CYBERSECURITY- THE FUTURE

SECURE CODE REVIEW (PHP)

CHAITANYA CYBER STRIX
TECHNOLOGIES

SECURE CODE REVIEW IN PHP

ONLINE TRAINING

OFFLINE TRAINING

WORKSHOPS

SECURE YOUR CODE

CERTIFIED ETHICAL HACKER TRAINERS WITH OVER 5+ YEARS OF EXPERIENCE

ONE MONTH COURSE PROGRAM WITH CERTIFICATE + INTERNSHIP

Contact us

+91 81251 30203

www.chaitanyacyberstrix.com

contact@chaitanyacyberstrix.com

It's not Bookish Hacking.
It’s Actual Hacking.

When it comes to the world of hacking, theoretical knowledge can only take you so far. In a landscape that is constantly evolving and changing, practical, real-world experience is essential. It signifies a hands-on, experiential approach to hacking, where the understanding of vulnerabilities and security breaches isn’t merely academic, but grounded in real-world scenarios and practical application. This tagline asserts the importance of lived experience in the field of hacking, conveying a message of expertise and proficiency that goes beyond mere book knowledge.

DRIVING PROGRESSION, EMPOWERING SECURITY.

COURSE PREREQUISITES

- No Coding Required.
- Basic knowledge of Computer Systems.
- One year in an information security role or equivalent experience is beneficial.
- Ability to read and understand PHP code will help, although it is not mandatory.

CLASSROOM TRAINING

When it comes to quality instruction in a classroom training experience a more stimulating learning environment with our optimized mix of lecture, hands-on practice, when you have doubts our instructors are available to clear and ensure you comprehend the course and knowledge.

ONLINE TRAINING

We are providing training through Online LIVE with a real time live instructor. The live instructor teaches the course and provides the opportunity for students to ask live questions via voice or instant message during the live training event with practicals

WORKSHOPS

We conduct workshops and seminars in Information Security. Ethical Hacking & Information Security Workshop will teach you how to protect yourself from the cyber attacks and make yourself come to know how to secure your organization from hackers.

What is this Course about ?

Secure Code Review in PHP

Secure code review is a manual or automated process that examines an application's source code. The goal of this examination is to identify any existing security flaws vulnerabilities. Code review specifically looks for logic errors, examines spec implementation, and checks style guidelines, among other activities.

Manual code review involves a human looking at source code, line by line, to find vulnerabilities. Manual code review helps to clarify the context of coding decisions. Automated tools are faster but they cannot take the developer's intentions and general business logic into consideration. Manual review is more strategic and looks at specific issues.

Modules Covered - Secure Code Review

Basics of Networking

DOS

SSRF

KALI LINUX

OSI Model

CSRF

BUG BOUNTY

XSS

Cryptography

XML External Entity Attacks

OWASP TOP 10

PROTOCOLS

FOOT PRINTING

Open Redirection

Social Engineering

NET CAT

RCE

System Hacking

DOS/ DOS Attack

Webserver Hacking

SQL Injection

Pen Testing

CHAITANYA CYBER STRIX

What will you learn?

- Gain a deep understanding of foundational principles in secure coding, including concepts like input validation, output encoding, and secure cryptographic practices.
- Explore common pitfalls in software development that can lead to security vulnerabilities, such as failing to sanitize user input or using weak encryption algorithms.
- Vulnerability Identification:
- Learn to identify a wide range of potential vulnerabilities, including but not limited to SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and insecure direct object references (IDOR).
- Understand how these vulnerabilities can manifest across different layers of an application, from the frontend user interface to backend server-side logic and data storage mechanisms.
- Manual Code Examination:
- Develop advanced skills in manual code examination techniques, including code review methodologies like static analysis and dynamic analysis.
- Gain proficiency in using manual code review to uncover subtle security weaknesses that automated tools may miss, such as logic flaws or design vulnerabilities.
- Mitigation Strategies:
- Explore a variety of mitigation strategies to address identified vulnerabilities, ranging from simple input validation and output encoding to more complex cryptographic techniques and secure authentication mechanisms.

