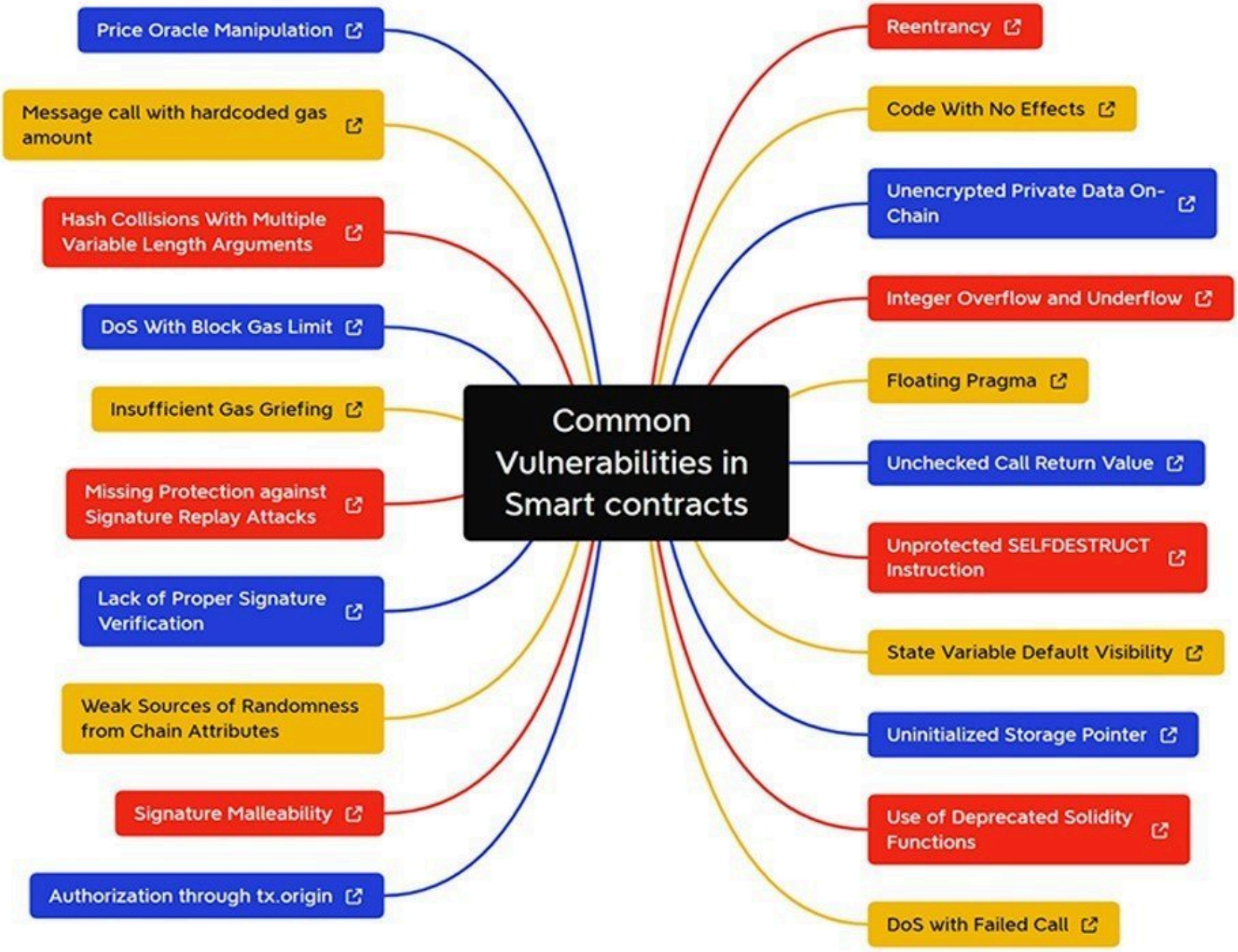
ITSOLERA
PVT LTD

Web Penetration Testing

1 LEARN
2 CERTIFY
3 ENGAGE
4 COMPETE


Common Vulnerabilities in Smart contracts
Price Oracle Manipulation
Message call with hardcoded gas amount
Hash Collisions With Multiple Variable Length Arguments
DoS With Block Gas Limit
Insufficient Gas Griefing
Missing Protection against Signature Replay Attacks
Lack of Proper Signature Verification
Weak Sources of Randomness from Chain Attributes
Signature Malleability
Authorization through tx.origin
Reentrancy
Code With No Effects
Unencrypted Private Data On-Chain
Integer Overflow and Underflow
Floating Pragma
Unchecked Call Return Value
Unprotected SELFDESTRUCT Instruction
State Variable Default Visibility
Uninitialized Storage Pointer
Use of Deprecated Solidity Functions
DoS with Failed Call

COURSE OUTLINE

Week 1:

Foundations and Common Vulnerabilities

Day 01	Introduction & Setup
Day 02	Reconnaissance Techniques
Day 03	Information Disclosure
Day 04	Cross-Site Scripting (XSS)
Day 05	SQL Injection
Day 06	Insecure Direct Object References (IDOR)
Day 07	Review & Practice

COURSE OUTLINE

Week 2:
Advanced Techniques and Less Common Vulnerabilities

Day	08	Server-Side Request Forgery (SSRF)
Day	09	Cross-Site Request Forgery (CSRF)
Day	10	Remote Code Execution (RCE)
Day	11	Broken Access Control
Day	12	API Security
Day	13	Vulnerability Chaining
Day	14	Final Challenge & Review

Day 01

Week 1: Foundations and Common Vulnerabilities

Introduction & Setup

- Overview of Bug Bounty Programs and Platforms (Bugcrowd, HackerOne)
- Setting up essential tools (Burp Suite, Nmap, Nikto, etc.)
- Creating a testing environment (e.g., vulnerable web apps like DVWA)

Day 02

Reconnaissance Techniques

- Passive Recon (Google Dorking, Whois, DNS Enumeration)
- Active Recon (Subdomain Enumeration, Port Scanning)
- Hands-on Labs

Day 03

Information Disclosure

- Understanding Information Disclosure (robots.txt, .git directories)
- Real-world examples and impact
- Practicing with Capture the Flag (CTF) challenges

