockchain-based DNS solution, **Deploying Blockchain-Based DDoS Protection :** DDoS attacks, Types of DDoS attacks, Challenges with current DDoS solutions, How blockchain can transform DDoS protection, **Facts about Blockchain and Cyber Security:** Decision path for blockchain, Leader's checklist, Challenges with blockchain, The future of cybersecurity with blockchain

(16 hours)

TextBooks:

(1). "Hands-On Cybersecurity with Blockchain", Rajneesh Gupta, Packt Publishing, 2018