- Learn to prioritize mitigation efforts based on factors such as risk severity, ease of implementation, and potential impact on system functionality.
- Communication and Collaboration:
- Practice effective communication and collaboration skills necessary for engaging with developers, project managers, and other stakeholders during the code review process.
- Develop the ability to clearly articulate findings, provide actionable recommendations, and justify the importance of addressing security issues in a timely manner.
- Integration into SDLC:
- Understand the role of secure code review within the broader context of the software development lifecycle (SDLC), including its integration with other security activities such as threat modeling, penetration testing, and security training.
- Explore best practices for incorporating secure code review into Agile, DevOps, and other software development methodologies, ensuring that security remains a priority throughout the entire development process.
- Advocacy for Security-first Approach:
- Become advocates for a security-first approach to software development within your organization, promoting the adoption of secure coding practices, code review processes, and security tools.
- Advocate for ongoing investment in security training and awareness programs to ensure that developers and other stakeholders remain informed about the latest security threats and mitigation techniques.

CHAITANYA CYBER STRIX
TECHNOLOGIES

SECURE CODE REVIEW IN PHP

1. Introduction to Secure Code Review

- Understanding the importance of secure code review
- Benefits of secure code review for identifying vulnerabilities
- Overview of common security vulnerabilities

2. Understanding Standards of Protocols and Browser Behavior.

- HTTP
- HTTPS
- HTTP Responses

1. Information Responses
2. Successful Responses
3. Redirection Messages
4. Client Error Responses
5. Server Error Responses

- Cookies, Session, Tokens
- Browser Behavior

3. Understanding how Front End Codes and Frameworks can affect a web application

- HTML, CSS, PHP, and Frameworks nature
- Dynamic web page creation
- Possible attack on dynamic web pages
- Securing the frontend

4. Understanding Cryptography

- Encryption, Encoding, and Hashing
- Understanding Secure Radom
- Why, Where, and When to use them
- Possible attacks on cryptography
- Implementing the security best practices

CHAITANYA CYBER STRIX
TECHNOLOGIES

5. Understanding Backend Code Issues

- Authentication bypass and the reason behind the bypass
- Fixing the code to protect from an Authentication bypass
- Direct object reference Issue and Fix in code level
- What is the issue of using If else improperly in the program
- Whitelisting and black listing, When and where to apply each
- Backend directory info leaks and keeping them safe from attackers

6. Fundamentals of Software Security

- Basics of secure software development
- Common security principles and best practices
- Introduction to the OWASP Top 10 vulnerabilities

1. - Injection
2. - Broken Authentication
3. - Sensitive Data Exposure
4. - XML External Entities
5. - Broken Access Control
6. - Security Misconfiguration
7. - Cross-Site Scripting(XSS)
8. - Insecure Deserialization
9. - Using Components with Known Vulnerabilities
10. - Insufficient Logging and Monitoring

7. Code Review Methodology

- Establishing a structured code review process
- Techniques for reviewing code effectively
- Integration of code review in the software development life cycle

8. Secure Coding Guidelines and Standards

- Understanding coding standards and secure coding guidelines
- Reviewing industry-specific coding standards (e.g., CWE)
- Applying secure coding practices to prevent vulnerabilities

CHAITANYA CYBER STRIX
TECHNOLOGIES

9. Static Analysis Tools for Code Review

- Introduction to static analysis tools for code review
- Configuring and using popular code analysis tools
- Analyzing results and identifying potential vulnerabilities

10. Basic Code Review Testing

- Secure Code Testing for Input Validation
- Secure Code Testing for Authentication
- Secure Code Testing for Authorization
- Secure Code Testing for Cryptography
- Secure Code Testing for Error Handling
- Secure Code Testing for Session Management

CHAITANYA CYBER STRIX
TECHNOLOGIES