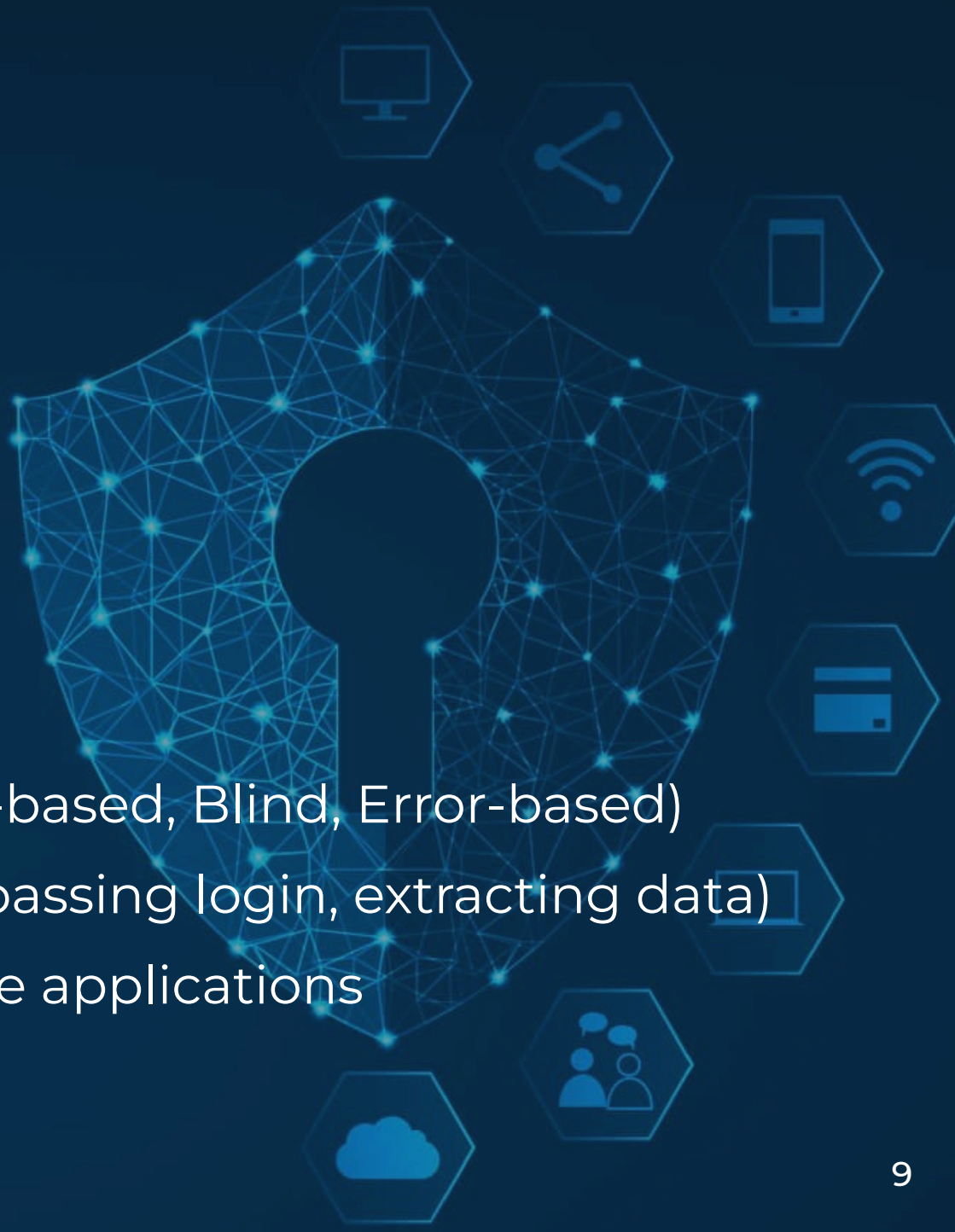
Day 04

Cross-Site Scripting (XSS)

- Understanding XSS (Reflected, Stored, DOM-based)
- Detecting and exploiting XSS vulnerabilities
- Lab exercises using XSS payloads

Day 05

SQL Injection



- SQL Injection basics (Union-based, Blind, Error-based)
- Exploitation techniques (Bypassing login, extracting data)
- Practicing SQLi on vulnerable applications

Day 06

Insecure Direct Object References (IDOR)

- Understanding IDOR and its impact
- Finding and exploiting IDOR vulnerabilities
- Lab sessions with IDOR scenarios

Day 07

Review & Practice

- Recap of the week’s lessons
- Practice with real-world bug bounty reports
- Q&A session with live examples

Day 08

Week 2: Advanced Techniques and Less Common Vulnerabilities

Server-Side Request Forgery (SSRF)

- Understanding SSRF (internal network scanning, data exfiltration)
- Exploitation techniques
- Lab exercises with SSRF scenarios

