Week 1: Introduction to Bug Hunting

- Overview of bug hunting and its importance
- Types of software bugs
- Setting up a bug hunting environment

Week 2: Common Types of Bugs

- Understanding common types of bugs (e.g., memory leaks, race conditions, buffer overflows, null pointer dereferences)
- Tools and techniques for identifying different types of bugs

Week 3: Debugging Techniques

- Overview of debugging techniques
- Understanding and using debuggers
- Using log files and other debugging tools

Week 4: Bug Reporting and Management

- Writing effective bug reports
- Understanding bug tracking systems
- Managing and prioritizing bug reports

Week 5: Fuzzing

- Understanding the principles of fuzzing

- Tools and techniques for effective fuzzing
- Fuzzing web applications and network protocols

Week 6: Reverse Engineering

- Overview of reverse engineering techniques
- Tools and techniques for reverse engineering
- Reverse engineering malware and other malicious code

Week 7: Exploit Development

- Understanding the principles of exploit development
- Common types of exploits (e.g., buffer overflows, format string vulnerabilities)
- Writing and testing exploits

Week 8: Security Testing

- Overview of security testing techniques
- Understanding and using security testing tools
- Conducting security testing on web applications, mobile apps, and other software

Week 9: Vulnerability Research

- Understanding the principles of vulnerability research
- Common types of vulnerabilities (e.g., SQL injection, cross-site scripting)
- Tools and techniques for identifying and exploiting vulnerabilities

Week 10: Real-World Bug Hunting

- Applying bug hunting skills to real-world projects
- Collaboration and teamwork in bug hunting projects
- Ethical and responsible bug hunting practices.

Week 11: Mobile Application Bug Hunting

- Overview of mobile application security
- Mobile app vulnerabilities and common attack vectors
- Tools and techniques for identifying and exploiting mobile app vulnerabilities

Week 12: Network Security and Penetration Testing

- Overview of network security
- Understanding common network vulnerabilities
- Conducting network penetration testing

Week 13: Hardware Hacking and Exploitation

- Overview of hardware hacking and exploitation
- Understanding and manipulating hardware components
- Writing and executing exploits on hardware devices

Week 14: Cryptography and Cryptanalysis

- Overview of cryptography and common cryptographic algorithms
- Cryptanalysis techniques for breaking cryptographic systems
- Identifying and exploiting cryptographic vulnerabilities

Week 15: Bug Bounty Hunting

- Overview of bug bounty programs
- Best practices for participating in bug bounty programs
- Collaborating with vendors and security teams to report and resolve vulnerabilities

Week 16: Post-Exploitation and Persistence

- Maintaining access to compromised systems

- Covering tracks and evading detection
- Understanding and mitigating post-exploitation threats

Week 17: Social Engineering and Phishing

- Overview of social engineering techniques
- Common types of phishing attacks
- Tools and techniques for identifying and exploiting social engineering vulnerabilities

Week 18: Web Application Bug Hunting

- Overview of web application security
- Common web application vulnerabilities (e.g., SQL injection, cross-site scripting)
- Tools and techniques for identifying and exploiting web application vulnerabilities

Week 19: Cloud Security

- Overview of cloud computing and cloud security
- Common cloud security vulnerabilities
- Conducting security testing on cloud infrastructure

Week 20: Advanced Bug Hunting Techniques

- Advanced bug hunting techniques and methodologies
- Research and development in the bug hunting community
- Staying up-to-date with emerging threats and vulnerabilities.