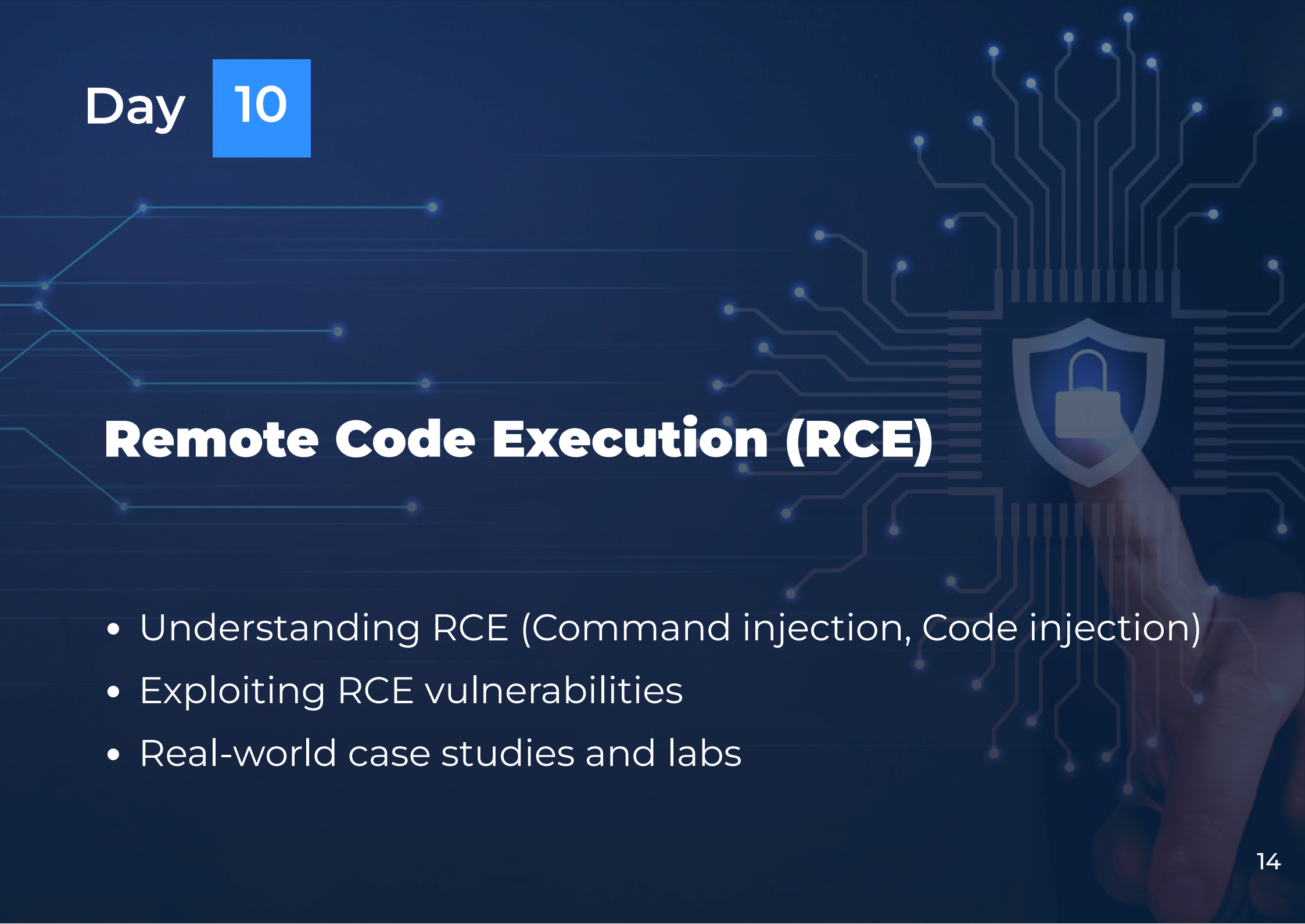
Day 09

Cross-Site Request Forgery (CSRF)

- CSRF basics (impact, exploitation)
- Bypassing CSRF protections
- Hands-on CSRF challenges

Day 10

Remote Code Execution (RCE)



- Understanding RCE (Command injection, Code injection)
- Exploiting RCE vulnerabilities
- Real-world case studies and labs

Day 11

Broken Access Control

- Types of access control issues (Vertical, Horizontal)
- Exploiting broken access controls
- Practice with vulnerable applications

Day 12

API Security

- Understanding API vulnerabilities (Broken Authentication, Rate Limiting)
- Finding and exploiting API vulnerabilities
- Lab exercises focusing on API flaws

Day 13

Vulnerability Chaining

- Understanding and identifying vulnerability chains
- Exploiting combined vulnerabilities for greater impact
- Case studies and practical exercises

Day 14

Final Challenge & Review

- Final CTF challenge covering all topics
- Review of key lessons and takeaways
- Q&A and closing session

ITSOLERA
PVT LTD

Foundations and Common Vulnerabilities

info@itsolera.com +923334471066 itsolera.com